논문 2021-2-10 http://dx.doi.org/10.29056/jsav.2021.12.10

비즈니스 연속성 보장을 위한 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)를 최소화할 수 있는 재해복구시스템 구축 방안 연구

강현선*†

A Study on How to Build a Disaster Recovery System that can Minimize Recovery Time Objective(RTO) and Recovery Point Objective(RPO) to Ensure Business Continuity

Hyun-Sun Kang*†

요 약

IT 의존도가 급격히 높아진 현재 비즈니스 환경에서 재해 또는 사이버 공격으로 인한 위험도 점차 증가하고 있다. 각종 재해로 인해 비즈니스 중단이 초래된 상황에서 서비스를 계속 제공할 수 있는 능력인 비즈니스 연속성은 필수적이다. 즉, 미리 정해진 복구시간목표(RTO)와 복구지점목표(RPO) 시간 내에 신속한 복구로 핵심 비즈니스 기능을 중단 없이 유지할 수 있는 계획을 세워야 한다. 본 논문에서는 비즈니스 연속성 보장을 위한 RTO, RPO를 최소화할 수 있는 재해복구시스템 구축방안을 제시한다. 재해복구시스템 구성은 Tier 7의 재해복구 모델 및 동기식 스토리지 복제, Hot 재해복구 사이트, 운영관리 자동화 솔루션을 채택하였다. 이를 통해 데이터 손실이 거의 없고 RTO 및 RPO를 최소화함으로써 핵심 비즈니스의 연속성을 보장한다.

Abstract

In the current business environment where dependence on IT has increased rapidly, the risk from disasters or cyber-attacks is also increasing. Business continuity, the ability to continue to provide service in the event of a business disruption caused by a disaster, is essential. In other words, you need to have a plan in place to keep your core business functions uninterrupted with rapid recovery within a predetermined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) time frame. In this paper, we propose a disaster recovery system construction method that can minimize RTO and RPO to ensure business continuity. The system configuration adopts Tier 7 disaster recovery model, synchronous storage replication, hot disaster recovery site, and operation management automation solution. This ensures continuity of core business with virtually no data loss and minimal RTO and RPO.

한글키워드 : 재해복구시스템, 연속성, 복구시간목표(RTO), 복구지점목표(RPO), 자동화 재해복구시스템

keywords : Disaster recovery system, Continuity, RTO, RPO, Automated disaster recovery system

* 남서울대학교 교양대학부
† 교신저자: 강현선(email: sshskang@nsu.ac.kr)

접수일자: 2021.11.16. 심사완료: 2021.12.11.
게재확정: 2021.12.20.

1. 서 론

최근 글로벌 비즈니스 환경에서 IT를 활용한 비즈니스가 더욱 성장하고 다양해짐에 따라 정보시스템의 중요성이 강조되고 있다. 이와 같이 IT 의존도가 급격히 높아진 상황에서 지진, 호우, 강풍 등 자연 재해 또는 날로 증대되고 있는 위협적인 사이버 공격 등으로 인해 정보시스템에 대한 위험도 증가하고 있는 실정이다. 위기의 상황에서 효율적으로 대처하지 못한 경우, 기업의 재정이나 이미지 손실은 물론 경우에 따라서는 기업의 존립이 좌우될 수도 있기 때문에 체계적이고 전략적인 준비가 필요하다. 각종 재해로부터 발생한 사고로 비즈니스의 중단이 초래된 상황에서 제품이나 서비스를 계속 제공할 수 있는 능력인 비즈니스 연속성은 국가와 기업의 당면 과제로 대두되고 있다. 경쟁력 있는 비즈니스 연속성을 위해서는 비즈니스 영향분석 (BIA, Business Impact Analysis) 및 위험분석 (RA, Risk Analysis)을 통해 핵심 서비스 중단에 따른 복구시간목표(RTO)와 복구지점목표(RPO)를 설정한다. 이를 기반으로 서비스 중단 발생 시 RTO와 RPO 시간 내에 신속한 복구로 핵심 비즈니스 기능을 연속적으로 유지할 수 있는 계획을 세워야 한다[1][2]. 본 논문에서는 비즈니스 연속성 보장을 위한 RTO와 RPO를 최소화할 수 있는 재해복구 시스템 구축 방안을 제시한다. 먼저 2장에서는 관련연구로 비즈니스 연속성 계획의 동향을 분석하고, 3장에서는 RTO와 RPO를 단축할 수 있는 재해복구시스템 구축 방안을 설명하고, 4장에서는 RTO 및 RPO를 최소화하기 위한 재해복구시스템을 구성해보고 적용 기술에 대한 평가 및 분석을 진행한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

1990년대 인터넷은 개인의 일상생활과 산업에 커다란 변화를 초래하였다. 인터넷을 통한 전자상거래를 비롯하여 IT를 활용한 새로운 비즈니스 모델이 끊임없이 등장했다. 이와 함께 재해 발생 시 비즈니스 연속성을 제공하기 위한 재해복구 계획(DRP,Disaster Recovery Plan)과 비즈니스 연속성 계획(BCP,Business Continuity Planning)이 도입 되었다. 재해복구 계획 및 비즈니스 연속성 계획은 예기치 않은 재해가 발생했을 때 비즈니스 연속성을 보장하기 위한 것이다. 재해복구 계획은 재해와 장기적인 시스템 장애 발생 시 제한 시간 내에 모든 핵심 비즈니스 프로세스를 복구하도록 설계된 계획이다. 비상 상황을 처리하는데 필요한 모든 절차를 포함하며, 주로 정보시스템 인프라의 연속성을 위한 기술 복구에 중점을 두고 있다. 비즈니스 연속성 계획은 재해가 발생한 후에도 중단 없이 비즈니스를 계속하는데 필요한 활동을 말한다. 데이터 및 IT 시설의 복원에만 집중하는 재해복구 계획보다 광범위한 복구 계획에 초점을 두고 있다[3-6]. 2000년대 이후에는 기업이 위기 상황에서도 핵심 비즈니스 기능을 계획된 수준으로 지속할 수 있도록 전사적 정책 및 절차를 수립하여 이행하는 비즈니스 연속성 관리(BCM, Business Continuity Management)가 도입되었다. 비즈니스 연속성 관리는 잠재적 위험 식별과 분석을 통하여 재해가 발생할 경우 효과적으로 대응하여 정해진 시간 내에 비즈니스를 제공한다. 최근 비즈니스 연속성 보장에 대한 인식이 높아짐에 따라 비즈니스 연속성 관리시스템 (BCMS, Business Continuity Management)을 도입하는 추세이다. 비즈니스 연속성 관리시스템은 비즈니스 프로세스 및 인프라를 보호하기 위한 정책, 절차 등의 개발을 포함하는 관리 프레임워크를 제공한다. 비즈니스 연

속성 관리가 지속적인 개선 및 재해 복구 능력을 향상시키기 위해서는 비즈니스 연속성 목표 설정 및 진행 상황 관리 그리고 정기적인 교육이 필요하다[7][8].

3. 본론

핵심 비즈니스의 연속성을 보장하기 위해서는 비즈니스 영향분석 및 위험분석을 통해 재해복구 시스템 구축 대상 선정과 RTO와 RPO 값을 설정해야 한다. 이번 장에서는 재해 및 비상사태로 서비스 중단될 경우 RTO와 RPO 최소화로 비즈니스 연속성을 보장할 수 있는 재해복구시스템 구축 방안을 제시한다.

3.1 비즈니스 영향분석과 위험분석

비즈니스 영향분석과 위험분석은 비즈니스 연속성 계획 수립의 첫 번째 진행단계이다. 재해 또는 비상사태 시 핵심 비즈니스 중단에 따른 잠재적인 영향을 분석하고 평가하는 체계적인 프로세스이다. 일반적으로 비즈니스 영향분석은 인터뷰 및 설문 조사로 수집된 정보를 평가하고 고위 경영진에 결과 보고하는 등 다양한 프로세스로 진행된다. 이 과정은 비즈니스 중단으로 인한 손실 비용을 정량화하여 RTO와 RPO에 따른 복구 우선순위를 도출하는 비즈니스 연속성 계획의 핵심 절차이다. 위험분석은 정보나 정보시스템 등의 모든 자산에 대해 재해 또는 사이버 공격과 같은 잠재적 위험을 식별하고 취약점을 평가하여 자산에 미칠 부정적인 영향을 줄이기 위한 완화 전략을 개발한다. 위험분석의 평가 단계에서 비즈니스 영향분석 결과는 검토를 통해 비즈니스 복구 우선순위를 지정하는데 사용될 수 있다[9][10]. 그림 1은 재해 및 비상사태가 발생한 시점부터 비즈니스가 재개되기까지의 시간흐름을 나타낸다. RTO와 RPO는 비즈니스 중요도와 위험에 따라 결정되며, 모두 시간 단위로 측정된다. RTO는 재해가 선언된 후 핵심 비즈니스의 기능을 재개하는데 걸리는 시간으로 애플리케이션과 데이터 복구 시간을 모두 포함한다. RPO는 비즈니스 중단 시 허용 가능한 데이터 손실의 양을 기준으로 결정된다. 최대 허용 중단기간(MTPD, Maximum Tolerable Period of Disruption)은 제품 및 서비스 제공을 재개 할 수 없는 경우 조직의 생존에 위협받는 최대 중단 허용 시간을 의미한다[11]. 따라서 핵심 비즈니스의 연속성을 보장하기 위한 재해복구시스템을 구축 시 RTO 및 RPO 최소화 방안을 고려해야한다.

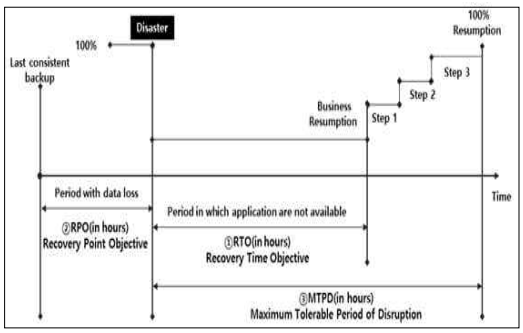

그림 1. RTO, RPO, MTPD 정의 [8]
Fig. 1. Definition of RTO, RPO and MTPD [8]

3.2 최적의 재해복구 모델 선정

1992년 SHARE(IBM 메인프레임 컴퓨팅 사용자 그룹)기술운영위원회에서 개발된 재해복구 7계층 모델을 2012년 IBM에서 보다 세부적인 내용으로 업데이트 하여 재해복구 8계층 모델을 제시하였다. 재해복구시스템 구축 시 각 계층의 특징을 정확히 이해하여 비즈니스 특성을 고려한 최적의 재해복구 모델 선정은 매우 중요하다. 다음 표 1은 IBM의 재해복구 8계층 모델에 따라 RTO와 RPO 관계를 나타낸다[10].

표 1. IBM의 재해복구 8계층 모델 [10]
Table 1. IBM as an eight tier model [10]

Classification		RPO	RTO
Tier 0	No off-site data	x	x
Tier 1	Data backup with no Hot Site	> 24H	> 48H
Tier 2	Data backup with Hot Site	16 - 24H	> 24H
Tier 3	Electronic vaulting	8 - 16H	12 - 24H
Tier 4	Point-in-time copies	4 - 8H	6 - 12H
Tier 5	Transaction integrity	8H	4 - 8H
Tier 6	Zero or little data loss	10min - few hours	1 - 6H
Tier 7	Highly automated business-integrated solution	Seconds - 10min	< 2H

Tier 0은 재해복구 계획이 없으므로 복구시간은 예측할 수 없고 비즈니스 회복이 불가능하다. Tier 1은 오프사이트(Off-site) 시설에 데이터 백업을 안전하게 보관은 하지만 데이터 복원할 시스템은 없다. 백업 빈도에 따라 몇 일에서 몇 주 동안의 데이터 손실이 발생할 수 있다. Tier 2는 핫사이트(Hot-site)를 통한 데이터 백업은 정기적으로 진행하며, 데이터 복원을 위한 오프사이트(Off-site) 시설과 인프라가 구축되어 있다. 복구시간을 예측할 수 없으며, 몇 시간에서 몇 일 분량의 손실된 데이터는 다시 생성해야 한다. Tier 3은 Tier 2의 시설 및 인프라를 활용하여 일부 필수 데이터는 전자적으로 보관되기 때문에 Tier 2보다 데이터가 최신이므로 재해 발생 후 데이터 재생성과 손실이 적다. Tier 4는 디스크 기반 솔루션을 사용하여 데이터를 복제하기 때문에 테이프 백업보다 더 많은 빈도로 복사본 생성이 용이하다. 데이터의 빠른 복구가 가능하지만 몇 시간의 데이터 손실은 여전히 발생할 수 있다. Tier 5는 백업 및 복구 시 데이터 무결성(Data integrity)이 요구되며, 일관성이 요구되는 모델이다. 데이터 손실이 거의 발생하지 않으며, 재해복구 시간은 전적으로 사용 중인 응용 프로그램에 의존한다. Tier 6의 재해복구 솔루션은 최고 수준으로, 데이터 손실이 거의 없으며 데이터 무결성을 유지한다. 애플리케이션의 신속한 복원을 요하는 모델이다. 마지막으로 Tier 7은 Tier 6의 재해복구 솔루션에 자동화된 비즈니스 통합 솔루션을 포함하며, 보다 높은 수준의 데이터의 무결성 보장과 함께 신속하고 안정적으로 시스템 및 응용 프로그램 복원이 가능하다 [10][12].

3.3 최적의 재해복구 솔루션 선정

핵심 비즈니스의 연속성을 보장하기 위해서는 RTO 및 RPO 값을 줄이기 위한 최적의 재해복구 솔루션이 필요하다. 그림 2는 재해복구 솔루션에 따른 RTO 및 RPO, 구축비용 간의 관계를 나타낸다. X축은 재해복구시스템 구축 비용을 나타내고 Y축은 RTO 및 RPO 값을 나타낸다.

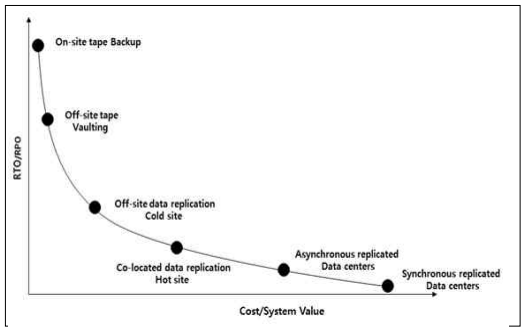

그림 2. RTO 및 RPO, 구축비용 간의 관계
Fig. 2. RTO, RPO and implementation cost

그림 2에서 데이터센터 내에 테이프 백업(on site tape Backup)은 센터 내에 주기적으로 데이터를 저장하는 방법으로 데이터에 대한 즉각적인 접근과 비용이 저렴한 반면 재해가 발생할 경우 데이터 손실 가능성이 매우 높다. 특정 장소에 테이프 금고 보관(off-site tape vaulting)은 RPO

조건에 따라 2개의 백업 테이프 복사본을 만들어 최적의 오프사이트 장소에 보관하는 것을 말한다. 특정 장소인 콜드 사이트에 데이터 복제(off-site data replication cold site)는 기본적으로 전원, 냉각, 통신장비와 같은 기본 시설을 갖춘 공간에 데이터를 복제하는 방법으로 재해 발생 시 복구하는데 상당한 시간이 소요된다. 공동으로 사용하는 핫 사이트에 데이터 복제(co-located replication data hot site)는 공용으로 사용하는 시설에 중요한 데이터 백업 또는 복제를 실시간으로 수행함으로 재해의 영향으로 가동 및 중지 시간과 데이터 손실을 최소화할 수 있다. 데이터센터에 비동기 복제(asynchronous replicated data centers)는 원거리에 정의된 일정에 따라 데이터 복제를 하며 RTO는 동기식 복제에 비해 길다. 데이터센터에 동기식 복제(Synchronous replicated data centers)는 실시간 데이터 복제로 RTO가 짧기 때문에 재해 발생 시 매우 안정적으로 재해복구 할 수 있다. 반면 실시간으로 지속적으로 복제를 해야 하므로 비용이 많이 든다. 동기식 스토리지 데이터 복제 방식은 운영 스토리지에 업데이트된 데이터가 원격지의 스토리지에 완전히 저장된 후 프로세스가 완료된다. 이 복제 방식은 데이터 복제를 위한 네트워크 대역폭 가용성과 네트워크 통신대기 시간이 중요하기 때문에 주로 단거리 재해복구 솔루션에서 사용한다. 비동기식 스토리지 데이터 복제는 원격지에 초기에 데이터를 복제한 후, 변경된 데이터만 원격지로 전송하는 복제 방식으로, 네트워크 지연 성능 문제로 인한 데이터 복제에 영향이 없기 때문에 장거리 재해복구 솔루션에서 주로 사용된다. 따라서 핵심 비즈니스의 연속성을 보장하기 위한 RTO 및 RPO 최소화를 위한 최적의 재해복구 솔루션은 동기식 스토리지 데이터 복제 방식을 고려해야한다[12].

3.4 최적의 재해복구 사이트 유형

재해복구 사이트 유형은 미러 사이트(Mirror Site), 핫 사이트(Hot Site), 웜 사이트(Warm Site), 콜드 사이트(Cold Site)로 분류한다. 핵심 비즈니스 연속성 보장을 위해서는 재해복구 사이트 유형의 특징을 정확히 파악하여 RTO 및 RPO 요구 사항에 맞는 최적의 재해복구 사이트 구축이 필요하다. 미러 사이트는 비즈니스 환경과 거의 동일한 환경으로 데이터가 동기화되고 운영하기 때문에 RPO는 거의 0에 가깝고, RTO는 거의 0에서 수분 이내로 소요된다. 핫 사이트는 재해 발생으로 영향을 받는 비즈니스 기능을 복구할 수 있도록 주 데이터센터와 동일한 운영 환경의 재해복구시스템이 대기 상태로 유지한다. 실시간 데이터 복제로 재해 발생 시 재해복구시스템으로 전환하여 복구되며, RTO는 약 4시간 이내로 소요된다. 웜 사이트는 부분적인 설비와 가격이 저렴한 정보시스템 주변기기를 가지고 있는 백업 사이트로 RTO는 수일 이내로 소요된다. 콜드 사이트는 전기, 냉방, 공간 정도만 마련되어 있는 백업 센터로 RTO는 수주에서 1개월 정도 소요된다[12][13].

3.5 재해복구 운영 자동화 솔루션 도입

재해복구 운영 자동화 솔루션 도입은 정보시스템 관리의 일반화, 표준화, 자동화로 운영 관리 및 비용 효율성 높일 수 있으며, RTO를 단축함으로 비즈니스 연속성을 보장한다. 재해복구 운영 자동화 솔루션은 주 데이터센터와 재해복구센터에 에이전트 서버를 구성하며, 에이전트 서버는 재해 발생 시 재해복구 시나리오에 따른 스크립트를 실행한다. 마스터 서버는 주 데이터 센터의 운영시스템과 재해복구센터의 재해복구시스템의 계정, 설치 패키지, 환경 설정 파일 등을 주기적으로 비교 점검한다. 또한 재해복구를 위한 시스템의 연관 관계 및 순서에 따른 가동 및 중

지 절차 스크립트 배포 및 등록, 통합 대시보드를 통하여 진행 상황 모니터링과 재해복구 조직과 정보를 공유한다. 정기적인 재해복구 모의 훈련으로 재해 복구 절차를 검증하고 문제점을 보완함으로써 재해발생 시 RTO값을 줄임으로 핵심 비즈니스 연속성을 보장할 수 있다[14][15].

4. 재해복구시스템 구성 및 분석

이번 장에서는 RTO 및 RPO를 최소화하기 위한 재해복구시스템을 구성해보고 적용 기술에 대한 평가 및 분석을 한다.

4.1 재해복구시스템 구성

재해복구시스템은 운영시스템의 비즈니스 연관 관계 및 비즈니스 영향도 분석(BIA)을 통해 대상을 선정하였다. 그림 3은 운영시스템과 재해복구시스템의 구성을 나타낸다.

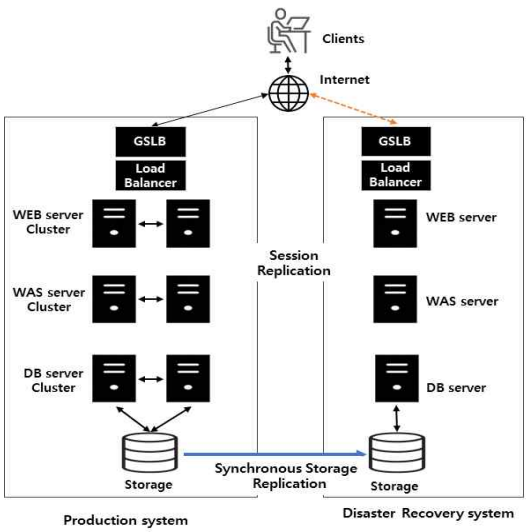

그림 3. 운영시스템과 재해복구시스템의 구성
Fig. 3. Operating system and Disaster recovery system

핵심 비즈니스의 연속성 보장을 위해 구축된 재해복구시스템의 RTO은 4시간 이내, RPO은 데이터 손실이 거의 없는 것을 목표로 한다. 운영시스템과 재해복구시스템은 Linux 서버, Oracle 데이터베이스, 통합 스토리지로 데이터를 공유하는 전형적인 3 Tier 아키텍처 구조이며, 운영시스템과 재해복구시스템의 부하분산 및 안정적인 서비스 전환을 위해 GSLB(Global Server Load Balancing)와 WEB/WAS 서버는 Active-Active로 구성하였다. 데이터의 무결성을 유지하기 위하여 동기식 스토리지 복제방식 적용과 재해복구 운영 관리 자동화 솔루션을 도입한다.

4.2 적용기술 분석 및 평가

이번 절에서는 재해복구시스템 구성에서 적용된 기술에 대해서 평가 및 분석한다. 표 2는 핵심 비즈니스 연속성 보장을 위한 RTO 및 RPO 최소화할 수 있는 적용 기술에 대한 분석 및 평가를 나타낸다. 비즈니스 영향도 및 위험 분석은 비즈니스 중단에 대한 잠재적 영향 및 위험을 평가하는 프로세스로 RTO와 RTO에 따른 복구 우선순위와 시스템의 상호 연관성 및 종속관계를 분석하여 최종적으로 재해복구시스템 구축 대상을 선정한다. 재해복구시스템 구축을 위해서는 복구범위와 수준 설정이 선행되어야 한다. 재해발생에 따른 비즈니스 중단에 따른 수용 가능한 RTO와 RPO을 고려하여 적절한 복구목표수준(RLO,Recovery Level Objective)을 설정한다. 재해복구시스템은 실제 평상시에 온라인 서비스에 활용여부에 따라 운영 환경을 결정할 수 있다. 일반적으로 재해 상황을 대비하여 서버는 운영시스템의 약 50-70% 용량, 스토리지 용량은 데이터복제를 위해 동일한 용량으로 재해복구시스템을 구축한다. WEB/WAS는 운영시스템과 재해복구시스템을 세션 복제방식의 Active-Active로 구성하면 평상시 운영 시스템의 부하 분산이 가

능하다. 또한 재해복구시스템을 재해복구 환경과 개발 및 테스트 환경으로 분리하여 테스트 및 검증용으로 활용하면 품질향상을 도모할 수 있다. 재해복구 모델은 Tier 7 및 동기식 스토리지 복제방식, Hot Site의 재해복구 사이트 선정으로 데이터손실이 거의 없고 재해복구 운영관리를 자동화된 솔루션으로 재해복구 운영관리의 표준화 및 자동화로 RTO 및 RPO을 최소화함으로 핵심 비즈니스의 연속성을 보장한다.

표 2. 적용 기술에 대한 분석 및 평가
Table 2. Disaster recovery application technology evaluation

구분	기술 분석 및 평가
비즈니스 영향분석(BIA) 및 위험분석(RA)	-비즈니스 중단에 따른 잠재적 영향 평가 및 위험 분석 -주요 업무 프로세스 상호연관성 분석 -시스템 상호연관 및 종속관계 -재해복구 우선순위 및 대상 선정
RTO ,RPO 목표 설정	-서비스 중단의 수용가능 복구수준 설정
재해복구시스템 환경	-전형적인 3 Tier 아키텍처 -평상시 활용을 위한 용량산정 -운영시스템의 50-70% 용량
재해복구 모델 선정	-재해복구모델은 Tier 7 선정 -데이터 손실 거의 없는 수준 -재해복구 운영관리 솔루션 -RPO는 10분 이내 -RTO는 2시간 이내
재해복구 솔루션 선정	-동기식 스토리지 복제 -실시간 데이터 복제
재해복구 사이트 선정	-핫 사이트(Hot Site) -운영센터와 동일설비와 자원 -WEB/WAS Active-Active구성 -Data Base 실시간 복제 -DB Server 대기 상태
재해복구 운영관리 자동화	-워크플로우, 재해복구운영관리 표준화와 자동화 -운영시스템과 재해복구시스템 구성 비교 -주기적인 모의 훈련으로 문제점 파악 및 보완
GSLB	-재해복구시스템 Health check -운영시스템의 부하 분산 -신속한 재해복구시스템 전환

GSLB 및 Load Balancer를 구성함으로써 서버 모니터링을 통한 운영 시스템의 부하 분산과 재해 발생 시 재해복구시스템으로 신속한 전환이 가능하다. 최적의 RPO 및 RTO 목표로 설계되고 구축된 재해복구시스템은 일정시간이 지나면 비즈니스 환경의 변화에 따른 복구에 대한 현실적인 의문이 생긴다. 따라서 변화하는 IT 환경에 대응하는 재해복구 훈련과 복구에 대한 운영관리에 대한 모니터링이 필요하다. 재해복구시스템과 운영시스템과의 재해복구를 위한 구성 요소 감시를 통해 재해복구훈련, 워크플로우 및 복구 절차에 대한 포괄적인 자동화로 RTO를 단축할 수 있는 재해복구운영 자동화 솔루션이 필요하다.

5. 결 론

비즈니스 연속성은 각종 재해 및 비상사태로 인해 서비스 중단이 초래된 상황에서 제품이나 서비스를 계속 제공할 수 있는 능력을 말한다. 비즈니스의 연속성을 보장하기 위해서는 가장 먼저 비즈니스 영향 분석 및 위험 분석을 통해 RTO와 RPO 설정을 통한 재해복구시스템 구축 대상을 선정해야 한다. 미리 정해진 RTO와 RPO 시간 내에 신속히 복구함으로써, 핵심 비즈니스의 연속성을 보장하게 된다. 본 논문에서는 비즈니스 연속성 보장을 위한 RTO와 RPO를 최소화할 수 있는 재해복구시스템 구축 방안을 제시, 구성하였다. 자연 재해와 위협적인 사이버 공격이 증가하는 최근 실정에 능동적으로 대비하기 위해서 현재 비즈니스 상황을 고려한 체계적이고 전략적인 비즈니스 연속성 계획을 준비하여 각종 재해 및 비상사태에 대비해야 할 것이다.

이 논문은 2021년도 남서울대학교 학술연구비 지원에 의해 연구되었음

참 고 문 헌

[1] Nijaz Bajgoric, “Business continuity management: asystemic framework for implementation”, Kybernetes, Vol. 43 No. 2, pp.156-177, Feb. 2014. https://doi.org/10.1108/K-11-2013-0252

[2] Paul Kirvan, Sonia Lelii, “Data center disaster recovery plan template and guide”, TechTarge, Nov. 2017. https://searchdisasterrecovery.techtarget.com/Data-center-disaster-recovery-plan-template-and-guide

[3] Vyshnavi Jorrigala, “Business Continuity and Disaster Recovery Plan for Information Security”, Submitted to the Graduate Faculty of Saint Cloud State University, Graduate dissertation. Saint Cloud State University, Saint Cloud, Dec. 2017. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1068&context=msia_etds

[4] Hyun-Sun Kang, “A study in Information System and Disaster Recovery System for Business Continuity”, Journal of Security Engineering, 15(5), 319-332, Oct. 2018. DOI: 10.14257/jse.2018.10.04

[5] TTA (Telecommunications Technology Association), “A Guide to the Contingency and Disaster Recovery Plan for Public Information Systems”, Bundang: TTA, Dec. 2013. http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAK.KO-12.0009/R1&nowSu=1

[6] Yasin AKILLI, Ali Güneş, “Disaster Recovery Planning for Data Centers and IT Services”, International Advanced Research Journal in Science, Engineering and Technology (IARJSET), 3(6), 145-149, June 2016. DOI: 10.17148/IARJSET.2016.3627.145

[7] ISO/TC 292 Security and resilience, “Security and resilience-Business continuity management systems-Requirements”, Geneva: International Organization for Standardization, Oct. 2019. https://www.iso.org/standard/75106.html

[8] ISO/TC 292 Security and resilience, “Societal Security-Business Continuity Management Systems-Requirements”, Geneva: International Organization for Standardization, May 2012. https://www.iso.org/standard/50038.html

[9] ISO/TC 262 Risk management, “Risk management-Guidelines”, Geneva: International Organization for Standardization, Feb. 2018. https://www.iso.org/standard/65694.html

[10] Ellis Holman, “A Business Continuity Solution Selection Methodology”, IBM Corporation, March 2012. https://share.confex.com/Handout/ Session10387

[11] Marek Zdrojewski, “Business continuity/disaster recovery”, default reasoning, Dec. 2013. https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

[12] Charlotte Brooks et al., “IBM System Storage Business Continuity: Part 1Planning Guide”, IBM Corporation, Mar. 2007. https://www.redbooks.ibm.com/redbooks/pdfs/sg246547.pdf

[13] Chongsoo Cheung, Woonggyu Choi, “A Study on the Framework of Quick-Hit for BIA and RA in BCMS”, J. Korean Soc. Hazard Mitig 2019, 19(4), 81-87, Aug. 2019. DOI: https://doi.org/10.9798/KOSHAM.2019.19.4.81

[14] Young-Hee Jeong, Jung-Hoon Lee, Eun-Young Kim, “A Study on the Critical Success Factors and Practical Method of Information System Disaster Recovery: Assuring Business Continuity of Information System Interface Specification Modeling”, Journal of the Korea society of IT services, 10(4), 83-101, Dec. 2011. DOI: 10.9716/KITS.2011.10.4.083

[15] Honglin Han, Lin Li, Dehai ZhuH, “Research and Implementation on Remote

Disaster Recovery System", International Conference on Computer Science and Service System, Aug. 2012, Nanjing, China. DOI: 10.1109/CSSS.2012.223

저 자 소 개

강현선(Hyun-Sun Kang)

2002.2 단국대학교 전자계산학과 졸업
2004.2 단국대학교 전자계산학과 석사
2007.2 단국대학교 전자계산학과 박사
2010.9-현재 : 남서울대학교 교수
<주관심분야> 정보보안, 정보시스템