通信情報保護學會誌
第6卷 第1號, 1996. 3

정보시스템에 대한 재난복구
- Comdisco사의 실시간 재난복구서비스 사례 -

Disaster Recovery for Information System
- Realtime Disaster Recovery Services Case of Comdisco, Inc. -

김 기 윤*, 나 관 식**

요 약

재난에 관한 내용적 연구로서 실시간 재난복구를 위한 의사결정지원시스템과, 과정적 연구로서 재난복구를 위한 위기관리모형을 설명한다. 또한, 정보시스템의 재난복구전략을 구체적으로 기술하고, 특히 Comdisco사의 실시간 재난복구서비스 사례를 제시하고자 한다.

1. 서 론

재난은 일반적으로 정보시스템의 자산에 대해서 위협이 매우 파괴적인 경우에 그 결과로써 발생되는 손실이다. 다양한 조직 마다 서로 다른 재난들을 만나게 된다. 모든 시스템은 하위 시스템들의 상호작용의 산물이므로, 특히 재난복구를 위해서는 하위시스템 간에 상호작용의 복합성을 연구 할 필요가 있다. 비상사태란 위험이 진행 중인 상태이며, 진행 중인 위험인 실시간 사건(real-time events)에 대한 실시간 의사결정 상황이다. 재난에 대한 대비는 '재난복구(disaster recovery)', '비상사태계획(contingency planning)', '사업연속(business continuity)', '운영연속(continuity of operations)', '사업재개계획(business resumption planning)' 등으로 불리고 있다. 비상사태 하의 재난에 대비하는 목적은 정전, 하드웨어 고장, 화재 등과 같은 위협에 의해서 장애를 받지 않고, 조직의 중요한 기능이 연속적으로 운영될 수 있도록 하는 것이다.

정보시스템의 재난복구는 실시간에 정보보호(information security)를 확보하는 것이다. 여기서 정보보호란 정보의 입력, 처리, 저장, 출력, 전송 등 모든 단계에서 정보를 보호하기 위해 정보의 비밀성(confidentiality), 무결성(integrity), 가용성(availability), 인증성(authenticity), 이용성(usability) 등을 확보하는 것이다. 따라서, 정보시스템 재난복구의 목적은 정보시스템이 제공하는 정보와 서비스에 대해 적절한 수준의 비밀성, 무결성, 가용성, 인증성, 이용성 등을 실시간에 유지하는 것이다.

* 광운대학교(인문사회과학연구소 위험관리연구실) 경영학과 교수
** 서원대학교 경영정보학과 전임강사

영국의 BIS Applied Systems에서 1987년에 발간한 '컴퓨터재난 사례집(Computer Disaster Casebook)'의 통계에 따르면, 175개 컴퓨터재난의 원인이 화재 및 폭발이 36%, 소프트웨어가 24%, 전력이 21%, 수재가 9%, 파업이 7%, 건물이 3% 등으로 조사된바 있다. 화재로 인한 컴퓨터재난의 59%가 컴퓨터실 밖에서 발생된 것이었다. 이와 같은 위험에 효과적으로 대처하기 위해서는 예방할 수 있는 보안대책, 여분의 대체설비, 원상복구시키는 설비 등은 물론이고, 이에 대한 체계적인 연구가 필요하다. 재난에 관한 연구분야는 가장 학제적인 분야(interdisciplinary fields) 중의 하나이며, 기존연구는 크게 내용연구와 과정연구(content rese-arch and process research)로 구분할 수 있다.

따라서 본 논문의 목적은 첫째, 재난에 관한 내용연구로서 실시간 재난복구를 위한 의사결정지원시스템을, 과정연구로서 재난복구를 위한 위기관리모형을 체계적으로 기술하는데 있다. 둘째, 정보시스템의 재난복구전략을 구체적으로 설명하고, 특히 Comdisco사의 실시간 재난복구서비스 사례를 제시하고자 한다.

2. 정보시스템의 재난에 관한 기존 연구

재난에 관한 연구는 크게 내용연구와 과정연구로 구분할 수 있다. 내용이란 의사결정되는 것이 무엇인지를 식별하는 것이고, 과정이란 그러한 의사결정이 어떻게 이루어지는지를 기술하는 것이다. 내용연구는 재난과 관련된 의사결정 내용자체에 대한 연구로서 재난의 개념정의, 분류체계, 실시간 위험관리의 구성요소 등에 대해서 기술하고, 과정연구는 재난에 대한 의사결정의 실행에 대한 연구로서 위기관리 5단계, 재난의 3수준, 비상사태계획 6단계 등에 대해서 기술하고자 한다.

정보시스템의 재난에 대한 개념을 NIST (1994)에서는 "컴퓨터 운영의 붕괴로 조직의 정상적 기능이 파괴되는 비상 사태"라고 정의하였으며, Owen(1995)은 "생명, 재산, 자산 그리고 정상적인 운영능력에 대한 위험"이라고 정의 했다. 이와같이 재난은 일반적으로 정보시스템의 자산에 대해서 위협이 매우 파괴적인 경우에 그 결과로써 발생되는 손실이라고 할 수 있다.

정보시스템의 재난에 대한 분류를 Owen (1995)은 인간오류에 의한 재난, 의도적인 재난, 자연재난 등의 세가지로 분류한 바 있다. Loch와 Carr 그리고 Warkentin(1992)은 위협을 원천(source)의 위치에 따라서 내부 및 외부(internal & external) 위협으로, 가해자(perpetrator)가 누구인가에 따라 인간 및 비인간(human & non-human) 위협으로, 또한 의도(intent)의 유무에 따라서 의도적과 비의도적(intentional & accidental) 위협으로 구분했다. 그러므로, 재난도 내부 및 외부 재난, 인간 및 비인간 재난, 우연적 및 의도적 재난으로 분류될 수 있다.

재난은 실시간 사건으로서 사전 신호 없이 발생할 수 있는 큰 위험이므로, 실시간으로 관리되어야 한다. Beroggi와 Wallace(1994)는 상호작용하는 실시간 위험관리(real-time risk management)를 위해 다음과 같은 새로운 파라다임을 제시했다. 즉, 큰 위험이 내재되어 있는 대규모 시스템을 관리하기위한 실시간 위험관리는, 다음과 같은 3가지 중요한 요소로 구성되어 있다는 것이다.

(1) 실시간 사건들(RTE's; Real-Time Events)에 대해서, 계획된 대체안(정보시스템에서는 보안대책)으로 대응해 나갈 수 있는 대규모 운영시스템(large-scale operational system).
(2) 잠재적인 긴급사태를 감지해서 대체안을 수정해야 할지를 추론하는 위험관리자인

실시간 통제자(real-time controller).

(3) 대규모 운영시스템과 실시간 통제자간에 자료 전달을 위한 통신시스템(communication links).

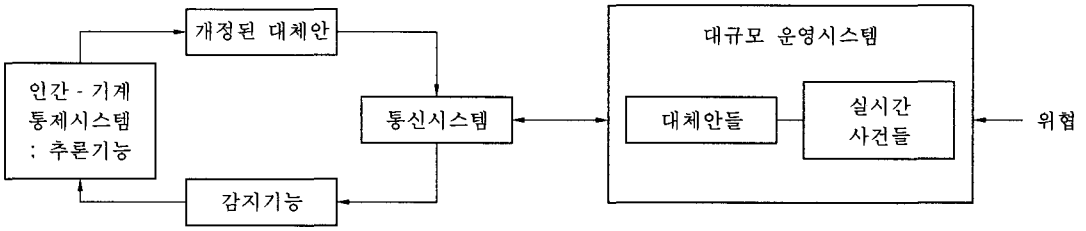

그림 1 실시간 위험관리

실시간 사건들은 기존의 대체안에 대해 변화를 줄 수 있는 사건들이고, 사전 신호 없이 발생할 수 있으므로, 시스템은 물론 외부 환경을 계속적으로 감시 해야만 한다. 통신시스템에 의해서 감지기능과 추론기능을 거쳐서 새로 개정된 대체안을 선택할 수 있는 시간은, 실시간 사건이 기존 대체안에 의해서 얼마나 효과적으로 처리되고 있는가에 달려있다. 그러므로, 위협에 의해 발생된 재난이란 실시간 사건에 대해서 기존 대체안의 비용 및 효과분석을 할 수 있는 평가시스템이 추론기능 안에 구축되어 있어야 한다. 추론기능에는 실시간 사건의 결과를 측정하는 기능, 그리고 이에 대해서 기존 대체안과 개정된 새로운 대체안의 효율을 비교 및 평가하는 기능이 있다. 이와 같은 분석 및 의사결정이 실시간에 이루어져야만 한다. 실시간 의사결정은 손실을 초래하는 예기치 않은 사고에 대응하기 위해서 필요하다. 이에 대해서 기존 방법들에서는 비상사태 및 재난상황에서 계획된 행동들의 선택과 실행을 자동적으로 하기 때문에, 긴급사태에 대한 대응과정에서 수정을 할 수 없었다.

정보시스템에 대한 컴퓨터 비상사태 대책팀(CERTS; Computer Emergency Response Teams) 혹은 긴급운영센터(EOC; Emergency Operation Center) 혹은 비상사태 계획팀(CPT; Contingency Planning Teams)과 같은 실시간 위험관리본부는, 조직 내의 자원들이 주요 기능에 어떻게 지원되는지를 파악하기 위해서 다양한 분야의 구성원들로 조직되어야 한다. 특히 기술관리분야, 시설관리분야, 재무 및 인사관리를 포함하는 조직의 기능적인 분야 등 세분야는 필수적으로 포함되어야 한다.

비상사태 및 재난 상황에서 안전과 비용문제에 대해 실시간 의사결정하는데는, 불확실성과 시간의 제약에 의한 인간의 인지적 한계(cognitive limitations)가 존재한다. 그러므로, 정보기술의 지원없는 위험관리자는 실시간 통제자가 될 수 없다. CERTS 혹은 EOC 혹은 CPT의 팀장이 실시간 통제자로서 위험관리를 수행하기 위해서는, 무엇보다도 과거 사고에 대한 데이터베이스의 지원이 필수적이다. 실시간 위험관리에서 핵심적인 것이 Moses(1995)가 ISO/IEC JTC1/SC27/WG1 N534 에서 제안한 사고분석서비스(IAS; Incident Analysis Services)를 위한 표준화된 데이터베이스의 개발이다. 현재 직면해 있는 위협의 대부분은 과거 사고의 범주를 크게 벗어나지는 않기 때문에, 사고분석서비스의 데이터베이스 구조는 유연성을 가지고 있어야 하며, 다음과 같은 장점이 있다.

(1) 실시간으로 사고 데이터를 분석해서 사고

발생의 유형과 추세를 식별하게 함으로써, 사고의 예방과 대책을 실시간으로 수립할 수 있다.

(2) 위험관리자가 선택할 수 있는 대체안들의 우선순위에 대한 신뢰성을 높일 수 있다.

(3) 위협의 빈도, 취약성 및 손실의 측정 등을 보다 정확하게 할 수 있으므로 위험분석 및 관리의 질을 높일 수 있다.

이와 같은 정보기술을 근거로 한 전략적 의사결정과 기계적인 지침서(guideline)의 효율적인 조합을 형성시키기 위해서, 인간-기계 통제 시스템은 메타-추론 구조(meta-reasoning structure)로 설계되어야만 실시간 사건이 발생되더라도 효과적으로 대처할 수 있다.

재난에 대한 과정적 연구로서 Mitroff(1988)은 다음과 같은 5단계로 되어있는 위기관리모형을 제시했다.

(1) 신호탐색단계:

실제 큰 위험이 발생되기 전에, 오랫동안 반복적으로 위기 징후를 알리는 초기 경고신호(warning signals)가 나타난다. 위기관리자는 이러한 신호를 알아차려야 한다. 이러한 경고신호에 주의하지 않기 때문에 많은 위기가 발생하고 있다. 위기의 초기 경고신호에 대한 대응을 어떻게 해야 하는지를 결정짓는 중요한 요소 중의 하나가 조직문화이다. 위기관리에 수동적인 조직은 초기 경고신호를 무시할 뿐만 아니라, 의도적으로 경고신호를 차단시키기도 한다. 그러나, 위기관리에 능동적인 조직은 초기 경고신호에 민감하게 반응하며, 적극적인 대응을 하려 한다.

(2) 예방 및 준비단계:

특정 위협에 대한 경고신호의 특성을 감지해서 평소에 마련한 비상사태에 대한 계획화(contingency planning)를 보다 구체화시키는 단계이다. 재난을 피하기 위해서 항상 조직내에 예방 및 준비체계가 현장에서 시험되어져야만 한다. 예방 및 준비체계는 취약성의 모든 신호를 적극적으로 탐색해서, 위기관리팀이 노출된 취약성에 적절히 대응할 수 있도록 해야 한다. 만약 재난을 막지 못했다면, 바로 그 순간이 재난에 대처해야 할 때이다.

(3) 손실축소단계:

재난 사태가 돌발한 후에는, 재난지역을 봉쇄하고 손실이 가능한한 축소되도록 해야 한다. 모든 위기를 피할 수 있는 대응책은 없으므로, 평소에 조직내의 손실축소체계가 현장에서 시험되어야 한다.

(4) 재난복구단계:

예방 및 준비단계에서 구체적으로 마련된 단기적 및 장기적 비상사태계획에 의해, 현장에서 여러 전략들 중 한가지 대체안을 선택해서 실행에 옮기는 일이다. 그러나, 이러한 복구체계를 예상할 수 없다면, 재난 사태 후에 응급조치를 취할 수 밖에 없다.

(5) 학습단계:

위험분석에 의해서 과거의 재난에 대한 대응책을 재평가하여 계속적으로 위기관리 능력을 향상시켜 나간다.

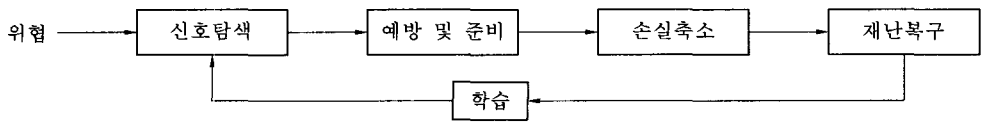

그림 2 위기관리모형

Stephenson(1994)은 재난의 세가지 수준을 단계적으로, 위기 → 사업운영의 중단 → 전체 규모의 재난으로 구분한 바 있다.

(1) 위기란 위험이 진행 중인 상태를 말한다. 진행 중인 위험을 위기라고 정의 할 때, 수학적으로는 위기는 위험의 변화율이 되므로, 위험을 시간 t 에 대해서 미분한 것이 위기가 된다고 할 수 있다.
(2) 사업운영의 중단은 설비고장 혹은 정전 등과 같은 위협에 의해서 일시적으로 정보시스템이 정상적인 기능을 발휘하지 못함으로써, 사업의 운영이 중단되는 상태를 말한다.
(3) 전체규모의 재난은 일반적으로 정보시스템의 자산에 대해서, 위협이 매우 파괴적인 경우에 발생된 손실이다.

여기서 (1)은 위기관리모형의 예방 및 준비단계에 해당되고, (2)는 손실축소단계에, (3)은 재난복구단계에 해당된다고 볼 수 있다.

미국의 NIST(1994)에서는 비상사태계획에 대한 6가지 기본단계를 다음과 같이 제시했다.

(1) 조직의 임무 혹은 주요 기능들의 식별

조직 내의 중요한 기능들을 식별해서 우선순위를설정한다.

(2) 중요한 기능들을 지원하는 자원들의 식별

인적자원, 처리능력, 컴퓨터 서비스, 자료 및 응용프로그램, 물적 하부구조, 서류 및 종이 등 필요한 자원의 상호작용 및 의존관계를 식별한다.

(3) 잠재적인 재난에 대한 예측

조직의 중요한 기능과 자원에 영향을 줄 수 있는 비상사태의 여러가지 시나리오를 예측한다.

(4) 비상사태 계획을 위한 전략의 선택

재난복구을 위한 전략들을 평가해서, 그 중의 한가지를 선택한다.

(5) 전략의 실행

선택된 전략을 실행에 옮긴다.

(6) 계획의 시험 및 개선

실행가능한 전략들을 반복 시험한 후에 개선시킨다.

여기서 (1), (2), (3)은 위기관리모형의 예방 및 준비단계에 해당되고, (4), (5)는 재난복구단계에, (6)은 학습단계에 해당된다고 볼 수 있다. 이와 같은 위기관리 혹은 비상사태계획의 과정 중에서, 재난복구를 위해 선택될 수 있는 전략들에 대해서 구체적으로 기술하고자 한다.

3. 정보시스템에 대한 재난복구

Owen(1995)은 네트워크 관점에서 재난복구를 "네트워크의 운영중단사태를 복구하는 과정"이라고 정의했다. 구체적으로 재난복구에는 생명, 재산, 자산의 보호, 그리고 사업운영능력 등의 복구가 포함된다. Rosenbaum(1995)은 재난복구의 5가지 목적으로, 조직구성원 및 고객의 안전과 복지를 지키는 것, 기업의 자원과 자산 그리고 기존 운영을 보호하는 것, 운영중단에 적시적이고 효과적으로 대응하는 것, 가능한 빠른시간 내에 정상적인 운영을 재개시키는 것, 변화하는 사업 목적과 운영에 대비하는 것 등을 제시 했다. 간단히 말해서, 정보시스템의 재난복구의 목적은 실시간에 정보보호(정보의 비밀성, 무결성, 가용성, 인증성, 이용성 등)를 확보하는 것이다. 또한, Owen(1995)은 재난복구의 5가지 주된 요소를 다음과 같이 제시했다.

(1) 위험관리자는 최악의 시나리오에 대한 계획을 세우고, 이에 대한 훈련을 해야 한다.

(2) 재난 발생 즉시 생명, 재산, 자산 등을 보호하기 위한 자원을 신속히 조달할 수 있는 긴급대책을 마련해야 한다.
(3) 사업재개(business resumption)를 위한 '사업연속성 계획(business continuity planning)'을 마련해야 한다.
(4) 보험 혹은 재난복구서비스 공급업자에 의해서 재난에 영향을 받은 정보시스템을 수리, 교체, 재건하는 과정인 복원(restoration)은 필수적 단계이다.
(5) 재난 발생 이전의 상태와 마찬가지로 조직내에 모든 자원이 활용되는 정상적인 운영의 재개이다.

Stephenson(1995)은 재난복구계획의 4가지 주요 목적으로, 운영중단의 요인을 식별하는 것, 재난예방책 및 재난에 대한 대응책을 마련하는 것, 생존에 대한 계획을 세우는 것, 최악의 경우에 대한 재난복구방법을 준비하는 것 등을 제시했다. Jackson(1994)은 정보시스템의 재난복구계획을 크게 수평적 지원서비스(horizontal support services)와 수직적 사업단위(vertical business units), 두가지 측면으로 작성되는 행렬표를 제시했다. 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 등 이다. 또한, Jackson(1994)은 구체적으로 재난복구계획을 5가지 영역(자료처리, 음성 및 자료 통신, 최종사용자, 부서시설, 주요시설)으로 구분했다. Corby(1994)는 재난복구계획을 8가지 영역(하드웨어, 시스템 소프트웨어, 응용 소프트웨어, 통신, 인적자원, 소모품, 보고서 및 문서, 자료처리 및 사무실 시설)으로 구분했다.

또한, Jackson(1994)은 본원적인 복구계획방법(generic recovery planning methodology)으로서 기본적인 5단계를 제시했다.

(1) 복구 프로젝트 초기단계

복구 프로젝트의 영역을 정의하고, 어떻게 프로젝트 팀을 조직할 것인지 결정한다. 소프트웨어 및 시설 구입비, 복구계획개발과 관련된 인건비 및 시험/유지관리비, 자료처리 매체의 원격지 저장비 등 최소한의 재난복구예산을 산정한다.

(2) 취약성 평가단계

재난으로 인한 손실을 추정한 후에, 조직내에 각 기능을 식별하고, 시간적으로 긴급복구가 필요한 자원 혹은 자산은 복구의 우선순위를 높게 설정한다.

(3) 복구대체안 선택단계

우선순위화된 자원 혹은 자산 별로 최대허용 가능한 운영정지시간(maximum allowable downtime or drop dead time)을 정의하고, 복구대체안 혹은 전략에 대해서 비용효과분석을 실시하여 최적안을 선택한다.

(4) 복구계획 개발단계

위 (1)에서 (3)까지 각 단계의 결정사항을 문서화 하고, 지원서비스 분야 복구계획, 사업단위 복구계획, 중요 기록 등에 관한 정보 등을 체계화 한다.

(5) 복구계획 시험 및 유지관리단계

복구계획 개발의 주기상 시험한 후에, 약점을 보완해서 복구계획을 유지관리 한다.

비상사태 계획에서 재난복구를 위한 대체안 혹은 전략에 대하여 영국의 CCTA(Central Computer and Telecommunications Agency, 1990)에서는 다음과 같은 9가지를 제시했다.

(1) 무대책(do nothing)

비용이 들기 때문에 비상사태에 대한 대책

을 전혀 마련하지 않는 것이다.

(2) 사무적인 지원절차
(clerical backup procedures)

비상사태에 대한 계획 중 사무적인 지원절차로만 가능한 대책을 마련한다.

(3) 상호계약(reciprocal arrangement)

이것은 두 회사 중에 어느 한 회사가 비상사태 일 때, 다른 회사의 컴퓨터시스템 일부 혹은 전체를 이용할 수 있도록, 사전에 상호계약을 하는 것이다. 컴퓨터시스템의 상호이용이 가능하도록 변경관리시스템(change management system)에 대한 서면협의가 사전에 이루어져야 한다.

(4) "요새" 접근방법(the "fortress" approach)

이것은 재난이 발생되어도 컴퓨터실을 이전시키지 않고, 손상된 컴퓨터시스템에 즉시 자금을 투입해서 원상회복시키는 것이다. 이와 같은 대책은 가능한한 손실을 축소하려는 것이지만, 모든 재난에 대해서 가능한 접근방법이 될 수는 없다.

(5) 편의시설만 구비된, 고정된 컴퓨터실을 제공하는 경우("cold" start fixed centre)

여기서 cold start란 컴퓨터를 지원하는 전기공급, 주변제어장치, 통신회선 연결 등(컴퓨터 설비를 제외한 주변장치를 포함한 편의시설만 제공 가능)을 제공하는 고정된 또는 이동가능한 건물에 대한 계약규정(provision of a building; accommodation only)을 말한다. 이것은 외부회사에서 고정된 장소로 비어있는 컴퓨터실을 제공하는 것이다. 이곳에는 필요한 전기, 주변제어장치, 외부 통신회선 등을 설치해 놓고, 서비스 이용자는 사전에 결정된 년간 예약금을 지불한다.

(6) 편의시설만 구비된 이동가능한 컴퓨터실을 제공하는 경우("cold" start portable centre)

이것과 (5)의 차이는 설비가 이동가능하기 때문에, 주차장과 같이 사전에 계약한 장소에 설치할 수 있다는 것이다. 이와 같은 대책의 장점은 기존 정보시스템의 인접한 곳에 컴퓨터실을 설치할 수 있다는 것이고, 단점은 이와 같은 컴퓨터실을 마련하는데 소요되는 시간이 3일에서 10일 정도 소요 된다는 것이다.

(7) 편의시설은 물론 컴퓨터 까지 구비된 전산실을 외부회사에 의뢰하는 경우("hot" start- external)

여기서 hot start란 컴퓨터를 지원하는 전기공급, 주변제어장치, 통신회선 등(컴퓨터 설비와 주변장치를 포함한 편의시설도 가능)을 제공하는 움직일 수 없는 혹은 이동가능한 컴퓨터 설비에 대한 계약규정(provision of computer accommodation; accommodation and equipment) 을 말한다. 이것은 외부회사의 서비스로서 하드웨어를 포함한 컴퓨터실에 대한 접근에 관한 규정을 충족시키고 있다. 비용은 중앙연산처리장치의 규모, 주변장치의 수와 형태, 소프트웨어 등에 따라 다르다. 이와 같은 대책의 장점은 고객입장에서 안전한 건물에서 즉각적으로 컴퓨터시스템을 운용할 수 있다는 것이고, 단점은 대부분의 경우 상당히 멀리 떨어진 장소에 이와 같은 건물이 마련되고, 비용이 비교적 비싸다는 것이다.

(8) 편의시설은 물론 컴퓨터 까지 회사 내부에서 마련하는 경우("hot" start-internal)

이것은 (7)과 같은 대책을 외부회사에 의뢰하지 않고, 내부에서 마련하는 것이다. 이와 같이 회사 내에서 준비해 둔 컴퓨터실은 비상사태 발생시 즉시 사용할 수 있다는 장점이 있지만, 컴퓨터 시스템에 대한 중복투자비용이 크다는 것이 단점이다.

(9) 편의시설은 물론이고 컴퓨터 까지 구비된 전산실을 배달해 주는 경우(mobile hot start or "computer on the back of a lorry")

이것은 고객이 지정한 장소에 사전에 합의한 컴퓨터시스템을 정해진 시간 이내에 배달해 주는 계약규정이다. 컴퓨터시스템은 트레일러 안에 있고, 트레일러 자체가 컴퓨터실 기능을 할 수 있도록 되어있으며, 화물자동차에 의해서 지정된 장소까지 운송한다. 회사가 지정한 장소에는 트레일러에 전기공급, 통신회선 접속과 주차가 가능한 안전한 장소이어야 한다. 이와 같은 대책의 장점은 사무실 가까이에 트레일러를 설치함으로써, 신속한 지원을 받을 수 있다는 것이고, 단점은 하드웨어의 종류가 제한되어 있고, 트레일러 설치장소에 전기공급 시설 등과 같은 특별한 조치가 필요하다는 것이다.

Owen(1995)은 재난 사건의 수준을 내부자원으로 통제할 수 있는 경우(수준 Ⅰ, Ⅱ)와 외부 도움이 필요한 경우(수준 Ⅲ)로 구분했다.

(1) 수준 Ⅰ - 수준 Ⅰ의 사건은 한 장소에서만 발생되고, 내부 자원에 의해서 처리되어질 수 있다. 정상적인 업무에 영향이 적으므로, 다른 부서에 통보되지 않을 수도 있다. 작은 수재, 건물 내의 부분적인 정전, 설비 고장 등과 같은 경우로써, 현장에서 즉시 시행가능한 긴급대책에 의해서 통제된다.

(2) 수준 Ⅱ - 수준 Ⅱ의 사건은 여러 장소에서 발생되고, 내부 자원에 의해서 처리되어질 수 있다. 일시적으로 정상적인 업무장애를 일으키며, 중요한 업무의 재배치가 필요하다. 화재, 특정 지역의 정전, 작은 지진 등에 의해서 발생된 사건으로써, CERTS 혹은 EOC와 같은 중앙본부가 사전에 준비한 긴급대책에 의해서 통제된다.

(3) 수준 Ⅲ - 수준 Ⅲ의 사건은 지역적인 재난에 의해서 발생되고, 복구를 위해서는 외부 지원에 의해서만 가능하다. 정상적인 업무로 복구되는 기간이 며칠 혹은 수 주일이 소요된다. 큰 지진, 홍수, 태풍 등에 의해서 발생된 사건으로써, CERTS 혹은 EOC가 사전에 준비한 긴급대책에 의해서 통제된다.

재난복구서비스란 Owen(1995)이 분류한 수준 Ⅲ의 사건이 발생한 경우에, 외부 재난복구서비스 공급업자의 지원에 의해 피해 정보시스템을 수리, 교체, 재건하는 복구과정에 대한 서비스를 말한다. 외부의 재난복구서비스 공급업자에 의해서 제공될 수 있는 것은 위에서 기술된 9가지 대체안들 중에서 (5), (6), (7), (8), (9)이다.

4. Comdisco사의 실시간 재난 복구 서비스 사례

전통적으로 대부분의 기업들은 정보시스템의 재난복구를 위해서 주기적인 백업(back-up) 시스템을 채택하고 있지만, 이 경우는 백업 시점과 재난발생 시점 사이의 자료가 복구 불가능하거나, 수작업으로 자료를 다시 입력하여야만 한다. 이때 재난발생 조직은 막대한 금전적 손실, 장시간의 업무 마비, 대외 이미지 손상 등의 피해를 감수 해야만 한다. 이러한 피해를 막을 수 있는 유일한 방법은 실시간 복구(realtime recovery) 시스템을 구현하는 것이다.

본 사례에서는 현재 가장 대표적인 실시간 가용성 서비스(availability service)를 제공하고 있는 Comdisco 사의 전략을 고찰 하고자 한다. 1969년 IBM 임대회사로 설립된 Comdisco 사는 현재 정보시스템의 재난복구 분야에서 선도기업이며, 자회사인 CCSC(Comdisco Computing Services Corporation)와 CDRS

(Comdisco Disaster Recovery Services)를 통해서 연속적인 가용성 서비스를 제공하는 회사이다. 이 회사는 실시간 재난복구 서비스를 위해서 원격 저널링(remote journaling)과 전자도약(electronic vaulting)과 같은 방법을 미국 및 유럽지역에서 제공하고 있다. 고객시스템의 복구를 위해서는 운영시스템의 복구, 데이터베이스의 복구, 응용시스템의 복구로 진행되는 3단계 복구절차를 적용하고 있다.

(1) **원격 저널링** - CCSC가 하루동안 발생한 거래들(intra-day transactions)을 포착해서 실시간으로 원격지(off-site)에 전달하는 능력을 제공하는 것을 말한다. 이는 ENET-1의 능력을 이용해서, 고객의 거래 데이터를 연속적으로 포착하여 실시간으로 CCSC설비로 전송한다. 데이터는 자동적으로 테이프에 기록되고, 표준기간인 3일 동안 보관된다. 이를 통해서 고객은 실제 재난이 발생되었을 때, 시스템을 복구하는 능력을 가지게되며, 정보를 재창출하는데 소요되는 노력을 극소화시키게 된다. 여기서 FEP(Front End Processor)는 차후의 처리를 위하여 본체에 자료를 보내기 전에 자료를 저장, 검증, 압축하기 위하여 사용되는 컴퓨터로서 전위처리기 라고 하고, VTAM(Virtual Telecommunication Access Method)은 데이터 통신용 프로그램 작성을 쉽게해주는 특수한 데이터 통신 소프트웨어 패키지로서 와류형 원격통신방법이라고 한다.

이와 같은 방법의 장점으로는 거래 데이터베이스의 원격지 전송이 가능하다는 점, 재난발생 시점에서 복구가 가능하다는 점, 복구 자료를 통신망을 통해서 전송할 수 있다는 점, 최종 이용자 자료의 재입력을 최소화시킬 수 있다는 점 등을 들 수 있다.

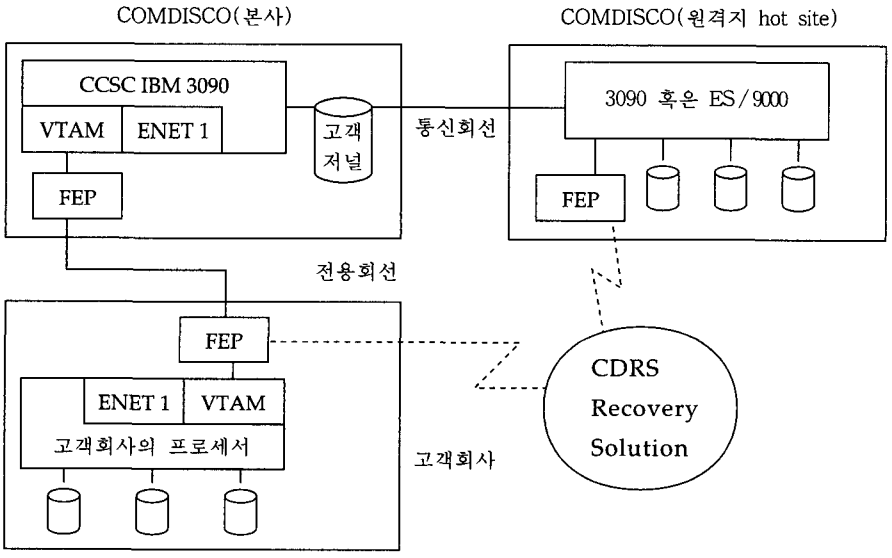

그림 1 원격 저널링

(2) 전자도약 - 일반적으로 시스템 복구를 위해서, 주기적으로 백업 테이프를 만들어 두고 있다. 이러한 백업 테이프는 평소 원격지에서 보관하고 있으며, 재난 발생시에 운반하여 시스템을 복구시킨다. 그러나, 이러한 방법은 시간이 많이 소요되고 운반 과정에서 운반자에 의한 오류가 발생될 여지가 있다. 따라서, CCSC는 채널이 확장된 STK(Storage Tek)와 ACS(Automated Cartridge System)를 이용해서 중요한 레코드 프로그램(records program)들을 전용회선을 통해서 전송 받아 저장하고 있다가, 재난 발생시에 실시간으로 복구 프로그램들을 전송하여 시스템을 복구한다. 여기서 STK는 CNT 채널확장기(channel extender)와 T3 광섬유 회로(fiber-optic circuit)를 이용해서 고객의 정보 센터로부터 채널을 확장시키는 기기이고, ACS는 자기테이프를 자기테이프 장치에 자동적으로 쉽게 탈착시키는 장치이다.

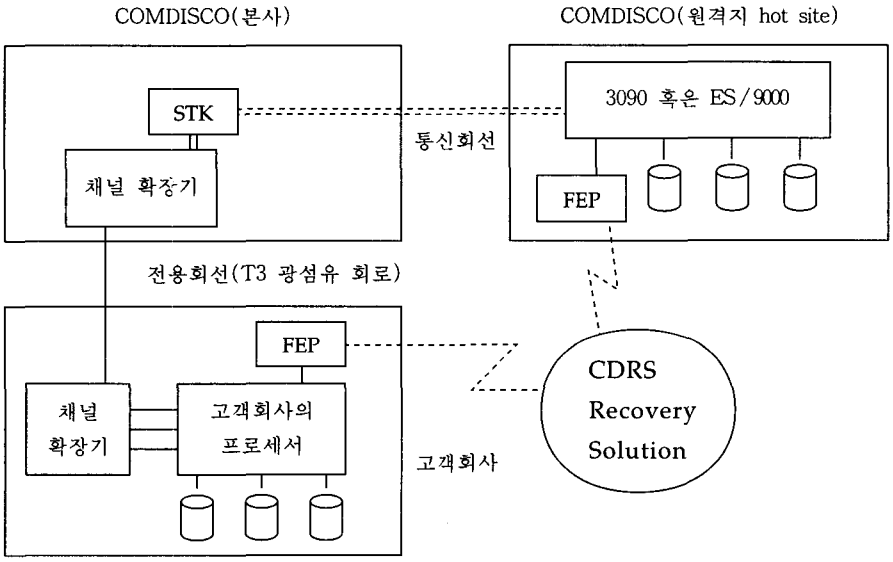

그림 2 전자도약

CCSC 데이터 센터는 고객들이 요구하는 보안수준을 제공할 수 있으며, 재난 발생시 시스템의 구성(configuration)을 채널 스위치에 의해서 복구대상 정보센터로 즉시 변경하여서, 지체없이 복구절차가 시작될 수 있도록 설계되어 있다. 이 시스템은 복구대상 자료를 복구대상 시스템에 위치시키며, 테입 운반상의 문제점을 제거시키고, 재난 발생과 동시에 복구절차가 수행된다는 등의 장점이 있다.

이러한 기법들을 이용하여 Comdisco사는 재난 발생시에 고객 시스템의 복구를 다음과 같이 3단계의 절차에 의해 수행한다.

1) 운영시스템의 복구 - 시스템 복구의 첫단계는 기본적인 운영시스템을 복구시키는 것이다. 즉각적인 복구를 위해서 고객의 운영 시스템은 CCSC가 제공하는 실시간 직접접근 기억장치인 DASD(Direct Active Storage Devices)에 저장되어 있다가, 재난 발생시에 즉시 복구대상 시스템에 접속된다. 이때 초기화 프로그램을 적재시켜서

먼저 수행시킨 후에 후속적인 복구절차가 계속 진행되도록 한다.

2) 데이터베이스의 복구 - 재난 발생시 데이터 복구에 소요되는 시간을 제거하기 위해서 CCSC는 각종 자료를 호출하는데 대기시간이 거의 없는, 즉시 처리가능한 대용량 기억장치인 DASD를 제공하고 있고, 초기 데이터베이스의 이미지 복사(image copy)를 지원하고 있다. 데이터의 재난 발생시점 복구를 위해서는 초기 데이타베이스 이미지 뿐만아니라 사용기간 동안의 거래내역이 필요하므로, 이를 위해서는 원격 저널링 시스템을 이용한다.

3) 응용시스템의 복구 - CCSC는 3090 프로세서 안에 하드디스크를 논리적으로 분할(logical partition)하여 고객의 응용시스템을 저장하기 위한 충분한 전산자원(MIPS, 기억장치, 채널 등)을 갖추고 있다. 재난 발생 시에는 이러한 시스템이 초기화 프로그램으로 적재되어 있으므로 고객 회사의 응용프로그램을 즉시 사용 가능하게 한다. 이러한 것이 재난 발생시에 테이프와 사람의 이동, 시스템의 복구 등에 소요되는 시간을 제거시켜서, 당일로 평상 업무처리가 가능토록 한다.

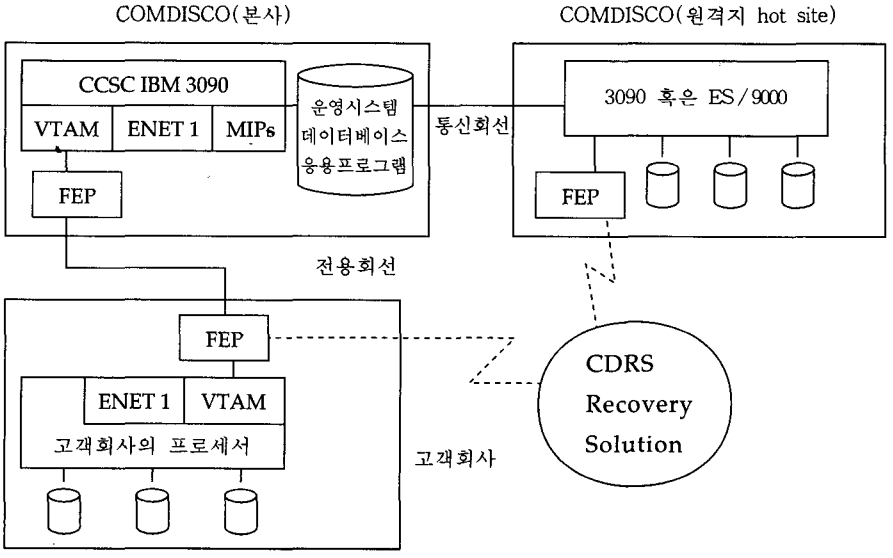

그림 3 운영시스템, 데이터베이스, 응용시스템의 복구

이와 같은 실시간 재난복구 서비스는 특히 시간 측면에서 실시간 복구가 중요시 되는 조직에 있어서 다음과 같은 장점이 있다. 첫째, 시스템 이용자에게 필요한 정보흐름을 계속 유지시키는 이득이 있다. 둘째, 이용자가 위탁한 데이터를 보호하는 효과적인 방법이 되므로 정보기술자에게 이득을 준다. 세째, 어떤 위기상황에서도 실시간 복구에 의해 회사가 정상적으로 운영되므로, 모든 조직 구성원들에게 이득을 준다.

5. 결 론

진행 중인 위험인 실시간 사건에 대한 실시

간 의사결정 상황을 비상사태라고 하며, 이러한 실시간 위험에 대한 관리를 위기관리라고 한다. 본 논문에서 연구대상이 되는 재난은 일반적으로 정보시스템의 자산에 대해서 위협이 매우 파괴적인 경우에 그 결과로써 발생되는 손실이다. 재난복구에는 생명, 재산, 자산의 보호, 그리고 사업운영능력 등의 복구가 포함된다. 정보시스템 재난복구의 목적은 실시간에 정보의 비밀성, 무결성, 가용성, 인증성, 이용성, 등을 확보하는 것이다.

재난에 관한 기존연구는 많지 않지만, 내용연구와 과정연구로 구분할 수 있다. 재난에 관한 내용연구인 Beroggi와 Wallace(1994)의 실시간 위험관리에 관한 연구에 의하면, 실시간 위험관리의 3가지 구성요소는 대규모 운영시스템, 위험관리자, 그리고 통신이다. 재난 상황인 실시간 의사결정 상황에서 CERTS나 EOC 혹은 CPT의 팀장이 실시간 통제자로서 위험관리를 하기 위해서는 인지적 한계가 있으므로, 무엇보다도 과거 사고에 대한 데이터베이스의 지원이 필수적이다. 재난에 관한 과정연구인 Stephenson(1994)의 재난의 세가지 수준과, NIST(1994)의 비상사태계획에 대한 6가지 단계도 일반적인 위기관리 5단계인 신호탐색단계 → 예방 및 준비단계 → 손실축소단계 → 재난복구단계 → 학습단계로 순환하는 관리체계로 이해 될 수 있다.

비상사태 계획에 대해서 영국의 CCTA가 제시한 9가지 재난복구 대체안은 (1) 무대책, (2) 사무적인 지원절차, (3) 상호계약, (4) "요새" 접근방법, (5) 편의시설만 구비된 고정된 컴퓨터실을 제공하는 경우, (6) 편의시설만 구비된 이동가능한 컴퓨터실을 제공하는 경우, (7) 편의시설은 물론 컴퓨터 까지 구비된 전산실을 외부회사에 의뢰하는 경우, (8) 편의시설은 물론 컴퓨터 까지 회사 내부에서 마련하는 경우, (9) 편의시설은 물론 컴퓨터 까지 구비된 컴퓨터실을 배달해 주는 경우 등이다. 재난복구서비스란 외부 재난복구서비스 공급업자에 의해서 피해를 입은 정보시스템을 수리, 교체, 재건하는 복구과정에 대한 서비스를 말한다. 재난복구서비스 공급업자에 의해서 제공될 수 있는 것은 위에서 기술된 9가지 대체안들 중에서 (5), (6), (7), (8), (9)이다.

Comdisco사의 재난복구서비스는 원격 저널링과 전자도약에 의한 고객시스템의 복구로 이루어 진다. 고객시스템의 복구는 3단계, 즉 운영시스템의 복구, 데이터베이스의 복구, 응용시스템의 복구 순으로 진행된다. 이와같은 실시간 재난복구서비스는 특히 시간 측면에서 복구가 중요시되는 조직에 다음과 같은 장점이 있다. 첫째, 시스템 이용자에게 필요한 정보흐름을 계속 진행시키는 이득이 있다. 둘째, 이용자가 위탁한 데이터를 보호하는 효과적인 방법이 되므로 정보기술자에게 이득을 준다. 세째, 어떤 위기상황에서도 실시간 복구로 회사가 정상적으로 운영되므로 모든 조직 구성원들에게 이득을 준다.

참 고 문 헌

〈국내문헌〉

[1] 김기윤, "정보기술에 대한 위험분석방법", 기업경영연구, 광운대학교, 기업경영연구소, Vol.3, 1994. 11, pp.1-18.

[2] _____ 과 김정덕, "정보시스템 위험분석과 관리", '94년도 추계학술대회논문집, 한국경영정보학회, 1994. 11., pp. 277-297.

[3] _____ 과 김정덕,"정보보호를 위한 위험분석방법: 분류와 선택기준을 중심으로", '94년도 학술대회논문집, 한국통신정보보호학회, 1994. 11, pp. 303-315.

[4] _____ 외 12인, "전산망 보안을 위한 위험관리지침서", 연구보고서, 한국전산원, 1994. 12.

[5] _____ 과 신동익, 김정덕, 박태완, "전산망 보안관리를 위한 기술지원서: 소프트웨 어 보안", 연구보고서, 한국전산원, 1994. 12.

[6] _____ 과 나관식, 김종석, "보안관리를 위한 위협, 자산, 취약성의 분류체계: BDSS 사례", 한국통신정보보호학회, 제5권, 제2호, 1995. 6, pp.49-63.

[7] _____ 과 김용겸, "정보시스템의 위험관리: 외국의 위험관리방법과 한국전산원의 위험관리방법의 비교", 리스크관리연구, 한국리스크관리학회, 제5집, 1995. 8, pp.27-52.

〈외국문헌〉

[8] Badenhorst, K. P. & Eloff, H. P., "Framework of a Methodology for the Life Cycle of Computer Security in an Organization," Computer & Security, Vol.8, No.5, 1989, pp.433-442.

[9] Beroggi, Giampiero E. G. & Wallace, William A., "Operational Risk Management: A New Paradigm for Decision Making," IEEE Transactions on System, Man, and Cybernetics, Vol. 24, No. 10, October 1994, PP.1450-1457.

[10] CCTA(Central Computer and Telecommunications Agency), Contingency Planning: IT Infrastructure Library, 1990.

[11] Corby, Michael, J., "Disaster Recovery Testing in a Client/Server Environment," Datapro, IS38-450, 1994, pp.101-107.

[12] ISO(International Organization for Standardisation)/IEC(International Electrotechnical Commission) JTC1/SC27/WG1 N501, IT Baseline Protection Manual, Nov. 1994.

[13] ISO(International Organization for Standardisation)/IEC(International Electrotechnical Commission) JTC1/SC27/WG1 N534, Study Period Document: Security Incident Reporting Analysis, Feb. 1995.

[14] Jackson, Carl B., "Business Continuity Planning: The Need and the Approach," Datapro, IS38-400, February 1994, pp.101-109.

[15] Mitroff, Ian I., "Crisis Management: Cutting through the Confusion," Sloan Management Review, Winter 1988, pp.15-20.

[16] _____, Thierry Pauchant, Michael Finney, and Chris Pearson, "Do (Some) Organizations Cause Their Own Crises ? The Cultural Profiles of Crisis Prone Versus Crisis Prepared Organizations," Working Paper, Center for Crisis Management, University of Southern California., 1990.

[17] March, James G. & Olsen, Johan P., Ambiguity and Choice in Organizations, Bergen: Universitetsforlaget, 1976.

[18] NIST(National Institute of Standards and Technology), NIST Handbook, 1994.

[19] Owen, Jeffrey, "Network Disaster Recovery," Datapro, IS38-400, 1995, pp.401-410.

[20] Ratliff, John, "Realtime Recovery-From Concept to Reality," Datapro, IS38-600, November 1993, pp.101-106.

[21] Rosenbaum, Joseph I., "Avoiding a Legal Disaster: Business Continuity Planning for Multinationals," Datapro, IS38-200, 1995, pp.101-109.

[22] Stephenson, Peter, "When Disaster Strikes," Datapro, IS38-700, 1994, pp.101-104.

□ 著者紹介

김 기 윤

1976년 고려대학교 공과대학 토목/환경공학 학사
1979년 고려대학교 경영대학원 석사
1985년 고려대학교 대학원 경영학과 박사
1980년 - 현재 광운대학교 경영학과 교수

※ 관심 분야 : 정보시스템 보안/위험관리

나 관 식

1985년 광운대학교 경영학과 학사
1987년 광운대학교 대학원 경영학과 석사
1992년 광운대학교 대학원 경영학과 박사
1992년 - 1995년 경민전문대학 사무자동화과 전임강사
1996년 - 현재 서원대학교 경영정보학과 전임강사

※ 관심분야 : 정보시스템 보안/위험관리