通信情報保護學會誌
第 11 券 第 1 號, 2001. 2

# 정보시스템 재해에 대비한 업무 지속성 관리

김 종 기*, 김 기 윤**, 이 경 석***, 김 정 덕****

요 약

정보시스템이 기업 활동의 중추적인 역할을 담당하게 됨에 따라 정보시스템을 안전하고 지속적으로 운영하기 위한 합리적인 방안을 모색하는 것은 기업의 활동의 연속성을 보장하기 위한 핵심적인 요소로 인식되고 있다. 최근의 기술 및 경영 환경의 급격한 변화는 정보시스템 재해에 대한 대책에 있어서도 종래의 기술 중심에서 업무의 지속성을 보장하기 위한 방안의 수립으로 변화하고 있다. 본 논문에서는 기업 활동에 치명적인 장애를 초래하는 재해에 대비하기 위한 비상계획의 개념과 변천과정을 살펴보고, 최근에 대두된 업무 지속성 관리의 측면에서 업무 지속성 계획을 수립하고 운영하는 방법론을 CCTA에서 제시한 수명주기를 중심으로 살펴본다.

## Ⅰ. 서 론

오늘날 기업 경영에 있어서 정보시스템은 필요 불가결한 기반체계로 자리잡고 있다. 기업 활동의 수행에 있어서 정보시스템에 대한 의존도는 나날이 높아지고 있으며, 특히 기업 활동의 지원 기능만을 수행하는 것이 아니라 전자상거래와 같이 수익 창출에 직접적인 수단으로 활용됨에 따라 정보시스템의 지속적인 운영은 기업 활동의 연속성을 보장하기 위한 핵심적인 전제조건이 된다. 따라서, 정보시스템 운영의 중단이 장기화된다면 기업 존립의 위기 상황으로 이어질 개연성이 커진다.

재해로 인하여 정보처리 능력에 심각한 타격을 입을 경우에 조직의 생존 자체에 위협을 받게 된다. 미네소타 대학의 연구에 따르면 10일 이상 전산능력이 상실되었을 경우에 해당 기업의 93%가 1년 내에 파산하였다[1].

영국의 CCTA(Central Computer and Telecommunications Agency)에서 1990년에 175개의 기관을 대상으로 비상사태의 발생원인을 조사한 바에 따르면 아래의 그림과 같이 많은 재해들은 인위적 혹은 자연적인 원인으로 발생한 물리적인 재해이다.[2] 그런데, 재해 발생 원인의 약 사분의 일 정도는 소프트웨어의 결함으로 인한 것으로 나타났다. 오늘날에는 물리적인 재해뿐만 아니라 소프트웨어나 하드웨어, 네트워크에 대한 기술적인 원인으로 인한 재해의 발생이 종종 보고되고 있으며, 향후에도 이런 유형의 장애 발생 가능성이 매우 높아질 것이다.

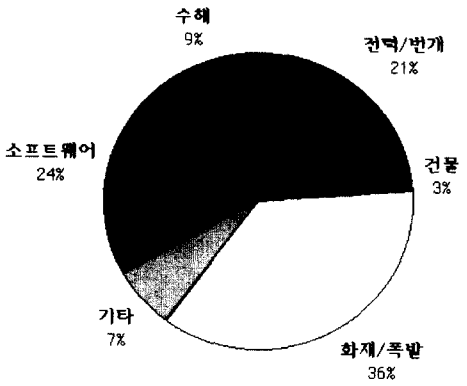



그림 1. 재해의 발생 원인

정보시스템의 분산화와 네트워크화와 같은 정보기술의 발전은 기업 활동의 수행에 있어서 보다 효과적이고 효율적인 의사소통 수단을 제공하지만, 그에 비례하여 중앙집중적인 관리와 통제가 어렵기 때문에 보안의 측면에서 불리한 요인으로 작용한다.

2000년 2월에 발생한 Yahoo, Amazon, e-Bay, CNN.com 등 미국의 여러 인터넷 싸이트에 대한 서비스 거부 공격이 발생한 사례와 미국 국방부 싸이트에 대한 공격이 급격하게 증가하고 있는 사례[3]에서도 보여지듯이 인터넷을 이용한 정보시스템의 네트워크화는 해커와 같은 시스템 외부로부터의 심각

한 위협 요인을 초래하고 있다.

본 논문에서는 변화하는 기업 환경에 부응하여 정보시스템 재해에 대비한 비상계획(contingency planning)의 새로운 개념을 살펴보고, 기업 활동의 지속성을 보장하기 위한 비상계획의 수립 방법론을 업무 지속성 관리(BCM: Business Continuity Management)의 관점에 논의하고자 한다.

## II. 업무 지속성 관리의 개념과 방법론

### 1. 업무 지속성 관리의 개념과 변천과정

정보시스템의 장애를 초래하는 원인과 그 결과의 심각성은 일상적인 유지보수 활동에 의한 해결에서부터 장기간에 걸친 해결 노력을 필요로 하는 것에 이르기까지 매우 넓은 범위를 가진다. 재해에 대한 개념을 NIST(National Institute of Standards and Technology)[4]에서는 "컴퓨터 운영의 붕괴로 조직의 정상적 기능이 파괴되는 비상사태"라고 정의하고 있으며, Owen[5]은 "생명, 재산, 자산, 그리고 정상적인 운영능력에 대한 위험"이라고 정의한다. 이와 같이 재해는 일반적으로 정보시스템의 자산에 대해서 위협이 매우 파괴적인 경우에 그 결과로써 발생되는 손실이라고 할 수 있다. 이러한 심각한 상황에 적절히 대응하여 손실을 최소화하기 위한 방안을 사전에 고안하는 것은 아주 자연스러운 행동이다.

이러한 정보시스템의 재해를 인간의 실수에 의한 재해, 의도적인 재해, 자연 재해 등 세 가지로 분류할 수 있다. 재해 복구에는 인명, 재산 및 자산의 보호, 그리고 사업 운영 능력의 복구가 포함된다. 재해복구의 목적을 구체적으로 살펴보면, 1) 조직구성원 및 고객의 안전과 복지를 지키는 것, 2) 기업의 자원과 자산 그리고 기존 운영을 보호하는 것, 3) 운영중단에 적시적이고 효과적으로 대응하는 것, 4) 가능한 즉시 정상적인 운영을 재개시키는 것, 5) 변화하는 사업 목적과 운영에 대비하는 것 등이다.[1]

재해에 대한 대응 방법의 역사적인 변천 과정을 살펴보면 1960년대에는 재해복구의 주 대상이 메인프레임과 주변장비와 같은 하드웨어에 초점을 맞추었다. 하드웨어의 안정성이 취약하고 비즈니스의 정보시스템에 대한 의존도가 상대적으로 낮았던 당시의 상황을 비추어 보면 당연한 결과이기도 했다. 1970년대 이후에는 전산센터의 역할이 커지면서 자연스럽게 재해복구의 대상도 전산센터의 복구에 초점을 맞추었고 이 당시 정보시스템 재해 복구를 위한 기술적 수단들이 상당부분 개발되었다. Hot site나 상호 협정과 같은 재해복구 수단이 유행되기 시작하였으며, 1980년대에 들어서 재해복구를 위한 상용 서비스를 제공하는 업체가 등장하였다.

정보시스템의 네트워크화와 분산화에 따른 기술환경의 변화와 더불어 권한 위임, 팀제, 자율 중심의 조직문화의 확산과 같은 조직 환경의 변화와 전세계적인 경쟁체제를 요구하는 경영 환경의 변화로 말미암아 정보시스템 재해 복구에 있어서도 기존의 하드웨어나 전산센터 중심의 복구계획만으로는 업무의 연속성을 유지하고자하는 비상계획의 본래의 목적을 달성할 수 없다는 사실을 인지하게 되었다. 따라서 1980년대 중반 이후 궁극적인 재해복구의 목적은 전산센터의 복구가 아니라 비즈니스의 중단 없는 운영, 즉 지속성을 유지하는 것이라는 인식이 대두되기 시작하였다.

중요 복구 대상이 하드웨어에서 핵심 응용시스템으로 전이됨에 따라 최종 사용자의 관점에서의 복구라는 패러다임의 변화가 요구되었다. 이와 같이 복구계획이 전산센터의 복구뿐만 아니라 고객 서비스에 초점을 두기 시작하면서 "업무 지속성(business continuity)", "업무 재개(business resumption)" 등의 용어가 1980년대 후반에 출현하기 시작했다. 그러나 비즈니스 운영의 백업 서비스를 제공하기 위해서는 수많은 난제를 해결해야 한다. 재해가 비즈니스에 주는 영향을 이해하는 것은 물론, 재해복구를 적절한 복구팀 구성, 훈련, 관련 응용분야간의 협력과 조화 등 전사적인 노력을 요구하는 비즈니스 문제로 간주하여야 한다.

1980년대 중반부터 출현하기 시작한 업무 지속성 계획은 아직까지 구체화되지 않은 개념 수준이고 이를 실무적으로 사용하기에는 아직 해결해야 할 문제가 많다. 실제 조직에서 사용할 수 있는 업무 지속성 계획을 위해서는 다음과 같은 요구사항을 만족시켜야 할 것이다:

- 최고경영자의 관심 및 지원 확보
- 전사적인 업무지속성 계획에 대한 협력과 조화
- 조직의 목표 및 전략과 업무 지속성 계획과의 연계
- 조직의 핵심 프로세스나 기능의 중요도를 측정할 수 있는 척도 개발
- 재해복구 기술 및 사용자 환경을 고려한 대안 개발 및 선택 기준

- 업무 지속성 계획의 효과성을 보장하기 위한 통제수단

업무 지속성 관리 계획의 수립은 일회성 프로젝트가 아니라 지속적으로 조직의 경영 및 기술환경의 변화를 즉각적으로 반영할 수 있어야 하는 일련의 관리과정이다. 계획의 실행에서 발견되는 미비점을 보완하여야 하며 응용시스템, 백업 설비나 자원의 변화를 반영하기 위해 지속적으로 갱신되어야 한다. 아무리 세심하게 계획을 작성하고 준비를 하여도 취약요소는 존재하기 마련이다. 예를 들면 hot site 계약을 체결하여도 국지적인 재해가 발생하였을 경우, hot site를 체결한 조직간에 경쟁이 발생할 수 있다. 즉 테스트 시간의 제한, 불충분한 하드웨어 능력 등이 문제가 될 수 있다. 또한 업무의 중단을 초래할 모든 가능한 위협 요인들을 정확하게 예상한다는 것은 불가능할 뿐만 아니라 바람직하지도 않다. 따라서 업무 지속성 계획을 효과적으로 개발하고 유지보수할 수 있는 업무 지속성 관리에 대한 개념적 틀과 방법론 개발이 필수적이다.

## 2. 업무 지속성 관리의 내용과 단계

정보시스템의 재해복구 계획을 크게 수평적 지원서비스(horizontal support services)와 수직적 사업단위(vertical business units)의 두 가지 측면으로 구성되는 행렬표를 이용하는 방안이 있다[8]. 여기서 수평적 지원서비스란 주요 사업단위를 지원하는 기능으로서 자료처리, 자료통신, 음성통신, 시설 등이고, 수직적 사업단위란 조직의 사업을 실행하는 것으로 예로써, 제조기업인 경우에 구매, 재고통제, 마케팅, 재무관리 등이다. 또한, 구체적으로 재해복구계획을 자료처리, 음성 및 데이터 통신, 최종사용자, 부서 시설 및 주요시설 등 5가지 영역으로 구분한다.

업무 지속성 관리를 수행하기 위해서 먼저 업무 지속성 계획을 수립하여야 하며, 업무 지속성 계획은 적절한 보호대책이 수립되어 있음에도 불구하고 발생할 가능성이 있는 각종 재해와 비상사태에 대비하기 위한 조직편성, 정책 및 절차의 수립과 대체처리 시설의 확보를 통해 조직의 업무가 지속적으로 유지될 수 있도록 하는 일련의 계획이다.

업무 지속성 관리의 단계에 대해서는 여러 연구가 있다[6, 8, 9, 10]. Jackson[8]은 다음과 같은 5단계로 분류하였다:

1) 프로젝트 개시단계
2) 취약성 혹은 업무영향 평가단계
3) 복구대안 선택단계
4) 복구계획 개발단계
5) 복구계획 테스트 및 유지관리 단계

그리고 Moore[10]는 다음과 같은 4단계로 분류하였다:

1) 프로젝트 개시
2) 업무영향분석
3) 계획수립
4) 계획의 테스트 및 유지

한편 Fulmer[6]는 다음과 같은 12단계를 제시하였다:

1) 목표, 영역 및 가정사항의 기술
2) 계획 조정자와 개발 팀: 직무기술
3) 행위, 책임 조정 및 시간의 할당
4) 위험평가 실시
5) 업무영향분석의 실시
6) 복구 팀의 구성
7) 응급조치계획의 개발
8) 대체 업무처리장소 및 서비스 공급업자 선정
9) 업무 지속성 계획의 기술
10) 계획의 테스트
11) 계획의 배포
12) 계획의 유지보수

CCTA[2]의 업무 지속성 관리 수명주기는 다음과 같은 4단계로 구성되어 있다. 첫 번째 단계는 개시단계로서 업무 지속성 관리에 관한 정책의 수립, 참조내용과 범위의 명시, 자원분배, 프로젝트 조직, 통제구조, 계획에 대한 정의 및 합의라는 활동으로 구성된다. 두 번째 단계는 전략수립 단계로서 업무영향분석, 위험평가, 업무연속성전략을 수립하는 활동으로 구성된다. 이 단계는 효과적이고 효율적인 업무 지속성 관리를 위해서 가장 중요한 단계라고 할 수 있다. 세 번째 단계는 구현 단계로서 조직 및 실행계획, 예비계획의 실행, 업무복구계획의 개발, 위험축소조치의 실행, 절차 개발, 초기 테스트이라는 활동으로 구성된다. 네 번째 단계는 운영관리 단계로서 교육 및 훈련, 테스트, 변경통제, 검토 및 보증 활동으로 구성된다(그림 2 참조).

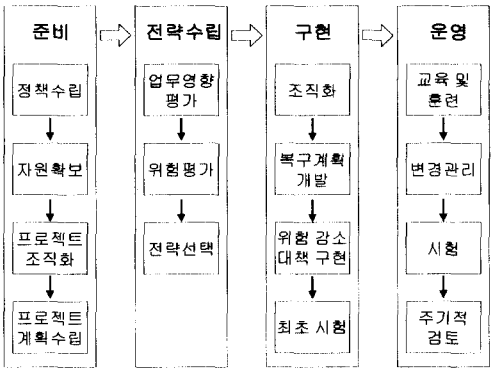



그림 2. CCTA[2]의 업무 지속성 관리 수명주기

이상에서 살펴본 바와 같이 여러 연구에서 다소 상이한 업무 지속성 관리 단계들을 제시하고 있으나, 구체적인 내용면에서는 대체로 유사하다. 본 고에서는 CCTA[2]에서 제시하고 있는 관리 단계를 중심으로 살펴보고자 한다.

## Ⅲ. 업무 지속성 관리 단계

### 1. 개시 단계

업무 지속성 관리를 시작하기 위한 핵심적인 성공요인은 최고 경영층의 의지와 적극적 참여(commitment), 인적 및 재정적 자원의 충분한 배분, 그리고 효과적인 계획 수립 프로젝트 관리 등이다. CCTA의 업무 지속성 관리(BCM) 수명주기의 개시 단계는 다음과 같은 활동들로 구성된다.

#### 1.1 업무 지속성 관리에 관한 정책 수립

업무 지속성 관리는 조직의 성과와 생존에 관한 것이므로, 최고 경영층으로부터 적극적인 지원이 있어야 한다. 경영층은 BCM 정책을 수립하고 문서화하여 조직 내에 배포되어야 한다. BCM 정책은 다른 업무 및 기술 정책과 많은 부분이 중복되므로 적절한 관리와 통제가 필요하다.

#### 1.2 업무 지속성 관리에 관한 내용과 범위 구체화

BCM의 내용은 전략 수립, 구현 및 운영을 포함한 BCM 수명주기 전체를 반영한다. BCM의 범위는 업무과정과 업무과정의 주요 구성요소들(직원, 설비, 전보, 시스템 등) 외부 서비스 공급업자들이 개입되는 정도 그리고 위험의 정도를 고려하여 결정한다.

#### 1.3 업무 지속성 관리에 관한 자원 배분

BCM의 정책을 수립하고 내용과 범위를 정의한 후에, 경영층에서는 적절한 재무 및 인적 자원들을 배분하게 된다. 업무지속성전략이 개발되기 전 까지는 BCM을 위한 전반적인 재정적, 인적 자원의 배분을 명확하게 할 수 없다. 그러나, 경영층의 합의를 토대로 잠재적인 업무영향과 인식된 위험에 상응한 수준까지는 재무 및 인적 배분을 명확하게 해야 한다. 자원배분은 요구사항 분석과 업무지속성전략을 개발하는데 소요되는 비용과 관련되어 있다.

#### 1.4 업무 지속성 관리에 관한 프로젝트 조직과 통제 구조 정의

모든 프로젝트와 같이 BCM 프로젝트는 잘 조직화되고 통제되어야 한다. BCM에 관한 전형적인 프로젝트 조직은 다음과 같다:

- BCM 프로젝트에 관한 전반적인 책임 및 결과물 인수를 담당할 이사급 책임자 임명
- 프로젝트를 지휘하기 위한 운영위원회를 설립해서 결과물에 대한 품질 평가 및 승인
- 프로젝트의 진행 일정을 통제하는 프로젝트 관리자와 많은 프로젝트 활동을 책임지는 프로젝트팀의 임명
- 복구대책의 실행, 시스템과 자료의 복구에 대한 상세한 절차 등과 같은 전문기술이 소요되는 프로젝트 활동을 책임지는 작업반 설립

BCM 프로젝트에 대한 전형적인 통제구조는 다음과 같다:

- 내용과 범위, 복구 활동과 보고서에 관한 용어를 기술한 프로젝트 개시문서와 프로젝트 계획, 품질계획, 위험 등을 조직화하고 통제하는 방법을 만들고 유지관리하여야 한다.
- 프로젝트 및 품질 계획에 대한 진척상황을 주기적으로 조사해야 한다.
- 모든 복구 활동의 결과물(프로젝트 개시문서, 업무영향분석 및 복구요구사항 보고서, 위험평가 보고서, 업무지속성전략 보고서, 업무복구

계획 등)에 대한 공식적인 승인을 통한 품질 검토과정이 정의되어야 한다.
- 이사회에 정기적으로 진척상황에 관한 보고서를 제출해야 한다.

### 1.5 업무 지속성 관리에 관한 프로젝트 계획 및 품질 계획 수립

BCM에 대한 프로젝트 계획의 전형적인 내용은 다음과 같다:
- 착수일자, 종료일자, 자원, 각 단계와 과정에서 할당된 책임, 적절한 장소, 행위 등이 제시되어야 한다.
- 프로젝트 계획의 초안과 최종 복구활동에 대한 일자가 기재되어 있어야 한다.
- 프로젝트 계획간의 중요한 상호의존성이 기술되어 있어야 한다.
- 품질검토 회의일자, 프로젝트 위원회 회의일자, 그리고 경영위원회에 계획 제시일자가 제시되어 있어야 한다.

BCM 품질 계획에는 다음의 사항이 포함되어야 한다:
- 모든 복구활동의 결과물에 대한 설명
- 복구활동 평가를 위한 품질기준
- 각 복구활동 결과물에 대한 품질을 검토하는 책임자

## 2. 전략수립 단계

전략수립단계에서는 업무요구사항과 위험을 평가하고 업무지속성을 관리하는 최적의 접근방법을 결정한다. 조직이 재해를 극복하고 실제로 얼마나 잘 생존할 수 있는지, 그리고 업무 지속성 관리에 소요되는 비용이 얼마인지를 결정하기 때문에, 업무 지속성 관리 수명주기에서 매우 중요한 단계이다. 요구사항을 분석해서 전략을 수립하는 단계는 구체적으로 업무영향분석, 위험평가 및 업무지속성전략이라는 하위 과정으로 구성되어있다.

업무영향분석, 위험분석, 위험평가에 대한 용어에는 차이가 있다. 업무영향분석은 조직 내의 중요한 업무기능을 파악하고, 업무기능의 중지로 인한 영향을 분석하는 것이다. 위험분석(risk analysis)은 조직에 가장 큰 영향을 주는 위협들을 파악하고, 이러한 위협과 관련된 조직의 취약성들을 분석하는 것이다. 위험평가(risk assessment)는 기존의 물적 및 환경적 보안과 통제를 평가하고, 조직에 대한 잠재 위협들의 적정성을 평가하는 것이다[7].

### 2.1 업무영향분석

업무영향분석의 주요 목적은 중요한 업무 프로세스를 파악하고, 중요한 업무 프로세스의 중단으로 인하여 조직에 발생하는 잠재적인 손실을 파악하는 것이다. 업무영향분석 과정은 다음과 같은 활동으로 구성되어있다:
- 업무 프로세스의 식별
- 영향 시나리오(impact scenario)의 정의
- 각 시나리오별 업무에 대한 잠재적인 영향에 대한 측정
- 업무복구 목표의 설정
- 최소 요구사항에 대한 평가

업무 지속성 관리는 중요한 업무 프로세스의 지속성을 유지하는데 초점을 두고 있기 때문에, 업무영향분석의 목적을 위해서 업무 프로세스들을 파악하는 것이 중요한 첫 단계가 된다. 각 업무 프로세스별로 업무영향분석이 수행된다. 업무 프로세스를 파악하기 위해서는 전략 또는 업무계획 문서, 업무처리 재설계(BPR: Business Process Reengineering) 산출물, 조직 정보모델과 같은 자료를 참조할 수 있다.

잠재적 업무영향은 각 업무 프로세스(혹은 업무 프로세스의 그룹)의 영향 시나리오에 대해서 측정된다. 예를 들어, 고객서비스가 x 시간 동안 운영될 수 없는 경우, 또는 송장처리가 y 일 동안 지연되는 경우 등이 예이다. 업무영향분석은 위험비용을 결정하는 방법으로서, 업무 혹은 서비스 중단의 영향을 파악해서 복구계획에 필요한 운영과 과정을 목표로 정하는 것이다.

업무영향 시나리오를 파악한 후에, 업무 프로세스를 책임지는 관리자들과의 인터뷰에 의해서 업무영향을 측정하게 된다. 각 업무 프로세스에 대한 잠재적 업무영향은 각 영향 시나리오와 시간기간 별로 측정된다. 업무영향의 영역에는 재무적(financial or hard) 영역과 비재무적(non-financial or soft) 혹은 운영적 영역이 있다. 재무적 영향은 화폐가치로 측정할 수 있으나, 비재무적 영향은 화폐

가치로 측정할 수가 없다.

업무영향분석에서 잠재적 업무영향에 대한 정성적 측정방법으로는 질문서, 인터뷰, 집단면접 등에 의해서 자료 수집하는 방법이 있고, 정량적 측정방법에는 전통적인 계량적 위험모형(quantitative risk model)과 일반화된 비용결과모형(generalized cost consequence model)이 있다[13].

업무복구의 목표를 설정하기 위해서는 잠재적 업무영향을 측정하고, 각 업무 프로세스의 운영을 위한 최소한의 수준을 기술해야 한다. 업무복구의 목표는 업무를 재개하는데 필요한 최소한의 인력과 설비를 복구시키는데 소요되는 시간과 잔류 인력과 설비에 대한 복구 일정의 관점에서 서술되어야 한다. 복구 목표는 잠재적 업무영향의 측정결과에 기초해서 업무 프로세스를 책임지는 관리자들과의 협의에 의해서 수립되어야 한다.

업무복구의 목표를 정의한 후에, 업무영향분석 과정의 최종단계는 목적에 따라서 충족시켜야 할 인원, 자산 및 서비스에 대한 최소한의 요구사항을 평가하는 것이다. 최소한 요구사항에는 컴퓨터 네트워크, 직원 및 설비, 컴퓨터 시스템과 자료, 음성, 팩스 그리고 기타 통신, 문서 기록, 기타 자산 및 서비스 등이 포함된다.

## 2.2 위험평가

업무영향분석에 의해서 취약성을 평가한 후에, 위협에 관한 구체적인 자료수집이 가능한 경우에는, 위험분석에 의한 위험평가(risk assessment)를 한다. 업무영향분석의 대상은 궁극적으로 업무지속성이며, 업무중단으로 인한 재무적 및 운영적 영향을 파악하는 것이다. 이러한 업무중단의 원인이 되는 위협에 관한 구체적인 추정자료가 있는 경우에는 자산의 식별, 위협 및 취약성 수준의 평가, 그리고 위험수준의 평가를 통하여 위험평가를 수행한다.

위험의 식별을 위해서 자산(asset)을 분류한 후에, 각 자산에 대한 위협(threat)을 파악해야 한다. 자산의 분류란 보호해야 할 전산자원들을 식별하고, 체계적으로 분류하여, 소유하고 있는 자산들의 가치를 평가하는 것이다. 여기서 자산이란 하드웨어, 소프트웨어, 데이터/데이터베이스, 사용자/전산요원, 시스템 관련문서, 전산자료, 저장매체, 통신망 및 관련장비, 등을 말한다. 또한, 위협은 자산에 해를 줄 수 있는 위험의 원천이다. 이와 같은 위협을 식별하고 분류해서, 궁극적으로 발생 빈도와 손실 크기(혹은 강도(severity))를 측정해야 한다.

어떤 재해가 실제로 발생할 가능성은 위협의 수준과 각 위협에 대한 조직의 취약성(vulnerability)의 정도와 함수관계가 있다. 여기서 취약성이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이와 같은 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 분석하는 목적이다. 취약성에는 경영적 혹은 관리적 취약성(보안관리, 인원관리, 절차상관리, 사고대책관리, 등에 대한 취약성), 논리적 혹은 기술적 취약성(하드웨어, 응용소프트웨어, 운영체계, 데이터베이스, 네트워크, 등에 대한 취약성), 물리적 취약성(출입통제, 환경관리, 등에 대한 취약성)이 있다.

위험수준의 평가를 위해서는 위험을 측정해야 한다. 위험측정은 자산에 대한 손실을 분석하는 과정으로서, 선택된 적절한 위험분석방법에 의해서 위협의 발생확률과 손실크기를 곱해서 기대손실을 가능하면 계량적으로 계산한다. 손실크기를 화폐가치로 계산할 수 없으면, 정성적인 위험분석법을 이용한다. 이와 같은 위험분석을 위해서 체크리스트 혹은 CRAMM(CCTA Risk Analysis and Management Method)[12], BDSS(Bayesian Decision Support System)[14] 등과 같은 위험분석 소프트웨어를 활용할 수 있다.

## 2.3 업무 지속성 전략

업무 지속성 전략의 수립 과정은 먼저 재해복구대책 옵션을 파악하고 평가하며, 두 번째 위험감소대책 옵션을 파악하고 평가하며, 마지막으로 전반적인 업무지속성전략 수립한다. 재해복구대책은 여러 옵션들이 있을 수 있는데 대표적인 옵션으로는 상호협약(reciprocal arrangement), 핫사이트(hot-site), 콜드사이트(cold-site) 등이 있다. 조직의 요구사항과 재정적, 시간적 제약조건을 고려하여 이들 옵션 중에서 선택해야 할 것이다.

효과적인 업무 지속성 관리를 통하여 위험감소를 위한 통제수단과 재해복구 대책간의 적절한 균형이 필요하다. 위험감소를 위한 통제수단으로는 시설물에 대한 출입통제, 화재, 홍수, 폭발물로부터의 보호, 전원, 전화회선의 보호, 바이러스 보호 등이 포함된다.

## 3. 구현 단계

구현 단계는 재해복구 대책 및 위험감소 조치의 구현과 이를 위한 계획과 절차의 개발을 포함한다. 이 단계는 다음의 세부 활동들로 구성된다.

### 3.1 조직화 및 구현 계획

효과적인 업무지속성전략의 구현을 위해서는 재해복구 책임을 가진 사람들에 의해 실시되어야 한다. 따라서 구현 단계에서 첫 번째 활동에는 C3 (command, control and communication) 구조 확립, 업무복구 계획을 위한 프레임워크 개발, 그리고 구현 계획의 개발이 포함된다.

최고 경영층/중역으로 구성된 위원회, 중앙 통제팀, 업무복구 팀이 주축이 되고 기타 관련되어 있는 자를 포함하는 지휘체계가 명확하게 규정되어야 한다. 업무복구계획을 위한 프레임워크는 전형적으로 긴급조치, 위기 관리, 피해 평가, 구제, 복구대책의 실행 여부 결정, 복구대책의 실행, 업무프로세스의 복구, 그리고 평상시로의 복구 등과 같은 활동을 의미한다. 또한 업무복구계획은 전형적으로 역할과 책임, 행동 리스트 그리고 참고 자료를 포함한다.

재해의 징후를 포착하여 긴급조치를 시작으로 평상시로의 최종 복구까지 전형적으로 실행되는 복구 활동은 아래와 같이 세 가지 단계로 요약될 수 있다.

- 경보 단계로서 사건이 보고되고, 초기 피해의 평가가 이루어지고 재해복구대책의 실행 여부를 결정할 때까지의 시간
- 복구 단계로서 재해복구대책이 실행되고 업무프로세스가 복구될 때까지의 시간
- 정상화 단계로서 평상시로의 복귀가 계획되고 설비와 자산이 원상 복귀되거나, 고쳐지거나, 교체되고 운영될 때까지의 시간

### 3.2 재해복구 대책 및 위험감소 대책의 구현

업무지속성 전략을 통하여 업무 처리 과정에서 반드시 필요한 공간, 시스템, 통신 등을 예비 확보해야 한다. 이를 위해서는 다음과 같은 사항에 대한 준비가 필요하다:

- 비상 통제 센터를 준비하고 가구, 전원, 전화 및 데이터 회선이 갖추어진 공간 준비
- 컴퓨터 시스템과 네트워크 접속 장비를 구입 혹은 설치
- 컴퓨터 시스템을 재배치하거나 컴퓨터통신 및 전화 네트워크를 재구성
- 비상용 컴퓨터 시스템에 의한 처리가 가능하도록 소프트웨어를 수정
- 자료 백업을 위한 정책과 절차를 개선
- 비상용 전화 교환기 설치
- 중요한 영역을 위해 백업 전원 공급
- 업무 지속성 관리와 관련된 외부 서비스 공급자를 결정
- 상업적인 복구 서비스 공급자를 선택하고 계약 협상

재해복구 대책을 운영, 테스트, 유지하기 위해 그리고 재해복구 대책이 필요할 경우 언제든지 작동할 수 있다는 것을 보장하기 위해 훈련과 새로운 절차가 요구될 것이다.

### 3.3 업무복구 계획 개발

업무복구 계획은 일반적으로 다음과 같이 3가지 수준의 계획으로 구성된다:

- 마스터 플랜과 긴급조치, 위기 관리, 공보 관계, 피해 평가, 구제 그리고 중요서류 등에 관한 계획
- 공간 및 시설, 서비스, 컴퓨터 시스템, 네트워크, 전화, 구성원, 재정부서, 관리부서 같은 핵심 지원 기능을 위한 계획
- 중요한 비즈니스 프로세스나 기능을 위한 계획

마스터플랜은 중앙 통제 팀의 취해야할 행동의 지침이 되는 자료로 재해사건의 통보, 초기 피해 평가 접수, 위기 관리와 구제 활동의 시작, 재해복구대책의 가동 여부 결정, 직원, 공급자, 제3자 간의 통신 채널 가동, 복구단계와 정상화 단계에서의 전반적인 협력 및 조화에 관한 내용을 포함하고 있다.

긴급조치 절차는 직원들이 준수해야 하는 사항으로 경보신호와 그것의 의미, 대피 절차, 건물로부터 대피후 집합 장소, 의심스러운 사건, 화재, 또는 다른 사고를 발견했을 경우의 행동요령, 중앙 통제 팀이나 업무복구 팀이 즉각적으로 수행해야할 행동 지침 등의 내용을 포함하고 있다. 피해 평가 계획은 전형적으로 다음과 같은 자산에 대한 피해를 계산한다: 건물 구조, 수도 공급, 전기 공급, 화재 경보와

같은 건물 서비스, 컴퓨터 시스템과 네트워크, 통신 서비스와 통신 기구, 사무 기구 및 다른 자산, 서류, 피해평가에 관련된 모든 정보를 수집하기 위해 사전에 준비된 피해평가 양식을 사용해야 한다.

재해가 모든 자산에 돌이킬 수 없는 피해를 주는 경우는 드물다. 대부분의 경우에는 신속한 구제활동을 취함으로써 일부 자산을 보호할 수 있고 피해가 악화되는 것을 방지할 수 있다. 구제활동은 전문 지식을 요구하며, 연기와 오염된 물뿐만 아니라 불연성 물질과 화약약품 같은 위험한 물질을 처리하는 정화활동, 먼지, 파편, 유리 조각 등의 제거, 공기 정화, 습기제거, 손상된 저자 매체로부터의 데이터 복구, 손상된 서류 기록의 복구 등의 활동을 포함한다.

### 3.4 절차 개발과 초기 테스트

업무복구 계획 내의 작업목록은 특정 작업을 지원하는데 필요한 세부 절차와 구별되어야만 한다. 즉, 절차는 일반적으로 세부적인 속성을 가지고 있고 특정 복구 작업의 지원에서 필요한 모든 단계를 나타낸다. 예를 들면, 주문의 기록과 신용 체크 그리고 송장 배포를 위한 수작업 절차, 대체 하드웨어와 네트워크의 설치 및 테스트, 백업 데이터와 소프트웨어의 재복구 절차 등이 있다.

테스트는 총체적인 업무 지속성 관리 프로세스의 중요한 부분이며, 선택한 전략, 재해복구대책, 업무복구 계획 및 절차가 실제 상황에서 유용하다는 것을 보장하는 유일한 방법이다. 초기 테스트는 업무 지속성 전략이 효과적으로 구현되었다는 것을 체크하기 위해서 그리고 이전 계획의 필요한 수정을 허용하기 위해서 구현 단계의 부분으로서 수행된다. 초기 테스트 프로세스는 테스트 목표 결정, 테스트 유형 결정, 테스트 시나리오 생성, 테스트 계획 개발, 테스트 실행, 그리고 테스트 결과의 문서화와 발간 등의 활동으로 구성된다.

테스트 유형에는 구조적 검토회(walkthroughs), 기술적 구성요소 테스트, 비즈니스 구성요소 테스트, 전체 테스트가 있다. 테스트 계획 준비를 위해 고려할 사항은 테스트 팀의 확인, 테스트 시간, 테스트를 위해 이용될 수 있는 자원(공간, 사무 기구, 컴퓨터 시스템과 네트워크 그리고 통신 설비), 예산 등이다.

## 4. 운영관리 단계

운영 관리 단계는 테스트, 교육과 훈련, 변화 관리, 보증과 같은 하위 과정을 포함한다. 업무 지속성 계획은 계획의 수립 그 자체만으로 의의를 가질 수 없으며 계획의 유효성에 대한 끊임없는 검증이 요구된다. 업무 지속성 계획의 효과성에 대한 실제적인 검증은 실제로 비상사태가 발생하였을 때 이루어질 수 있을 것이나, 비상사태가 실제로 발생할 때까지 기다린다는 것은 너무 위험부담이 크다. 따라서 비상사태가 실제로 발생하기 전에 계획의 유효성을 검증하는 작업이 필요하다. 업무 지속성 계획을 수립할 때는 비상사태가 발생하였을 때 일어날 수 있는 여러 가지 상황을 가정하게 되는데 이러한 가정사항이 얼마나 현실적이냐에 따라서 업무 지속성 계획의 적합성이 결정된다. 가정사항의 현실성 여부는 비상사태가 현실적으로 발생하기 전에 밝혀져야 하는데 이는 결국 테스트를 통하여 알 수밖에 없다.

테스트는 비상사태가 발생하였을 때 데이터 처리 활동의 전반적 능력을 평가하는데 그 목적이 있다. 또한, 테스트를 통하여 이미 수립된 업무 지속성 계획의 미비점을 식별할 수 있을 뿐만 아니라 업무 지속성 계획에 대한 조직 구성원들의 인식을 고취하는 데에도 유용하다. 사용자의 적극적인 참여를 전제로 하는 테스트는 실제로 비상사태가 발생할 경우 사용자에게 비상사태의 대처에 대한 자신감을 주는 심리적인 효과도 크다. 재해가 실제로 발생하였을 때 필요한 핵심기술을 식별하고 이를 습득하기 위한 훈련은 테스트 과정에서 아주 중요한 부분을 차지하며, 업무 지속성 계획의 성공과 실패를 가늠하는 중요한 요인이 된다[6]. 한정된 자원으로 업무 지속성 계획을 수립할 때는 계획 자체가 시스템 복구에 필요한 가장 기본적인 요소를 제공하는지를 테스트하는데 중점을 두어야 한다. 예정된 데로 테스트가 진행되면서 계획 자체의 오류가 식별되어 사후에 계획이 보완될 수 있다면 테스트 자체는 매우 성공적이라고 볼 수 있다.

업무 지속성 계획의 테스트는 정보시스템 이외의 다른 업무 분야에도 중요한 효과를 가져다준다. 테스트에서 중요한 응용체계의 한 부분을 실행하는 것을 요구할 때, 이의 부산물로서 응용체계의 흐름을 확인하고 재수행할 수 있는 능력을 검증할 수 있게 된다.

테스트를 수행함으로써 종종 정상적인 업무수행 과정상에서 발생하는 운영상의 미묘한 문제가 부각되는 경우가 있다.

테스트를 실시함으로써 관리자에게 업무 지속성 계획의 수립 및 유지에 필요한 예산을 정당화하는 가시적인 결과를 제공한다. 업무 지속성 계획의 수립은 종종 생명보험에 드는 것에 비유된다. 테스트를 수행함으로써 계획에 대한 관점이 추상적인 비용회피적인 것에서 실존하는 것으로 바뀌게 된다. 업무 지속성 계획의 테스트가 수행될 때 관리자는 보통 관심을 가지게 되고, 테스트의 변수(parameter)를 설정하는데 적극적인 역할을 수행하며 테스트에 참여하기도 한다. 업무 지속성 계획이 업무의 정상적인 복구를 목적으로 하는 것이라는 점을 신뢰한다면 대부분의 고위 관리자는 계획이 실제로 목적을 달성할 수 있는지를 확인하는데 직접적인 관심을 가지게 된다.

업무지속성 정책과 전략, 계획에 대한 교육과 훈련은 업무 지속성 관리의 지속적인 수행에서의 성공여부를 결정하는 중요 요인이다.

교육과 훈련을 통해 업무 지속성 관리가 비즈니스에서 일상적인 활동으로 인식하게 하는 것이다. 테스트는 교육 및 훈련을 위한 효과적인 방법이 되지만 지속적인 교육을 통해 재해로 인한 위험을 인식하고 업무 지속성 계획이나 전략의 변화를 숙지하며 조직 구성원이 각자의 책임과 역할을 충분히 인식해야 한다.

시간이 경과함에 따라 업무 지속성 계획이나 전략도 변경될 필요가 있다. 변경은 크게 유지보수를 위한 변경과 새로운 업무나 시스템의 추가, 자산의 획득이나 폐기 등으로 인한 변경이라는 두 범주로 구분할 수 있다. 변경관리 과정은 변경전략 결정, 변화를 위한 필요성 파악, 변화 실행, 계획과 절차의 변경 등의 활동으로 구성된다.

업무 지속성 관리 수명주기의 마지막 과정은 보증과정으로 업무 지속성 관리의 결과에 대한 품질에 대한 보증과 운영관리 과정이 만족스럽게 작용하고 있는지 여부에 대한 보증의 획득을 포함한다. 경영층은 업무 지속성 관리의 결과물에 대한 평가를 실시하고 이를 문서화한다. 평가는 업무 지속성 관리의 첫 번째 단계인 개시단계에서 명시한 품질계획에 근거하여 실시하고 결과가 성공적으로 평가될 경우, 차기 검토일자를 포함한 경영층이 승인을 표시하는 인증서를 발급할 수 있다.

## Ⅳ. 결 론

업무 지속성 관리는 조직의 생존을 위협하는 재해에 대응하기 위한 필요 불가결한 활동이다. 특히 정보시스템을 근간으로 경영 활동이 수행되고 있는 오늘날에는 그 중요성이 한층 더 부각되고 있다.

업무 지속성 관리 수명주기의 성숙과정은 다음과 같은 중요한 이정표에 의해 확인될 수 있다:

- 영향 분석과 위험 평가의 완전성
- 업무지속성 전략의 정의와 합의
- 재해복구 대책과 위험감소 대책 구현 그리고 업무복구계획의 개발
- 지원 절차의 개발과 구현
- 재해복구대책과 위험감소대책 그리고 업무복구계획의 성공적인 초기 테스트
- 모든 업무 지속성 관리 결과물에 대한 테스트, 재검토, 유지보수와 감사를 위한 관리 프로세스의 개발

한 이정표에서 다른 이정표로의 이동을 위해서는 조직 내부에서의 새로운 투자와 의지가 필요하며 마지막 이정표를 달성하였을 때 비로소 업무 지속성 관리가 조직 내부의 내재적/일상적인 활동으로서 인식될 수 있으며 갑작스런 재해에도 효과적으로 대응할 수 있다.

이상과 같이 4단계로 구분된 업무 지속성 관리의 체계는 재해로 인한 업무서비스의 지속적인 제공을 위해 반드시 수행해야 할 과정과 활동을 체계적으로 제시하는 프레임워크이다. 이를 기초로 보다 구체적이며 현실에 적용 가능한 업무 지속성 계획 개발방법론이 필요하다. 특히 두 번째 단계인 전략수립 단계는 매우 중요한 과정으로서 업무영향평가, 위험평가 등의 하위 과정으로 구성되며 비용 효과적인 재해복구를 위한 업무 지속성 계획을 수립하는데 주요 방향제시를 가능하게 한다. 기존의 문헌에는 이에 대한 여러 평가 방법론이 존재하나 논리적으로 완전하지 못하며 국내 실정에 적합하지 않은 모델을 사용하는 경우도 많다. 따라서 업무영향평가나 위험평가에 대한 보다 구체적이며 국내 현실에 적합한 방법 개발이 요구된다.

## 참 고 문 헌

[1] Butler, J. *Contingency Planning and*

*Disaster Recovery Strategies*, Computer Technology Research Corp., 1994.

[2] CCTA, *An Introduction to Business Continuity Management*, The Government Centre for Information Systems, 1995.

[3] "미 국방부 올해 7월까지 14,000회 해킹 공격당함," *정보보호뉴스*, 한국정보보호센터, p.3, 2001. 1.

[4] *NIST Handbook*, National Institute of Standards and Technology, 1994.

[5] J. Owen, "Network Disaster Recovery," *Datapro*, IS38-400, 1995, pp.401-410.

[6] K.L. Fulmer, *Business Continuity Planning: A Step-by-Step Guide*, Disater Recovery Institute, 1996.

[7] ISO/IEC JTC1/SC27 N1845, *Guidelines for the Management of IT System Security(GMITS): Part3 - Techniques for the Management of IT Security*, ISO, Dec. 1997.

[8] Carl B. Jackson, "Business Continuity Planning: The Need and the Approach," *Datapro Reports on Information Security*, February 1994, pp.101-109.

[9] Michael Miora, "Protecting the Enterprise: Seven Steps to Safety," *Carolina Computer News*, April 1997.

[10] Pat Moore, "How to Plan for Enterprise-Wide Business and Service Continuity," *Strohl Systems*, 1997.

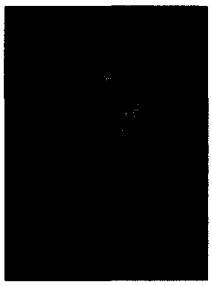
[11] Robin Moses, "Risk Analysis and Management," *Computer Security Reference Book* edited by K.M. Jackson, J. Hruska, & Donn Parker, CRC Press, Inc., 1992, pp.227-263.

[12] _____ , "CCTA Risk Analysis and Management Methodology(CRAMM)," *Datapro Reports on Information Security*, December 1992, pp.101-110.

[13] Ozier, Will., "Issues in Quantitative Versus Qualitative Risk Analysis," *Datapro Reports on Information Security*, March 1992, pp.101-107.

[14] Rex K. Rainer, C. Snyder and Houston Carr, "Risk Analysis for Information Technology," *Journal of Management Information Systems*, 1991, Vol.8, No.1, pp.129-147.

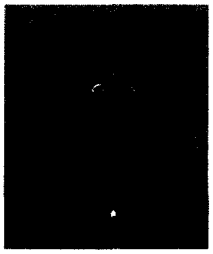
## 〈著者紹介〉



**김 종 기 (Jongki Kim)**
1987년 : 부산대학교 경영학과 학사
1988년 : Arkansas State University, MBA
1992년 : Mississippi State University, Ph.D. in MIS
1993년 3월~1998년 12월 : 국방정보체계연구소 선임연구원
1999년 3월~현재 : 부산대학교 경영학부 조교수
관심분야 : 정보시스템 보안관리, 전자상거래, 프로젝트 관리

**김 기 윤 (Kiyoon Kim)**
1976년 : 고려대학교 공학사
1979년 : 고려대학교 경영학 석사
1985년 : 고려대학교 경영학 박사
1980년~현재 : 광운대학교 경영학과 교수
관심분야 : 위험관리, 보안관리, 성과관리

**이 경 석 (Kyung-Seok Lee)**
1978년 : 숭실대학교 전산학 학사
1981년 : 성균관대학교 전산학 석사
1986년 : 프랑스 파리 7대학교 박사 (암호이론 전공)
1983년 10월~1986년 12월 : ITODYS(Paris 7대학 연구소) 연구원
1978년 3월~현재 : 산업연구원 전산정보실장
관심분야 : 정보보호관리, 시스템 감사, 전자상거래, 정보시스템의 전략적 응용



**김 정 덕 (Jungduk Kim)**
1979년 : 연세대학교 정치외교학과 학사
1981년 : 연세대학교 경제학과 대학원 석사
1986년 : University of S. Carolina MBA
1990년 : Texas A&M University, Ph.D. in MIS
1991년~1993년 : 한국전산원 선임연구원
1993년~1995년 : 원광대학교 조교수
1995년~현재 : 중앙대학교 교수
관심분야 : 정보보호관리, 시스템 감사, 전자상거래, 정보시스템의 전략적 응용