정보시스템 환경별 업무지속성관리 적용 연구

신순자[0*],이병만[*],선우종성[*],김정덕[**],김기윤[***],김종기[****]
한국전산원[*],중앙대학교[**],광운대학교[***],국방연구원[****]

Business Continuity Management Application for Each Information Systems Environment

Shin, Soonja[0*], Lee, Byungman[*], Sunwoo, Jongsung[*]
Kim, Jungduk[**],Kim, Keeyun[***], Kim, Jonggi[****]
NCA[*], ChungAng Univ.[**], KwangWoon Univ.[***], IDIS[****]

요약

1980년대 후반과 90년대 초반부터 정보시스템의 비상계획과 재해복구의 새로운 개념으로 대두된 업무지속성관리(BCM:Business Continuity Management)는 정보시스템이 조직의 업무처리(Business Process)에 중심을 두고 활용되는 현실에서 업무의 중단없는 지속적인 업무수행이 조직의 중요 이슈로 대두되는 추세를 반영하여, 비상시 또는 재해시 복구의 대상을 단순한 전산센터나 시스템 단위에 초점을 맞추는 것이 아니라, 가장 중요한 업무처리 차원에서 중단없이 업무를 수행할 수 있도록 관리하는 것을 말한다.

본 연구에서는 이러한 업무지속성관리가 기존의 재해복구나 보안관리 등의 개념들과 어떠한 관계를 갖고 있는지를 정의함으로서, 업무지속성관리의 개념과 범위를 좀 더 명확히하고, 정보시스템의 운영환경별(중앙집중처리, 분산처리, 외부위탁처리) 업무지속성관리를 적용하는 방안에 대해 살펴보고자 한다.

1. 서론

급격한 업무 환경의 변화와 경쟁 상황에서 어떠한 경우에도 중단 없이 지속적인 업무를 수행할 수 있어야 함은 조직의 생존을 위해 매우 중요한 명제가 되고 있다. 특히 업무의 정보화가 가속화됨에 따라 정보서비스 중단에 의한 업무상의 손실은 과거와는 달리 막대한 금전적 손실을 초래하고 있다. 따라서 정보서비스의 지속적 제공이 중요한 문제로 대두되고 있어 재해에 대한 비상계획 및 재해복구계획의 중요성이 점증되고 있다.

1990년대에 들어 분산시스템, 최종사용자 전산화, 네트워크화의 급진전, 인터넷과 인트라넷의 급속한 보급 등은 비상계획을 수립하는데 있어 보다 다양한 기술적 요소를 고려하게 하였고, 더욱이 정보시스템에 대한 조직의 의존도는 더욱 더 심화되어 정보시스템과 조직의 업무 프로세스의 분리가 무의미하게 되었다. 따라서, 비상계획의 수립에 있어 업무처리와 사용자 측면을 강조하게 되었으며, 재해복구는 단순한 기술적인 문제가 아닌 관리의 문제(business issue)로 등장하게 되었다. 이와 같이 복구계획이 전산센터의 복구뿐만 아니라 고객 서비스에 초점을 둔 업무의 지속에 비중을 두면서 "업무지속성관리(business continuity management) "라는 개념이 출현하게 되었다. 업무지속성관리는 업무지속성계획을 개발 및 유지보수를 위한 일련의 관리 과정(management processes)으로 보고, 조직이 재해로 인한 위험에도 불구하고 조직의 업무를 사전에 결정된 최소한의 수준으로 영위하기 위한 일련의 통제 행위라고 정의할 수 있다. 이러한 업무지속성관리를 위해서는 팀 구성, 조직의 중요 업무 프로세스의 파악, 재해 위협에 대한 업무영향평가, 위험분석 등 복잡한 과정 및 행위가 요구된다.

본 연구에서는 이러한 업무지속성관리가 기존의 재해복구나 보안관리 등의 개념들과 어떠한 관계를 갖고 있는지를 정의함으로서, 업무지속성관리의 개념과 범위를 좀 더 명확히하고, 정보시스템의 운영환경별(중앙집중처리, 분산처리, 외부위탁처리) 업무지속성관리를 적용하는 방안에 대해 살펴보고자 한다.

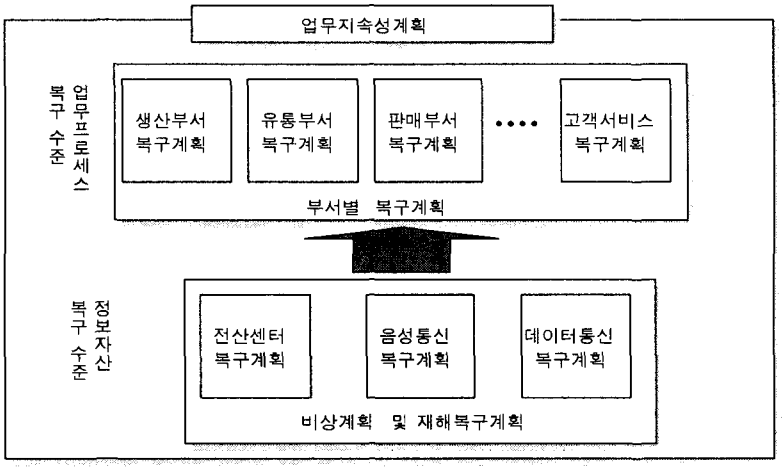
2. 업무지속성관리 범위

(1) 업무전략/기술전략과의 관계

업무전략은 조직이 목표로 하는 사업 대상 및 방향 등을 정의하며 이를 위한 주요 성공요인을 제시하고, 기술전략은 이러한 사업을 지원하기 위한 기술의 도입, 개발, 관리 등을 위한 전략으로 기존의 사업전략과 연계되어 적절한 지원 역할을 수행한다. 이들 전략은 업무지속성관리 수행시 조직이 추구하는 주요 목표와 성공요인을 분명하게 해주며 핵심 업무 프로세스와 기능, 기술적 인프라에 대한 정보를 제공한다.

(2) 비상계획/재해복구와의 관계

비상계획 및 재해복구계획은 대부분의 업무가 정보기술 분야별로 이루어지는 활동들로서 업무지속성관리의 인프라적인 역할은 한다고 볼 수 있다. 업무지속성관리에서 다루는 범위는 (그림 1-1)에서와 같이 기존의 재해복구계획보다 정보기술을 포함한 전반적이고 포괄적인 비즈니스 이슈를 다루고 있다.



(그림 1-1)

(3) 보안관리와의 관계

일반적으로 보안관리는 일상적인 상황에서의 위험에 대처하여 정보서비스의 비밀성, 무결성, 가용성을 위한 관리 활동이라고 보면 업무지속성관리는 재해 상황이라는 극한 상황에 초점을 맞추어 정보서비스의 가용성을 보장하기 위한 관리

활동이라고 구별할 수 있다.

(4) 업무지속성관리 범위 결정요인

개략적인 수준에서 업무지속성관리의 범위는 대상 업무 프로세스와 주요 구성요소(정보, 시스템, 직원), 해당 위험과 같은 사항에 의해 결정되어 진다. 초기에는 경영층의 관점에서 핵심 업무 프로세스와 가장 큰 위험에 초점을 맞추고 일단 이러한 분석이 완료되면 핵심 프로세스 중에서 가장 취약한 부분에 집중함으로써 범위를 축소시킬 수 있다.

3. 업무지속성관리 단계

업무지속성관리는 단계적 접근방법을 채택하고 있으며 다음과 같은 프로세스로 구성되어 있다.[3]

단계1 : 개시단계 - 업무지속성관리에 관한 정책을 수립하는 단계로 조직의 업무와 기술관련 정책과의 통합을 보장하며 업무지속성관리에 관한 제반 사항을 준비하는 프로세스이다.

단계2 : 전략수립단계 - 재해가 업무에 미치는 잠재적인 영향 및 위험을 평가하고 위험감소 및 업무 프로세스 복구를 위한 여러 옵션을 파악한 후 평가하여 업무지속성관리를 위한 비용효과적인 전략을 수립하는 프로세스이다. 이 단계는 다음과 같은 프로세스로 구성되어 있다.

- 업무영향분석(Business Impact Analysis)
- 위험평가
- 업무연속성전략 수립

단계3 : 구현단계 - 업무가 지속적으로 운영되기 위한 프로그램을 수립하는 단계로 업무지속성전략에서 수립한 위험감소조치 및 재해복구를 위한 설비를 구현하며 필요한 업무복구를 위한 계획 및 절차를 작성하고 초기 시험을 수행하는 프로세스로 구성되어 있다. 구체적인 프로세스는 다음과 같다.

- 조직화 및 구현계획 개발

- 복구대책의 실행
- 업무복구계획의 개발
- 위험감소대책의 실행
- 절차 개발
- 초기 시험

단계4 : 운영관리단계 - 업무지속성전략, 계획 및 절차를 계속적으로 시험, 검토 및 유지보수하며 적절한 교육 및 훈련 프로그램을 운영하는 프로세스로 구성되어 있다. 구체적인 프로세스는 다음과 같다.

- 교육
- 훈련
- 시험
- 변경통제
- 보증

위의 업무지속성관리 4단계의 세부 절차를 다음과 같이 10개의 프로세스로 정리할 수 있다.

(1) 업무영향분석

업무영향분석(BIA)의 주요 목적은 첫째, 중요한 업무 프로세스를 파악하고 둘째, 중요한 업무 프로세스의 정지로 인해서 조직에 발생되는 잠재적인 손해 혹은 손실을 파악하는 것이다. 업무영향분석에서는 다음과 같은 사항을 파악한다:

- 수입 상실, 추가적 비용부담, 신용 상실 등과 같은 형태의 손실
- 사건 발생 이후 시간이 경과함에 따라 손해 혹은 손실이 점증되는 정도
- 업무 프로세스가 최소한의 수준으로 계속 운영되는데 필요한 최소한의 직원, 시설, 서비스
- 최소한의 운영에 필요한 직원, 시설, 서비스를 복구하는데 소요되는 시간
- 전체 업무 프로세스를 운영하는데 필요한 직원, 시설, 서비스를 충분히 복구하는데 소요되는 시간

업무영향분석(BIA) 프로세스는 다음과 같은 활동으로 구성되어 있다.

- 업무 프로세스의 식별

- 영향 시나리오(impact scenario)의 정의
- 잠재적 업무영향(potential business impact)에 대한 측정
- 업무복구 목표의 정의
- 최소한의 요구사항에 대한 평가

(2) 위험평가

업무영향분석에 의해서 취약성을 평가한 후에, 업무중단의 원인이 되는 위협에 관한 구체적인 자료수집이 가능한 경우에는, 위험분석에 의한 위험평가(risk assessment)를 한다. 위험평가 프로세스는 다음과 같은 활동으로 구성되어 있다:

- 위험의 식별
- 위협 및 취약성 수준의 평가
- 위험수준의 평가

(3) 위험감소대책

위험평가에 의해서 파악된 위협과 취약성을 평가해서 적절한 대책을 마련해야 한다. 효과적인 업무지속성관리를 위해서는 사전에 위험을 감소시킬수 있는 다음과 같은 대책을 고려해야 한다.

- 단일 사고 때문에 장애를 받는 업무 기능/프로세스를 정상화시키는 대안을 고려해야 한다.
- 외부서비스 공급업자에게 위탁하는 업무량의 한도를 고려해야 한다.
- 정보기술시스템과 네트워크 내에 고장 허용한도를 설정해야 한다.
- 허가받지 않은 접근 혹은 의도적인 물적 공격을 탐지하는 접근통제 혹은 CCTV와 같은 추가적인 보안을 실행해야 한다.
- 심각한 손해가 발생하기 전에 화재 혹은 홍수와 같은 사고를 탐지하는 추가전인 통제대안이 마련되어야 한다.
- 프로젝트관리, 구조화된 시스템설계, 형상관리, 변경통제, 사고보고 등과 같은 사고 발생 가능성을 감소시키는 절차를 개선해야 한다.

(4) 복구대책

복구대책들은 항상 중요한 업무 프로세스를 지원할 수 있어야 하며, 다음과 같은 요소에 대한 복구대책을 고려해야 한다:

- 사람과 설비
- 정보기술시스템, 네트워크와 자료
- 전력, 통신, 우편 등과 같은 중요한 서비스
- 서류기록, 관련자료와 같은 중요한 자산

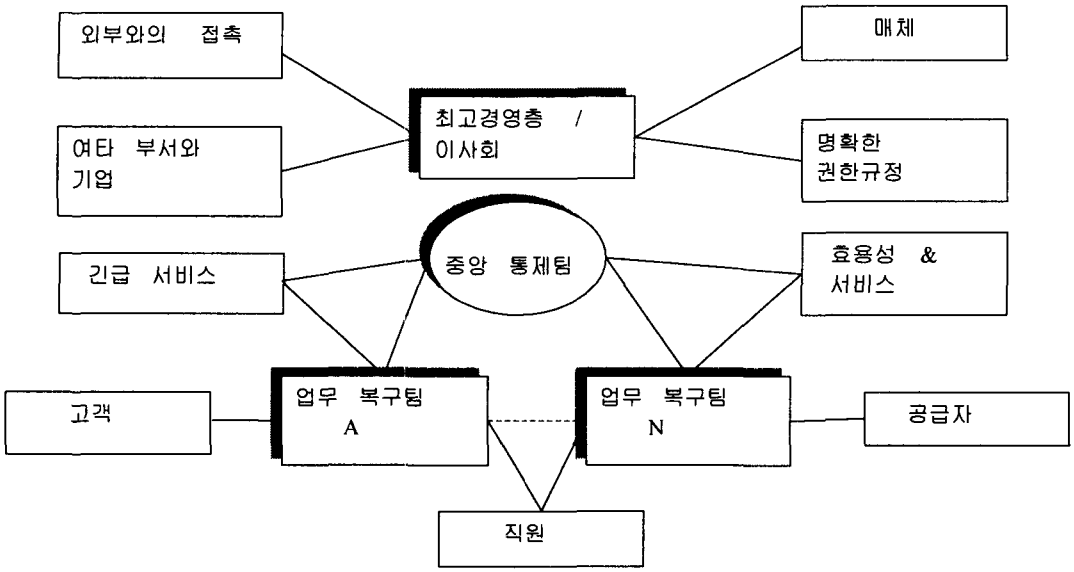
(5) 대안평가

복구대책을 마련하고, 이의 효율성을 파악하기 위해서는 다음과 같은 요소에 대해 평가를 해야 한다.

- 보안대책 구현의 결과로 인한 잠재적 영향의 축소
- 보안대책의 구축, 유지관리, 시험에 소요되는 비용, 예로서 인적자원, 자본비용, 계약료, 훈련비, 자문비 등
- 사고 혹은 재해 시에 보안대책을 선택하는데 소요되는 비용, 예로서, 임시직원고용비, 상업적 복구서비스 비용으로서, 보험이 가능한 경우도 있다.
- 실제 발생할 사고 혹은 재해의 가능성

(6) 명령, 지휘, 의사소통 구조

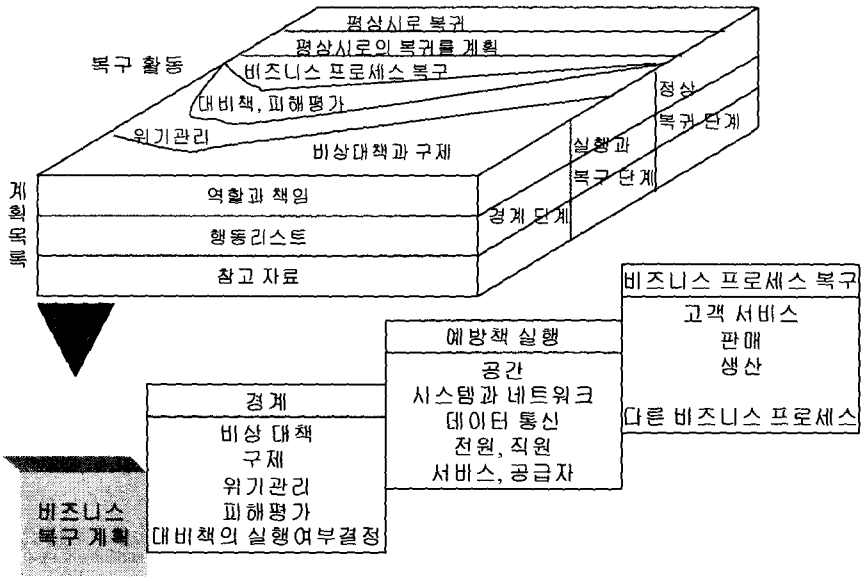
지휘, 통제, 의사 소통 구조는 재해 발생시 즉각적인 업무 복구 활동을 관리하기 위해 명확하게 규정될 필요가 있다. (그림 3-1)[3]은 최고 경영층/이사회, 중앙통제 팀, 업무복구 팀이 주축이 되고 기타 관련되어 있는 조직이나 인원을 포함하는 지휘, 통제, 의사 소통 구조의 예를 보여주고 있다.



(그림 3-1) 지휘, 통제, 의사소통 구조 구축의 예

(7) 업무복구계획을 위한 프레임워크

업무복구계획을 위한 프레임워크는 전형적으로 긴급조치, 위기 관리, 피해 평가, 구제, 복구대책의 실행 여부 결정, 복구대책의 실행, 업무프로세스의 복구, 그리고 평상시로의 복구 등과 같은 활동을 포함하며, 각각의 역할과 책임, 행동 리스트 그리고 참고 자료 등을 명시하여야 한다



(그림 3-2) 업무복구계획의 전형적인 구조와 내용

(그림 3-2)[5]는 긴급조치를 시작으로 최후의 평상시로 복구까지의 전형적인 복구활동을 나타낸다. 그러한 활동은 다음과 같은 세 가지 단계로 요약될 수 있다.

- 1단계: 경보단계로서 사건이 보고되고, 초기 피해의 평가가 이루어지고 재해복구대책의 실행 여부를 결정할 때까지의 시간
- 2단계: 복구단계로서 재해복구대책이 실행되고 업무프로세스가 복구될 때까지의 시간
- 3단계: 정상화 단계로서 평상시로의 복귀가 계획되고 설비와 자산이 원상 복귀 또는 수리되거나 교체되어 정상 운영될 때까지의 시간

(8) 비상대책 및 위험감소 대책의 구현

비상대책 및 위험감소 대책의 구현은 다음과 같은 활동을 포함한다:

- 비상통제 센터를 준비하고 가구, 전원, 전화, 데이터 회선이 갖추어진 공간 준비

- 컴퓨터 시스템과 네트워크 접속점을 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
- 업무지속성관리 상의 외부 서비스 제공자를 결정하고 가능하면 그들을 감사
- 상업적인 복구 서비스 제공자를 선택하고 계약 협상

(9) 업무복구계획 개발

전형적인 업무복구계획의 구성은 다음과 같다;

- 서론 부문: 계획의 목적과 범위, 복구 단계, 계획의 구조, 다른 계획과의 관계 등 개략적인 윤곽 서술
- 복구팀의 구조와 작업 리스트 부문: 특정 계획을 사용할 팀 구조와 팀이나 팀 구성원 각각의 역할을 위한 작업 리스트의 집합
- 참고자료 부문: 팀 구성원이 그들에게 부여된 작업을 수행하기 위해서 필요한 참고 정보

(10) 운영관리

지속적으로 변화하는 조직의 효과적인 업무지속성관리를 위해서는 운영관리가 매우 중요하다. 운영관리 단계에서는 다음과 같은 프로세스가 포함된다:

- 시험
- 교육과 경각심 제고
- 훈련
- 변경 관리
- 보증

4. 시스템 환경별 업무지속성관리의 적용

시스템 환경을 3가지로 분류하고 환경별 특성에 관한 이슈에 대해 고려해 보고자

한다. 일반적인 시스템 환경을 다음과 같은 3가지 형태로 구분할 수 있다.

- 중앙집중처리 환경 : 업무 프로세스가 중앙집중적으로 처리되고 있거나 중앙집중적인 정보기술 서비스에 높은 의존도를 보이는 환경
- 분산처리 환경 : 업무 프로세스가 지리적으로 분산되어 처리되고 있거나 분산된 정보기술 서비스와 네트워크에 높은 의존도를 보이는 환경
- 아웃소싱 또는 제3자의 통신 및 기타 서비스에 의존하는 환경 : 업무 기능이나 프로세스가 외부위탁(outsourcing)에 의해 처리되거나 조직의 통제권 밖에 있는 통신 또는 기타 서비스에 높은 의존도를 보이는 환경

(1) 중앙집중처리 환경

중앙집중처리 환경에서는 단일 지역에서 발생한 대규모 사건으로 인해 전체적인 업무 프로세스가 중단될 가능성이 높으므로 분산처리 환경보다 물리적 시설물이나 장비에 대한 침해 사건에 대해 훨씬 취약하다고 할 수 있다. 이 환경에서 재해복구와 관련한 주 이슈는 얼마나 빨리 대체 지역에서 업무 프로세스가 복구될 필요가 있는가와 관련 있다.

(2) 분산처리 환경

분산처리 환경은 중요한 업무 프로세스와 컴퓨터 시스템과 같은 구성요소들이 지리적으로 분산되어 동일한 재해나 사고로 인한 위험에 노출되지 않는 경우에 해당된다. 따라서 분산환경에서의 업무 프로세스들은 물리적 재해에는 비교적 취약성이 덜한 반면 다양한 지역을 상호 연결한 통신이나 전송 서비스에 취약하다고 할 수 있다. 그러므로, 통신과 전송 서비스(특히, 제 3자에 의해 공급받는)에 관련된 위험에 특별한 주의를 기울일 필요가 있다. 또한 다양한 사이트로 분산되어 있는 업무 프로세스의 구성요소들 간의 상호 의존성을 고려하여 전반적인 시각에서 업무지속성관리를 수행해야 위험감소와 재해복구대책 구현 비용이 감소되거나 공유될 수 있다. 만약 업무 프로세스들이 연계되어 취급하지 않는다면 비록 개별적인 구성요소가 복구되었더라도 업무 프로세스는 여전히 수행되지 못하는 중대한 위험이 발생할 수 있다.

(3) 외부위탁 및 제3자 서비스 의존 환경

외부위탁 및 제3자 서비스 의존 환경은 조직의 정보기술이나 업무 프로세스를 외부에 위탁하여 서비스를 받고 있는 환경으로서 조직은 자신의 주력 분야에만 더욱 더 집중하고, 그 외의 기능이나 프로세스는 외부에서 서비스를 제공받음으로써 비용을 절감할 수 있는 장점이 있다. 이 환경에서는 서비스 수준 협정(service level agreement)에 의거해 서비스를 제공하고 문제발생시 이에 따라 보상을 받을 수 있기 때문에 이 협정을 작성할 때 업무지속성관리도 충분히 고려해야 한다. 또한 외부위탁 서비스의 중요성에 따라 서비스 제공자에 대한 면밀한 검토가 있어야 한다. 만약 다수의 서비스 제공자에게 서비스 위탁을 하였을 경우, 각 서비스 제공자가 나름대로의 업무지속성전략을 개발하고 구현한다면 큰 위험은 없을 것이다. 그러나 하나의 서비스 제공자에게 서비스 위탁이 되었을 경우, 단일 실패점을 제공하게 되므로 이 경우 위탁 의뢰기관에서 보다 심층적인 조사를 해야 한다. 조직에 매우 중요한 서비스를 외부위탁하였을 경우에는 서비스 제공자의 대표자를 업무지속성 운영위원회나 전담 팀의 일원으로 참여시킬 수 있다.

위의 3가지 환경별로 업무지속성관리 10단계를 적용할때 고려해야할 사항들을 살펴보면 아래 <표 4-1>과 같다.

<표 4-1> 정보시스템 환경별 업무지속성관리 적용시 고려사항

단계 \ 환경	중앙집중처리	분산처리	외부위탁처리
①업무영향분석	· 단일 지역의 처리 업무 분석	· 업무프로세스간의 상호 의존도	· 위탁 업무의 중요도와 프로세스 분석
②위험평가	· 주요 단일 실패점 (단일 전화 교환기, 전원공급기)의 안전성 파악	· 사이트간의 통신/ 네트워크 서비스 손상	· 서비스 업체내의 문제 (재해, 파업, 부도 등) · 다른 고객과의 이해 충돌 가능성
③위험감소 대책	· 중요 시설물과 장비에 대한 물리적 보호 · 통신/네트워크의 우회 경로 · 사고(화재) 확산 방지 대책 · 핵심 업무처리를 위한 자원 및 구성요소의 위치 고려	· 중요 자산 분산 · 통신/네트워크에 대한 특별한 주의 (우회 경로마련) · 모든사이트에 동일한 통신보안정책 마련	· 서비스 제공자 평가기준 · 여러 업체에 위탁 업무 분산 · 업무지속성을 위한 전략 개발 및 구현 요구 · 서비스 수준 협정에 위험에 대한 대책 명시 · 문제발생시 즉각적인 의사소통 구조 보장 · 서비스 제공자와 협력하여 업무지속성관리 전담팀 구성
④복구대책	· Cold-site(가구, 전원,통신회선 설치) · Hot-site(컴퓨터, 네트워크 장비) · 원격지 백업	· 대체사이트에 인력, 기자재재배치 · 대체사이트로 통신/네트워크전환 · 중요데이타 분산	· 자체백업(in-house back up)설비 · 제2의 외부위탁 업체와 업무지속성 복구계약

단계 \ 환경	중앙집중처리	분산처리	외부위탁처리
⑤대안평가	· 구현 비용 · 대안의 효율성 · 업무상 위험	· 업무프로세스간의 상호 의존도	· 위탁 업무의 중요도와 프로세스 분석
⑥명령,지휘,의사소통 구조	· 연락 체계 분산	· 사이트별 복구팀 원들간의 상호 협력	· 의뢰기관과 서비스 업체 복구팀간의 상호 교류 · 책임과 권한 명시
⑦업무복구계획을 위한 프레임워크 개발	· 일반적인 프레임워크 구성과 동일	· 사이트간의 원활한 의사소통 · 사이트간의 변경 통제 협력(호환성) · 상호 백업을 위한 표준	· 서비스 제공 업체와의 관계 고려
⑧재해복구대책과 위험감소 대책의 구현	· 중앙 통제팀과 업무 복구팀과의 원활한 의사소통 및 체계 · 통신분야 대책	· 대체설비(공간, 시스템, 통신 등) 활용	· 비상통제센터와 고객, 서비스 업체의 연락수단 · 위험감소와 재해복구 장비의 소유권 · 변경사항 반영
⑨업무복구계획 개발	· 핵심 인력 부재시에도 복구계획 가동 · 비상연락망 체계 · 복구설비에 통신수단 확보 · 백업절차,복구방법	· 사이트간의 정확한 연락망과 통신수단 · 우선 복구업무 순위 기준	· 고객과 서비스 제공측과의 작업 배정 · 변경 통제의 필요성 · 감사절차
⑩운영관리	· 단일 사이트 실패에 대비한 전체 테스트 또는 개별 구성요소별 연속적인 테스트	· 최신 정보 유지 (연락망, 자산구성) · 교육/훈련,테스트 · 다수 테스트의 복잡함에 대비한 사전준비 및 계획	· 테스팅에 대한 책임 정의 · 계약서에 테스트에 대한 증거자료 제출 명시 · 계약에 명시된 적절한 변경관리

5. 결론

업무지속성관리는 정보시스템에 대한 조직의 의존도가 커지는 현재 상황에서 반드시 고려해야할 분야이다. 단순한 재해복구 차원을 넘어서 정보시스템이 이용되는 목적인 업무 측면에서 중단없는 서비스를 위한 전반적인 관리가 필요하다. 하지만, 아직까지 업무지속성관리 개념이 국내에는 생소하고, 적용하기에도 어려움이 많다. 업무영향분석(BIA)이나 위험평가 등의 작업은 그 세부 방법이나 기법이 적용하는데 어렵고, 국내 환경에도 알맞지 않은 부분이 많다. 그러므로, 전반적인 업무지속성관리를 위해서는 이러한 세부절차에 대한 연구부터 좀 더 활발히 이루어져야 한다. 또한 정보시스템 이용 환경이 더욱 다양화되고 혼합되는 추세이므로 이들 환경에 대한 업무지속성관리 적용에 대해서도 고려해야할 필요가 있다.

참고문헌

[1] Butler, J., *Contingency Planning and Disaster Recovery Strategies*, Computer Technology Research Corp., 1994.

[2] Carlton, R. A., "Telecommunications Disaster Planning," *DATAPRO,* 1994.

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

[4] Corby, M., "Disaster Recovery Testing in a Client/Server Environment," DATAPRO, July 1994, pp.101-107.

[5] Devlin, E., C. Emerson, and L. Wrobel, *Business Resumption Planning*, Auerbach, 1998.

[6] ISO/IEC JTC1/SC27 N689, *Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security*, ISO, Mar. 1993.

[7] ISO/IEC JTC1/SC27 N720, *Guidelines for the Management of IT Security(GMITS): Part2- Managing and Planning IT Security,* ISO,

May. 1993.

[8] ISO/IEC JTC1/SC27 N777, *Guidelines for the Management of IT System Security (GMITS): Part1-Concepts and Models for IT Security*, ISO, Oct. 1993.

[9] Jackson, Carl B., "Business Continuity Planning: The Need and the Approach," *DATA PRO*, February 1994, 101-109.

[10] Menkus, B., "The New Importance of "Business Continuity" in Data Processing Disaster Recovery Planning," Computers & Security, (Vol. 13, No. 2) May 1994, pp.115-118.

[11] Smith, M. and J. Sherwood, "Business Continuity Planning," Computers & Security, (Vol. 14, No. 1) Jan. 1995, pp.14-23.

[12] UCG (United Communications Group), "Trends in Disaster Recovery," I/S Analyzer, (Vol. 26, No. 11) Nov. 1988, pp.1-12.

[13] 김정덕, 업무지속성관리에 관한 연구, WISC, 1998.