通信情報保護學會誌
第9卷 第1號, 1999. 3

행정전산망의 재해복구를 위한 비상계획 현황과 개선방안

김 기 윤*, 김 종 기**, 김 정 덕***, 이 경 석****

요 약

범국가적으로 추진되고 있는 정보화 사업은 행정 분야에서도 활발히 추진되고 있다. 본 고에서는 정보시스템의 재해복구를 위한 대체처리시설의 확보전략과 데이터의 백업 방법에 대하여 살펴보고, 대민업무에 직접적으로 활용되고 있는 광역지방자치단체의 행정전산망을 대상으로 각종 재해에 대비한 정보시스템 비상계획의 현황을 살펴보고 가용성을 확보하기 위한 효과적인 방안을 제시하였다.

핵심어: 비상계획, 데이터 백업, 행정전산망, 재해복구

1. 서 론

국가 공공기관 업무의 전산망에 대한 의존도가 높아짐에 따라 정보시스템의 운영 중단에 의한 행정업무의 수행에 차질을 가져옴으로써 대 국민 서비스 제공에 막대한 지장을 초래할 가능성이 상존해 있다. 이에 따라 정보시스템의 가용성(availability)이 중요한 문제로 대두되고 있고, 이러한 정보시스템의 재해복구를 위한 비상계획이 중요한 문제로 부각되고 있다.

정보시스템의 재난은 "컴퓨터 운영의 붕괴로 조직의 정상적 기능이 파괴되는 비상사태"로 인하여 "생명, 재산, 자산, 그리고 정상적인 운영 능력에 대한 위험"이라고 정의할 수 있다[1][2]. 재난은 일반적으로 정보시스템의 자산에 대해서 위협이 매우 파괴적인 경우에 그 결과로써 발생되는 손실이라고 할 수 있다. 정보시스템의 재난은 인간의 실수에 의한 재난, 의도적인 재난, 자연적인 재난 등 세 가지로 분류할 수 있다[3]. 특히 전산망(네트워크) 관점에서는 재해복구를 "네트워크의 운영중단 사태를 복구하는 과정"이라고 할 수 있다[2]. 구체적으로 재해복구에는 생명, 재산 및 자산의 보호, 그리고 사업운영능력의 복구가 포함된다.

재해복구의 목적은 조직 구성원 및 고객의 안전과 복지를 지키는 것, 조직의 자원과 자산 그리고 기존 운영 방식을 보호하는 것, 운영중단에 적시적이고 효과적으로 대응하는 것, 가능한 한 즉시 정상적인 운영을 재개시키는 것, 변화하는 사업 목적과 운영에 대비하는 것 등

* 광운대학교 경영학과 교수
** 국방정보체계연구소 선임연구원
*** 중앙대학교 정보산업학과 교수
**** 산업연구원 전산정보실장

다섯 가지로 세분할 수 있다[4]. 간단히 말해서, 정보시스템의 재해복구의 목적은 실시간에 정보보안(정보의 비밀성, 무결성, 가용성, 인증성, 이용성 등)의 목적을 보장하는 것이다. 이러한 목적을 달성하기 위하여 운영중단의 요인 식별, 재난예방책 및 재난에 대한 대응책 마련, 생존에 대한 계획 수립, 최악의 경우에 대비한 재해복구방법 준비 등의 활동이 필요하다[5].

재해복구의 요소는 다음과 같이 분류할 수 있다[2]. 첫째, 위험관리자는 최악의 시나리오에 대비한 계획을 세우고, 이에 대한 훈련을 하여야 한다. 둘째, 재난 발생 즉시 생명, 재산, 자산 등을 보호하기 위한 자원을 신속히 조달할 수 있는 긴급대책을 마련해야 한다. 셋째, 신속한 업무재개(business resumption)를 위한 '업무연속 계획(business continuity planning)'을 마련해야 한다. 넷째, 보험 혹은 재해복구 서비스 공급업자를 통하여 재난에 의해서 영향을 받은 정보시스템을 수리하고, 교체하고, 재구축하는 과정인 복구(restoration)는 필수적 단계이다. 마지막으로, 재난 발생 이전의 상태와 마찬가지로 조직 내에 모든 자원이 정상적으로 활용되는 운영의 재개이다.

정보시스템의 재해복구를 위한 비상계획의 적용 대상이 되는 조직단위를 크게 수평적 지원 서비스(horizontal support services)와 수직적 사업단위(vertical business units)의 두 가지 측면으로 작성되는 행렬표를 이용하여 식별하는 방법이 있다[6]. 여기서 수평적 지원서비스란 주요 사업단위를 지원하는 기능으로서 자료처리, 자료통신, 음성통신, 시설 등이고, 수직적 사업단위란 조직의 사업을 실행하는 것으로, 예로써 제조업인 경우에 구매, 재고통제, 마케팅, 재무관리 등이다.

본 연구는 광역지방자치단체에서 운영하는 행정전산망의 재해복구를 위한 비상계획의 실태를 평가하고, 비상계획에 대비하기 위한 효과적인 전략 수립 방안을 제안하고자 한다.

2. 정보시스템 복구 전략

비상계획의 수립은 먼저 정보시스템의 복구 전략을 선정하고, 선택된 전략을 기초로 하여 상세한 복구 절차와 방법을 준비하는 과정을 거친다. 비상사태의 발생 이후에 정보시스템의 운영을 신속히 재개하기 위하여 대체처리시설을 확보하기 위한 전략과 데이터의 백업을 위한 기술적 대안에 대하여 살펴본다.

2.1 대체처리시설의 확보 전략

대체처리시설을 확보하기 위한 기본적인 전략은 다음의 세 가지로 구분할 수 있다[7][8]. 첫째는 정보처리 활동을 백업 싸이트(backup site)로 옮기는 것이다. 백업 싸이트는 정보시스템의 운영을 일시적으로 이전하여 정보처리 활동을 수행할 수 있도록 제반 설비와 장비가 구비된 장소이다. 여기에는 두 조직이 전산센터를 공동으로 이용하고자 하는 상호 협약(reciprocal agreement)을 채결하는 방법, 자체적으로 핫 싸이트(hot site)를 보유하는 방법, 그리고 상용 서비스를 제공하는 업체의 핫 싸이트를 이용하는 방법이 있다. 두 번째 전략은 전산센터를 운영할 장비는 없이 공간만을 제공하는 콜드 싸이트(cold site)를 이용하는 것이다. 장비를 주문하고 설치하여 운영을 재개하는데 보통 10일에서 14일이 소요됨으로 정보처리 활동의 재개에 상당한 시간이 필요하다. 따라서 업무재개에 긴급성이 없는 경우에만 선택될 수 있는 전략이며, 보통 잘 활용되지는 않는다. 세 번째 전략은 손상된 전산센터를 복구할 때까지 기다리는 것이다. 어떤 전략을 선택하는지는 업무 수행이 정보시스템에 얼마나 의존하느냐에 달려있다. 백업 싸이트를 확보하는 방안에 대하여 구체적으로 살펴보면 다음

과 같다.

2.1.1 상호 협약

상호협약은 두 조직 사이에 협약을 맺어 한 조직이 재해로 인하여 정보처리 능력을 상실할 경우에 다른 조직의 전산센터를 이용하는 방법이다. 조직마다 고유의 정보처리 환경이 있으므로 상호 협약된 싸이트에서 핵심적인 응용 프로그램의 처리에 따르는 복잡성 때문에 활용 상에 많은 제약요인이 따르게 된다. 하지만, 비용의 측면이나 업무재개의 긴급성이 아주 많이 높지는 않는 경우, 또는 대체처리시설의 이용 가능성에 대하여 최고의 보증성이 요구되지 않는 경우 등 제한된 상황하에서는 상호 협약이 유용한 대안이 될 수 있다.

상호 협약은 두 조직간에 정보처리시설을 서로 지원하겠다는 의정서를 교환함으로써 성립한다. 협약서에는 지원 수준, 백업 처리에 이용되는 정보시스템의 구성, 지원 방법, 비용 보상 등에 관한 내용이 포함되어야 한다. 상호 협약의 체결 대상으로는 동일 지역에 위치한 조직, 동일 업종에 있는 조직, 그리고 동일 기관의 다른 부서가 있다. 동일 지역의 조직과의 협약은 지리적인 이점으로 인하여 작업을 수행하기 편리하며, 동일 업종의 조직과의 협약은 업무 수행 방식의 유사성이 높기 때문에 지원을 받기 편리한 점이 있다. 동일 기관의 내부 부서간의 상호 협약은 최대한의 복구 업무 지원을 기대할 수 있다.

2.1.2 자체 보유 핫 싸이트

비상사태의 발생 시에 핵심적인 응용 프로그램을 처리할 수 있도록 제2의 전산센터를 자체적으로 보유하는 전략이다. 이러한 백업 센터는 비상사태가 발생할 때까지 유휴 상태로 있는 것이 아니라, 필요한 경우 핵심적인 응용 프로그램을 수용할 수 있는 처리 능력을 갖춘 전산센터로서 평상시에는 응용 프로그램의 개발이나 테스트와 같은 통상적인 업무를 수행한다.

자체 보유의 백업 싸이트는 기술적인 측면에서는 최선의 대안이지만, 가장 많이 비용이 소요된다. 하드웨어와 소프트웨어의 호환성에 대한 문제를 사전에 통제할 수 있고, 네트워크의 구성에 있어서도 조직 고유의 필요성에 부응할 수 있도록 설계할 수 있으며, 백업 싸이트에 이미 운영 요원이 배치되어 있으므로 복구 작업이 진행되는 동안에 인력의 재배치에 관련된 제반 문제를 최소화할 수 있는 점들이 다른 대안과 비교하여 장점으로 대두된다. 또한, 테스트의 수행에도 다른 대안보다 훨씬 유리하다. 자체 보유의 백업 싸이트는 여러 가지 기술적인 문제의 해결에 있어서 이상적인 대안이기는 하나, 추가적인 인력과 장비 및 설비의 구비에 따른 비용 상승을 초래하기 때문에 소수의 조직만이 이를 채택하고 있다.

2.1.3 상용 핫 싸이트

상용 핫 싸이트는 완전한 가동이 즉각적으로 가능한 전산센터를 구비하여 비상사태의 발생 시에 조직의 중요한 응용 프로그램을 처리할 수 있는 서비스를 업체에 의해서 상업적인 목적으로 제공되는 시설이다. 계약은 재해의 발생 이전에 성립되어야 하며, 핫 싸이트 제공자는 일반적으로 재해의 발생 이후에 핫 싸이트의 이용에 대한 교섭에 응하지 않는다.

상용 핫 싸이트는 다른 대안에 비해서 몇 가지 장점을 가지고 있다. 첫째, 상용 핫 싸이트는 백업용으로만 이용되는 전용 시설로서 고객의 업무 복구에 전적으로 이용되며, 고객의 복구계획의 테스트 장소로도 유용하게 활용된다. 이와 관련하여, 상용 핫 싸이트의 이용 계약에는 일반적으로 전산센터 복구계획의

테스트를 위하여 일정한 시간동안 자유롭게 시설을 이용할 수 있는 권한이 포함된다. 이것은 전산센터 복구계획의 유효성을 검증하는데 필수적인 요소이며, 또한 비상계획의 절차와 방법에 대하여 신입직원을 교육하고 훈련하는 좋은 기회로 활용된다. 마지막으로, 상용 핫 싸이트는 자체 보유 핫 싸이트에 비해서 사분의 일 정도의 비용으로 대체처리시설의 확보가 가능함으로 비용 면에서 유리하다.

상용 핫 싸이트를 선택할 때에는 다음의 몇 가지 요소를 고려해야 한다[7]. 우선 고려해야 할 점은 핵심 응용 프로그램을 처리하기 위한 하드웨어 구성을 식별하여 허용 가능한 최소한의 시스템의 구성(minimum acceptable configuration)을 결정하여, 이러한 구성을 제공할 수 있는 업체를 선정해야 한다. 복구계획 수립의 초기 단계에서 백업 싸이트에서 처리되는 응용 프로그램을 식별하고, 이를 지원하기 위한 시스템 구성을 결정하여 허용 가능한 최소 시스템 구성을 식별한다.

두 번째는 접근 권한(right of access)이다. 싸이트가 사용 중이거나 여러 고객이 영향을 받을 수 있는 광범위한 지역에 영향을 미치는 재해가 발생했을 때 핫 싸이트의 사용 권한을 보장받을 수 있는지는 중요한 문제이다. 일반적으로는 선입 선지원 (first-come first-served) 방식으로 서비스가 제공된다. 서비스 제공 업체에 따라서는 복수의 장소에 핫 싸이트를 운영하기도 한다. 업체를 선정할 때에는 계약된 싸이트가 다른 고객에 의해 선점되었을 경우에 대체 싸이트의 마련과 지원 방안에 대하여 면밀하게 검토하여야 한다.

세 번째는 서비스 제공 업체의 신뢰성이다. 핫 싸이트의 신속한 이용 가능 여부, 고객 지원의 적극성, 싸이트에 설치된 장비 및 설비의 적절한 유지보수 등 지금까지의 고객지원 기록을 검토하여 평가한다.

네 번째는 비용이다. 비용의 산정에는 월간 또는 연간 계약금, 핫 싸이트 이용 요청비 (declaration fee), 복구 업무 수행 기간 동안의 일일 사용료, 특수 장비 설치료 등이 포함된다. 마지막으로 전산센터 복구계획의 수립 및 유지보수, 데이터 복구 및 네트워크 분석, 테스트 등에 관련된 컨설팅과 지원과 같은 추가적인 서비스의 제공 여부도 업체 선정에서 고려되는 사항이다.

2.2 데이터 백업 방법

정보시스템 비상계획에서 가장 중요한 요소는 데이터의 복구이다. 데이터 복구는 핵심 데이터를 백업하고, 원격지 저장장소에 보관되는 백업 데이터를 주기적으로 순환시키며, 복구에 필요한 데이터를 즉각 확보할 수 있도록 준비하는 활동들이 포함된다. 백업된 데이터는 원격지에 위치한 백업 데이터 저장장소에 보관하여야 하는데, 이는 전산센터에 재해가 발생하여도 데이터는 손상이 없도록 하기 위함이다.

백업 대상이 되는 데이터는 시스템 소프트웨어와 유틸리티, 응용 소프트웨어, 데이터베이스, 디스크에 저장된 프로덕션 데이터, 트랜잭션 로그 파일 등이 있으며, 이 밖에 테이프에만 저장되는 데이터 파일, 개발중인 응용 프로그램, 최종 사용자에게 할당된 디스크 드라이브 등이 필요에 따라 백업된다. 백업 대상이 데이터와 백업 주기를 식별하는 책임은 데이터의 종류에 따라 다르다. 시스템 소프트웨어와 유틸리티는 시스템 소프트웨어 관리자가 담당하고, 데이터베이스 파일은 데이터베이스 관리자가 담당하며, 기타 데이터 파일은 데이터의 소유자가 책임진다.

디스크 드라이브의 백업에는 다음의 몇 가지 방법이 이용된다[9][10].

- 전체 백업 (full-volume backup): 디스크 전체를 복사하는 방법으로, 다른 방법들

보다는 더 많은 처리시간을 필요로 하나 관리하기가 쉽고 오류가 발생할 가능성이 적다. 보통 백업 처리에 필요한 시간을 충분히 확보할 수 있는 주말에 실시한다.

- 부분 백업 (incremental backup): 이전 백업 이후에 변경된 파일만을 백업하는 방법으로, 전체 백업보다는 처리시간이 덜 필요한 방법이다. 이 방법은 보통 전체 백업과 연계하여 이용된다. 데이터의 복구절차는 먼저 재해의 발생 이전 주말에 만들어진 전체 백업을 시스템에 복사하고, 전체 백업 이후에 변경된 파일은 부분 백업에서 복구한다.
- 데이터베이스 백업: 전체 백업과 유사한 방법으로 데이터베이스 파일을 복사하는 방법이다. 차이점은 근래의 분산처리 환경에서 데이터베이스 파일이 하나 이상의 디스크 드라이브에 존재하고 있다는 점이다. 따라서 데이터베이스의 백업은 오프라인 상태에서 데이터베이스의 모든 요소가 동시에 백업될 수 있도록 하여야 한다.
- 데이터 셋 백업 (data set backup): 특정한 응용 프로그램과 비활성 (inactive) 파일을 백업하는데 이용되는 방법이다. 디스크 공간을 차지하는 비활성 파일을 테이프에 백업하여 보관하고 필요할 때 사용한다.

하나의 백업본 만을 원격지에 보관하는 것은 바람직하지 않다. 백업이 원격지로 운반 도중에 파손될 수도 있고, 보관상의 문제점으로 인하여 손상될 수도 있으며, 소프트웨어의 에러로 인하여 데이터 복구에 실패할 수도 있다. 따라서 백업은 최소한 3세대를 유지하는 것이 바람직하다[11].

원격지에 보관된 백업을 이용하여 데이터 파일을 재구축하는 절차가 너무 많은 시간을 필요로 하여 효과적이지 못하다고 판단되면 전자 저장소(electronic vaulting)를 이용하는 방안이 있다[12]. 전자 저장소는 세 가지 형태가 있다.

- 온라인 테이프 저장소(online tape vaulting): 백업 데이터를 통신선로를 통하여 원격지 보관 장소에 전송하는 방법이다. 즉, 전산센터에서 테이프 백업을 실행하면 로컬 테이프 드라이브에 기록하는 것이 아니라 통신선로로 연결된 원격지에 위치한 저장소에 있는 테이프 드라이브에 저장된다. 이 방법은 테이프를 원격지의 보관장소로 운반하는 절차를 생략할 수 있는 장점이 있으나, 높은 대역폭을 가진 통신선로를 확보하여야 함으로 비용이 많이 든다는 단점이 있다.
- 원격 트랜잭션 기록(remote transaction journaling): 이 방법은 DBMS에 이용되는 것 (즉, 마지막 백업을 복구하고 DBMS 로그를 재처리하여 데이터 파일을 복구하는 방법)과 동일한 로깅 절차를 이용한다. 전산센터에서 만들어지는 로그 이외에 원격지에서도 동일한 로그를 생성하여 파일을 재구축하는데 필요한 시간을 단축하고 재해에 의해서 손상되는 정보의 양을 줄이는 효과를 가진다.
- 쉐도우 데이터베이스 (database shadowing): 데이터베이스를 갱신할 때 로그를 생성하고 데이터베이스의 복본을 바로 원격지의 전산기로 보내는 방법이다.
- 전자 저장소를 이용하는 방안은 데이터 파일을 재구축하는데 필요한 시간을 많이 단축하여 주기는 하지만, 많은 비용이 필요하기 때문에 짧은 시간 내에 운영을 재개할 필요가 있는 경우에 고려되는 방안이다.

3. 행정전산망의 현황과 비상계획 관련 지침

행정전산망의 발전단계는 행정업무의 정보화에 따라 〈표 1〉과 같이 도입단계('60년대), 조성단계('70년대), 확충단계('80년대), 발전단계('90년대), 그리고 성숙단계(2000년대)로 구분할 수 있다[13][14]. 도입단계에는 1967년에 조사통계국에 IBM1401, '68년에 육군경리단에 UNIVAC 9300이 도입되면서 각종 통계 및 보고서의 전산처리가 시작되었다. 정보화기반 조성단계에서는 1974년에 총무처 정부전자계산소가 행정전산화 추진체계가 조성되었고, 1979년에 행정업무전산화추진에 관한 규정이 제정된 이후에, 정부차원에서 최초로 행정전산화 5개년 계획('78년-'82년)에 의해서 각종 통계, 인사, 급여, 연금, 출입국관리 등의 업무가 전산화되었다.

정보화기반 확충단계에는 1986년에 전산망 보급확장과 이용촉진에 관한 법률이 제정되었고, 제1차 행정전산망사업('87년-'91년)이 추진되어서, 주민, 부동산, 자동차, 고용, 통관관리 등 6대 우선 업무를 중점적으로 개발하였다. 정보화 발전기에는 제2차 행정전산망사업('92년-'96년)이 추진되어 EDI 통관자동화, 국세정보통합관리, 토지종합전산망, 여권민원전산망 등 11개 업무를 개발하였다. 또한, 1995년에 정보화촉진기본법이 제정되었고, 1996년에 정보화 촉진기본계획이 수립되어 전자정부구현 등 10대 과제를 추진하게 되었다. 이에 따라서 전자정부구현을 위한 행정정보화촉진 시행계획이 수립되어서 행정정보공동이용, 전자문서시스템, 열린 정부 서비스 등의 사업을 추진하고 있다.

〈표 1〉 행정정보화의 발전단계별 특성

특성 \ 단계	도입단계	조성단계	확충단계	발전단계	성숙단계
정보화 목적	비용절감		업무효율화	업무처리재구축	성숙단계
정보화 목적	일괄처리	온라인처리	DB 개발	통합 DB 구축	정책정보구축
정보화 투자	하드웨어		소프트웨어	네트워크	
사용자 활용	무활용	자료처리	자료관리	PC 통신	의사결정
사용자 교육	없음	권유	정기교육	적극적	자발적
관리층 인식	무관심	표면적 관심	부분적 인식	적극적 지원	지휘/명령
관리층 활용	무활용		부분적 활용	전자결재	정책결정

현재 행정정보화는 발전단계로서, 업무처리 재구축을 위하여 통합 DB를 구축하고 네트워크에 집중 투자해서 통신망을 이용한 전자결재를 적극적으로 추진하고 한다. 행정정보화가 발전됨에 따라서 네트워크를 포함한 정보시스템에 대한 의존도는 나날이 높아지고 있다. 특히 업무지원기능만을 수행하는 것이 아니라 전자결재와 같은 정책결정에 직접적인 수단으로 활용됨에 따라서 행정망 비상계획은 행정업무의 연속성을 보장하기 위한 필수적인 요소가 되고있다. 즉, 행정전산망의 운영 중단이 장기화된다면 행정의 위기상황으로 이어질 개연성이 매우 커지고 있다.

총무처의 행정전산망 안전관리 지침('95. 3 개정)은 전산처리되는 국가정보의 유출 및 파괴를 방지하고 컴퓨터 범죄를 예방하여, 행정전산망의 안전성과 신뢰성을 확보하고 전산자료의 효율적인 관리와 운영을 도모함을 목적으로 하고 있다. 이 지침에 의해서 행정전산망을 운용하고 있는 9개시도 전산본부의 안전관

리 현황을 분석한 "행정전산망 안전관리 현황 및 분석"[15]에 의하면 행정전산망의 보안관리 실태 중에서 물리적 보안(방재설비, 출입통제 등)은 양호하지만, 논리적 보안(허가 받지 않은 자의 주전산기 접근통제, 식별 및 인증, 암호화 등)은 취약한 편이다. 또한, 관리적 보안의 측면에서는 문서화된 지침이 보다 철저하게 준수될 필요가 있고, 특히 전문성 있는 인적관리가 요망된다고 분석되었다.

〈표 2〉 행정전산망 안전관리 지침에서 재해복구를 위한 비상계획에 관한 항목

LLNL 항목	행정전산망 안전관리 지침	'95년 조사 현황
(4) 중요 자료보관	제5조(구분관리) 비밀자료, 중요전산자료, 일반자료로 구분관리, 별도의 자료보관실에 보관. 이 중 비밀자료와 중요전산자료는 별도의 자료보관실 혹은 용기에 보관해야 한다. 제19조(전산실, 자료보관실 및 통신실의 보호대책) 통제구역을 설정하고 보호대책(방재대책, 비인가자 출입통제, 이중문 설치 등)을 강구해야 한다.	비밀자료와 중요전산자료는 내화금고에 보관하고 있지만, 내화금고가 부족해서(전산본부에 1대) 일부는 캐비넷에 보관하고 있다.
(10) 주요 파일의 백업	제8조(전산자료의 안전성 확보) 전산자료의 파괴, 소실 등에 대비한 백업 등의 복구계획과 재해, 비상시 등에 대비한 소산계획 등을 수립 및 운영하여야 한다.	지역정보화 본부설치 운영조례 및 각 업무별 지침에 의해서 전산자료를 일일, 주, 월, 분기, 년 단위로 백업을 받고 있으며, 각 시도가 중요 전산자료를 상호 소산하고 있다.
(12) 백업자료의 통신절차 문서화	제29조(중요전산자료 전송대책) 통신회선을 이용하여 중요전산자료를 송수신하고자 할 때에는, 인가된 보안장비 혹은 보안프로그램(자료내용을 암호화하는 경우)을 사용하고, 통신선로 및 배전반에 대한 보호대책을 강구해야 한다.	보안프로그램 사용은 안기부 승인사항이고, 지방전산본부에는 송수신용 보안프로그램이 없다.
(14) 백업시스템 복구계획에서 암호화 통제	제10조(입력) 3항 및 4항 - 중요전산자료를 주전산기(혹은 개인용 컴퓨터)에 입력할 때, 필요한 경우 인가된 장비 및 보안 프로그램을 적용하여 암호화하여야 한다.	암호화 프로그램은 안기부 승인사항으로 실제로 암호화한 경우는 한 건도 없다.

LLNL(Lawrence Livermore National Laboratory) 체크리스트[16]에서 백업과 복구에 관한 74개 항목 중 가장 핵심적인 14개 항목은 (1) 비상시 공급업자 설비이용에 관한 계약, (2) 백업장소의 설비 시험, (3) 백업장소의 특수설비, (4) 중요 자료보관, (5) 재해복구계획의 문서화, (6) 비상연락망, (7) 직원들의 교차훈련, (8) 최고경영자의 비상계획에 대한 인식, (9) 비상시 복구훈련, (10) 주요 파일의 백업, (11) 정량적 위험분석, (12) 백업자료의 통신절차 문서화, (13) 비상발전기 설치, (14) 백업시스템의 복구계획에서 암호화 통제 등이다. 행정전산망 안전관리지침 중에서 특히 재해복구를 위한 비상계획에 관한 사항(즉, 전산망의 운영 중단을 복구하는 과정에 관한 사항)을 LLNL 체크리스트 항목과 비교하면, 행정전산

망 안전관리 지침과 관련된 항목은 〈표 2〉에 나타난 바와 같이 (4), (10), (12), (14)이다.

4. 행정전산망의 재해복구를 위한 비상계획 현황분석

4.1 분석 방법

행정전산망의 비상계획에 관련한 실태를 분석하기 위하여 광역지방자치단체의 정보시스템 운영부서를 대상으로 설문 조사를 수행하였다. 설문지는 전산망의 생존력을 나타내는 백업과 복구에 관한 14개 항목으로 구성되어 있다. 이것은 LLNL 체크리스트 전체 857개 항목 중에서 백업과 복구에 관한 74개 항목 중 14개 항목(5점 척도 중에서 가장 중요시한 항목들)을 선택하였다[17]. 설문지는 16개 광역지방자치단체의 정보통신 관련 담당관실의 담당 과장/계장 급이 작성하도록 하였다. '예' 라고 답한 경우에는, 기존 설치된 보안대책에 대한 구체적인 사항을 기술하도록 하였고, '아니오' 라고 답한 경우에도 백업 및 복구에 관한 계획으로만 수립된 것은 참고로 기술하도록 했다.

4.2 분석 결과

4.2.1 비상시 공급업자 설비이용에 관한 계약

비상시 데이터 처리 활동이 신속하게 시스템 공급업자의 장비나 설비 등을 활용하여 수행되도록 계약되어 있어야 한다. 현재 행정전산망 지역전산시스템 유지보수 시, 공급업자가 주요 부품을 항시 확보하여 유지보수에 응하도록 계약서 상에 명기되어 있다. 행정전산망의 광역지방자치단체가 운영하는 정보시스템은 방대해서 주전산기, 통신시설, LAN 등 대체 시스템 확보하기는 어렵다. 각 시스템은 2대 이상의 서버로 연결해서 운영하고 있고, 장애발생 시에 fault tolerant 기능을 수행하고 있다. 그러나, 국산 주전산기가 노후화되어 있고, 단종된 것은 대체장비를 확보하기 어렵다. 무엇보다도 지방재정이 열악하므로, 국가차원의 백업시스템 체계를 확립할 필요가 있다.

4.2.2 백업장소의 설비 시험

데이터 처리 활동을 백업장소로 옮겨 수행하게될 때, 이 과정이 순조롭게 적시에 이루어질 수 있도록 사용중인 애플리케이션들과 시스템 소프트웨어에 관련하여 모든 백업 설비들은 적어도 2-3개월에 한번 정도는 테스트해야 한다. 그러나, 각 광역지방자치단계가 운영하는 행정전산망을 위한 별도의 백업장소가 없다. 국가차원의 백업시스템 체계를 구축해야하고, 이곳의 모든 백업 설비들이 적어도 분기별로 테스트되어야 한다.

4.2.3 백업장소의 특수설비

주 데이터 처리 지역에서 특별히 주문 제작된 또는 구입하기 힘든 장비가 사용되고있다면, 이들 장비가 백업지역에도 역시 설치되어 있어야 한다. 그러나, 행정전산망을 위한 별도의 백업장소가 없다. 국가차원의 백업시스템에는 백업을 위한 특수 설비(예로서, 실시간 재해복구 설비)가 구비되어야 한다.

4.2.4 중요 자료보관

중요 서류뿐만 아니라 중요한 파일이나 소프트웨어가 있는 테이프나 디스크가 안전한 외부 시설에 보관되어 있어야 한다. 현재 행정전산망의 중요 전산자료 및 소프트웨어를 매월 1회 내화금고에 보관하고 있으며, 매 분기마다 타 광역지방자치단체와 교환보관하고 있다.

인천의 경우에는 전산자료만 내화금고에 보

관하고 있다.

4.2.5 재해복구계획의 문서화

공식적으로 문서화된(formal written) 재난 복구 계획이 존재해서, 그것이 최소한 6개월마다 모두 테스트되어야 한다. 그러나, 행정전산망을 위한 재해복구계획이 문서화되어 있지 않다.

4.2.6 비상연락망

비상사태 시에 연락할 수 있는 인원의 명단이 준비되어 있고, 필요로 하는 사람들에게 분배되어야 한다. 현재 비상연락망 체계가 구축되어 있으며, 각 업무담당자 별로 유지보수요원의 연락망도 숙지하여 필요시 상시 비상소집이 가능하다. 비상연락명단에는 공급사의 A/S 직원 연락처도 포함되어 있다.

4.2.7 직원들의 교차훈련

어떤 중요한 직원이 가용하지 않은 경우를 대비해서, 백업될 수 있도록 직원들간에 교차훈련(cross-trained)을 실시해야 한다. 현재 행정전산망에서는 업무별 담당자를 정, 부 또는 팀제로 운영하고 있으며, 담당업무를 6-12개월 단위로 순환보직을 실시하고 있다. 각 시스템 담당자간 업무순환은 물론 합동근무를 실시하고 있다.

4.2.8 최고 행정관리자의 비상계획에 대한 인식

데이터 처리센터의 사용이 불가능할 경우에 예상되는 손실크기(손실액)를 최고경영자가 인식하고 있어서, 재해복구계획의 준비 및 유지관리를 위해서 충분한 자원을 할당하고 있어야 한다. 그러나, 현재 행정전산망에서는 최고 행정관리자가 중요성은 인식하고 있으나, 재해복구계획에 의해서 충분한 자원을 할당하지 못하고 있다. 단지 유지보수계약에 의해서 관리하고, 백업지침에 따라서 백업을 실시하고 있을 뿐이다.

4.2.9 비상시 복구훈련

비상사태와 재해 복구 절차가 직원들에게 훈련되어야 한다. 현재 행정전산망에서는 업무처리별 지침에 의거해서 백업을 실시하고 있다. 업무처리별 지침에 의거해서 백업을 포함한 재해복구 절차에 대한 문서화 지침에 의한 훈련을 실시해야 한다.

4.2.10 주요 파일의 백업

모든 중요한 파일, 데이터베이스, 그리고, 소프트웨어가 백업되고 규칙적으로 순환되어야 한다. 현재 행정전산망을 운영하는 광역지방자치단체에서는 지역정보화 본부설치 운영조례 및 각 업무별 지침에 의해서, 전산자료를 일일, 주, 월, 분기, 년 단위로 백업을 받고 있으며, 각 시도가 중요 전산자료를 상호 소산(부산은 대구에, 광주는 전남에 소산)하고 있다. 주전산기 내부의 자체 백업기능(fault tolerant 기능)을 활용하고 있다. 소산자료를 각 시도가 상호 소산할 것이 아니라 중앙부처 차원에서 한 곳에 모아 일괄 관리할 필요가 있다.

4.2.11 정량적 위험분석

정량적 위험분석이 다양한 백업 및 복구 통제에 대한 투자를 정당화하기 위하여 수행되어야 한다. 그러나, 행정전산망에서는 정량적 위험분석을 실시하지 못하고 있다.

4.2.12 백업자료의 통신절차 문서화

통신망을 통하여 공식적(formal)인 백업 데이터를 교환하는 방식에 대하여 통신 계획 및 절차가 문서화되고 검증 및 시험되어야 한다. 그러나, 행정전산망에서는 자료량이 방대하여 통신망을 통한 데이터 복구가 오히려 많은 시간이 소요되므로 고려하지 않고 있다. 송수신용 보안프로그램은 관계기관과 협의해서 중앙부처 차원에서 승인을 얻어야 한다.

4.2.13 비상발전기 설치

정전 시에도 계속적으로 전력을 공급하여 중요한 응용시스템이 작동할 수 있도록 비상발전기가 설치되어 운영되어야 한다. 현재 행정전산망에서는 전산실 내부 전원은 UPS시설을 이용하고(전남의 경우, 12kw 1시간 무정전 전원공급장치 설치), 정전 시에는 본청사의 비상발전기를 가동할 수 있다.

4.2.14 백업시스템의 복구계획에서 암호화 통제

백업시스템으로 이행된 후에도, 패스워드와 같은 시스템접근통제의 중요한 기능이 제대로 작동되도록 복구절차계획 안에 암호화 같은 통제들에 대한 계획이 명백히 기술되어 있어야 한다. 그러나, 행정전산망에는 암호화와 같은 통제는 물론 재해복구계획이 문서화되어 있지 않다. 암호화 프로그램에 대해서는 행정기관의 장이 관계기관의 협조 및 승인을 얻어 비밀자료 및 중요 전산자료의 보관을 위해 암호화 통제를 해야 한다.

5. 광역지방자치단체의 행정전산망 복구전략 수립 방안

2장에서 살펴본 대체처리시설의 확보 전략 중에서 지방단체 행정전산망의 현실과 비용 효과성을 고려할 때 상호 협약이 바람직한 전략이라고 본다. 즉, 광역지방자치단체가 행정자치부라는 동일한 상급기관의 통제를 받기 때문에 국가적인 차원에서 비상계획을 수립하고자 하는 정책이 뒷받침된다면 상호 협약의 형태로 인근 지방단체의 전산시설을 비상시에 활용할 수 있을 것이다. 또한, 지방단체의 정보시스템이 유사 업무를 취급함으로 상호 협약을 추진하는데 장점으로 작용한다. 상호 협약이 유용한 전략으로 유지되기 위해서는 몇 가지 전제조건이 필요하다[7]. 우선 각 지방단체의 하드웨어가 호환성이 유지되어야 한다. 또한, 온라인 시스템을 수용할 수 있는 통신기반이 마련되어야 한다. 오늘날의 정보시스템은 클라이언트/서버를 기반으로 하는 분산시스템이 주류를 이루고 있다. 상호 협약을 맺은 상대방 단체에 충분한 네트워크 수용 능력이 없다면 협약 자체의 유용성은 크게 감소할 것이다. 세 번째는 테스트에 관한 사항이다.

상호 협약된 전산센터에서 테스트를 수행하는 것은 상당히 어렵다. 상대방 전산센터의 작업 스케줄에 맞추어야 할뿐 아니라 테스트 방법과 범위에도 상당한 제약이 따르게 된다. 마지막으로 규정상의 문제인데, 전산센터 복구계획의 유용성을 최대한 보장하기 위해서는 매우 엄격한 내용의 상호 협약이 필요하다. 즉, 서로의 전산센터를 충분히 활용할 수 있어야 한다. 대부분의 단체의 정보시스템은 자체의 정보처리 요구에 부응하여 구축됨으로 처리능력의 여유가 많지 않다. 따라서 상호 협약에 의해서 제공할 수 있는 정보처리 능력은 상당히 제한적일 수밖에 없다.

이상의 전략은 기존의 전산센터를 가급적 활용하는 단기적인 해결책이다. 장기적으로는 행정전산망에서 처리되는 정보의 가용성에 대한 중요도가 한층 더 높아지게 될 것임으로

실시간 백업 방안을 고려하여야 할 것이며, 기존의 전산센터와는 별도로 백업센터를 마련하는 방안을 수립할 필요가 있다.

6. 결 론

행정전산망의 재해복구를 위해서는 무엇보다도 국가차원의 백업시스템 체계를 구축해야 하고, 이곳의 모든 백업 설비들이 적어도 분기별로 테스트되어야 한다. 행정전산망의 재해복구계획이 문서화되어 있어서, 이러한 계획에 필요한 자원을 할당하고, 정량적 위험분석을 실시해야 한다. 또한, 행정기관의 장은 관계기관의 협조 및 승인을 얻어 비밀자료 및 중요 전산자료의 보관을 위해 암호화 통제를 하여야 할 것이다.

행정전산망의 조직적 특성상 체크리스트 항목 중에서 규정화된 부분은 비교적 잘 지켜지고 있었다. 따라서, 규정의 개선을 위하여 재해복구를 위한 비상계획과 관련된 LLNL 체크리스트 14개 항목 중에서 8개 항목((1) 비상시 공급업자 설비이용에 관한 계약, (2) 백업장소의 설비 시험, (3) 백업장소의 특수설비, (5) 재해복구계획의 문서화, (6) 비상연락망, (7) 직원들의 교차훈련, (8) 최고경영자의 비상계획에 대한 인식, (9) 비상시 복구훈련, (11) 정량적 위험분석, (13) 비상발전기 설치)도 행정전산망 안전관리 지침에 명시적으로 추가할 필요가 있다.

기존의 행정전산망 안전관리 지침에서는 재해복구를 위한 비상계획이 핵심적인 업무의 계속적인 운영이라는 관점에서 출발하지 않고, 시스템 운영관점에서 복구와 백업만을 부분적으로 강조하고 있다. 그 결과 전산본부는 복구되었으나 정작 필요한 업무는 재 가동되지 않는 오류를 범할 수 있다. 즉, 전산망 재해복구를 위한 비상계획이 전산센터의 직원에 의해 수행되기 때문에, 전산센터만을 복구하는데 중점을 두고 있지 뿐, 필요한 행정조직의 프로세스나 기능 단위의 복구에 관한 절차는 포함되지 않았다. 따라서 앞으로는 응용시스템과 최종 사용자의 요구사항을 포함하는 업무 지속성 관리(business continuity management)의 관점에서 비상계획의 수립이 필요하다.

참고문헌

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

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

[3] Leo A. Wrobel, Disaster Recovery Planning for Municipalities and Government, Premiere Network Services, Inc, 1995.

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

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

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

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

[8] Jon W. Toigo, Disaster Recovery Planning, Yourdon Press, 1989.

[9] Don Williamson, Tape Backup for Network, Datapro, 5055, June 1994.

[10] Michel Kabay, Backups and Data Integrity, Datapro, 5882, October 1996.

[11] 김종기, "정보시스템 장애에 대비한 비상계획을 세우자," 경영과 컴퓨터, 1996년 5월, pp.301-307.

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

[13] 총무처, 전자정부의 비젼과 전략, 1997. 12.

[14] 총무처, 행정정보화촉진시행계획, 1997. 2.

[15] 한국전산원, 행정전산망 안전관리 현황 및 분석, 1995. 12.

[16] C. Wood, W. Bank, S. Guarro, A. Garcia, V. Hampel, E. Viktor, and H. Sartorio, Computer Security: A Comprehensive Controls Checklist, John Wiley & Sons, 1987.

[17] 김종석, 정보시스템 취약성 평가: 체크리스트 접근방법, 광운대학교 경영학석사 학위논문, 1994.

□ 著者紹介

김 기 윤

1976년 고려대학교 (공학사)
1979년 고려대학교 (경영학 석사)
1985년 고려대학교 (경영학 박사)
1980년 ~현재 광운대학교 경영학과 교수

※ 주관심분야: 위험관리, 보안관리, 성과관리

□ 著者紹介

김 종 기

1987년 부산대학교 경영학과 (학사)
1988년 미국 아칸소 주립대학교 (경영학 석사)
1992년 미국 미시시피 주립대학교 (경영학 박사)
1993년 3월 ~ 1998년 12월 국방정보체계연구소 선임연구원
1999년 3월 ~ 현재 부산대학교 경영학부 조교수

※ 주관심분야: 정보보안 위험관리, 비상계획, 정보시스템 보안 평가

김 정 덕

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 부교수

※ 주관심분야: 정보보호관리, 시스템감사, 전자상거래, 정보시스템의 전략적 응용

□ 著者紹介

이 경 석

1978년 숭실대학교(전산학 학사)
1981년 성균관대학교(전산학 석사)
1986년 프랑스 파리 7 대학교 암호이론 전공(박사)
1983년 10월 ~ 1986년 12월 ITODYS(Paris 7 대학연구소) 연구원
1978년 3월 ~ 현재 산업연구원 전산정보실장

※ 주관심분야 : 암호이론, 인증시스템, 정보보안관리, 암호기술 표준화