기업의 재해복구 대책 방안에 대한 연구

김재경*, 정윤수**, 오충식***, 김재성****

A Study on the Policy for Disaster Recovery of Company

JaeKyeong Kim*, Yoon-Su Jeong, ChungShick Oh***, JaeSung Kim****

요 약 최근 정보화의 진전에 따라 기업에서 업무의 정보시스템 의존도는 점점 심화되고 있으며, 국지전, 테러, 기상이변, 대규모 자연재난 등 재난위험으로부터 중요 IT자원의 보호가 필수적이다. 본 연구에서는 국내외 동향 및 선진 유사기관 사례 분석을 통하여 기업 환경에서 사용하고 있는 중요 IT자원을 재난으로부터 보호하기 위한 종합적인 대응 방안 현황을 분석한다. 특히, 본 논문은 재난으로부터 기업 정보자원을 보호하고, 신속하고 체계적인 복구 및 운영연속성 전략 수립을 수립함으로써 기업의 재해복구 종합 정책 수립과 운영연속성 구축시 활용할 수 있도록 한다.

주제어 : 기업, 재해복구, 정책

Abstract Recently, the rate of dependence on information system in company is increase through domestic and international trends with the cases of developed similar institutions. In this paper, we analysis current state of company that protect company information resources from disaster, rapid and systematic recovery and business continuity strategic planning. Especially, proposed model was designed. disaster emergency response capacity to enhance disaster preparedness simulation training for standardized measures were established and maintained. In addition, operational continuity, building on the methodology to meet the international standard methodology is presented.

Key Words : Company, Disaster Recovery, Policy

1. 서 론

최근, 기업이 추진하고 있는 정보화사업이 확산됨에 따라 다수의 정보시스템이 기업에 도입되고 이를 통해 내부 업무프로세스 및 대외서비스 등을 정보시스템을 통해 수행하고 있다[1-4]. 최근까지 지속·확장되고 있는 정보시스템의 고도화는 업무의 정보시스템 의존도를 더욱 심화시키고 있으며 만약 기업의 정보시스템이 중단되는 사태가 발생한다면 기업은 기업 전체의 업무가 마비될 수 있는 위험한 상황이 발생한다.

기업은 9·11 테러 사태 이전까지만 해도 재해재난에 대한 정보시스템 대비책이 극히 미약한 실정이었다. 그러나 국지전, 테러, 기상이변, 대규모 자연재난 등 재난위험으로부터 각종 국내·외 사고 사례가 발생하면서 이에 대한 대비책의 마련은 선택 사항이 아니라 필수 사항으로 자리 매김하게 되었으며, 중요 IT자원의 보호가 필수적이다[5-10]. 대표적인 사례로 지난 2001년에 발생한 미국의 대규모 테러사건과 최근 2011년 사이버테러에 의한 농협 전산시스템의 마비는 국가 및 기업의 주요 정보시스템의 안전성 확보문제가 주요 정책과제로 대두되게 되었다.

기업은 2008년 “재해경감을 위한 기업의 자율활동 지원에 관한 법률” 이 제정 되었으나 자연/재해로 그 범위를 한정되어 있고 IT분야의 재해복구(DR)에 대해서는 규정이 없어 일부 해외 수출기업을 중심으로 영국의 BCI의 기업연속성계획 인증을 준비하고 있다[11-13]. 대기업

*한국과학기술정보연구원 정보화전략실, 선임연구원
**목원대학교 정보통신공학과 조교수
***한국과학기술정보연구원 정보화전략실, 책임연구원
****한국과학기술정보연구원 정보화전략실, 실장 : 교신저자
논문접수: 2012년 11월 20일, 1차 수정을 거쳐, 심사완료: 2012년 12월 23일

을 중심으로 자율적으로 중요 업무시스템과 데이터에 대한 백업과 복구 그리고 재해복구센터를 운영하고 있고 최근에는 그룹사를 중심으로 통합전산센터와 구축과 연계하여 재해복구센터를 추진 중에 있다[14].

본 논문에서는 국내외 동향 조사·분석 및 유사기관 사례 분석을 통해 기업의 중요 IT자원의 재난복구를 위한 기업의 현황을 분석한다. 본 논문에서는 방안은 재난복구센터의 구축과 백업 시스템 운영체계의 수립과정의 산출물을 통하여 유지관리를 평가하여 기업의 재난관리 체계와 핵심리스크 지표를 제시한다.

이 논문의 구성은 다음과 같다. 2장에서는 기업의 재해복구 전략 및 재해복구 대책과 관련된 국내외 기술동향에 대해서 알아본다. 3장에서는 기업의 재해복구를 위한 대응 방안에 대해서 제시하고, 4장에서는 비상체계에 따른 모의훈련 및 재해 복구를 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 기업의 재해복구 전략

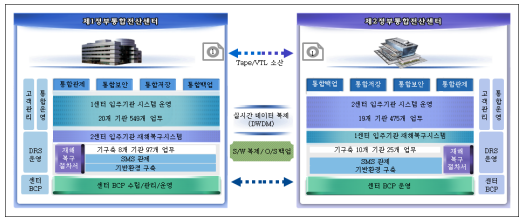
기업의 IT 전산 재해에 따른 대책을 수립하기 위해서는 우선 재해 복구범위와 복구소요 시간을 정의하여야 한다[1]. 재배 복구범위는 기업이 재해시 어느 정도의 복구가 우선적으로 이루어져야 기업이 운영되는가에 대한 기준을 정하는 것을 의미하며 복구소요 시간은 전산재해로부터 복구시간까지 소요되는 시간으로 얼마나 빠르게 정보시스템을 복구하는가를 의미한다[6,11,14].

기업이 재해복구체제를 구축하기 위한 방법은 크게 3가지로 구분된다[10,12]. 첫째, 현재 업무 및 영업을 위하여 수행 및 처리되는 모든 데이터는 실시간으로 백업 센터에 이중화하고 영업을 할 수 있는 장소와의 네트워크 접속 역시 이중화하여 시스템을 복구하는 방법, 둘째, 온라인 서비스를 위한 서브시스템에서 작성되는 거래로그만을 실시간으로 이중화하여 재해시에 전일원장을 백업테이프를 이용하여 복구하고, 그 이후에 발생한 거래를 당일 거래로그를 이용하여 재해시점 바로 이전까지 복구하는 방법. 셋째, 재해가 난 시점에서 가장 최근의 안전한 백업테이프를 이용하여 복구하는 방법이 있다.

2.2 재해복구 방법

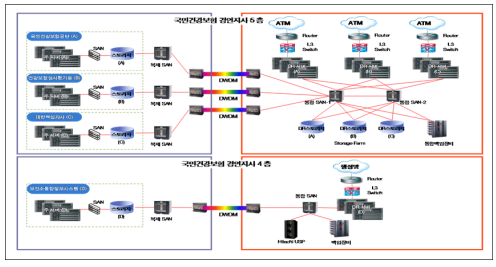
2.2.1 국내사례

정부통합전산센터는 제1센터, 제2센터에서 운영되고 있는 39개 정부 부처의 1024개 업무 중 재해복구구축대상 260개 업무시스템에 대해 재해복구시스템을 5개년도 연차별 로드맵에 의거하여 제1센터, 제2센터에 상호 교차 구축하고 재해복구대상 외 업무시스템에 대하여 백업인프라 확충을 통해 데이터 유지보수를 실시한다[14].



[그림 1] 정부통합전산센터 개요도

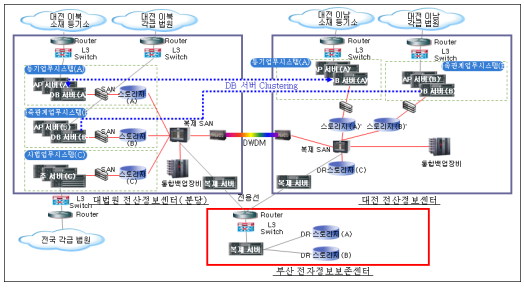
정부통합전산센터는 전자정부 31대 과제의 일환으로 통합 운영되고 있는 39개 정부부처의 핵심업무시스템을 지진, 화재, 홍수, 전쟁 등 각종 재해로부터 정보자원을 안정적으로 보존하고 단 시일 내 복구 가동할 수 있도록 재해에 대한 적극적인 대응체계를 구축하였다.
공동재해복구센터는 보건복지가족부 산하 4개 기관(건강보험관리공단, 건강보험심사평가원, 대한적십자사, 공공보건의료정보화)의 핵심업무시스템에 대한 재해복구시스템을 공동재해복구센터에 구축함으로써 기반시설, 인력, 장비 등을 공동 활용할 수 있어 초기 구축비용과 운영비용을 대폭 절감하고, 기술력을 공유한다[7].



[그림 2] 보건복지가족 공동재해복구센터 개요도

대법원 전산정보센터는 대법원의 3대 기간 업무시스템

(사법업무시스템, 등기업무시스템, 가족관계업무시스템)의 전산자원을 관리하는 사법부 통합전산센터로서 분당 주 센터를 2008년도 신축하였으며 대전전산정보센터와 상호백업 구성 및 제3센터(부산전자정보보존센터)에 데이터 변동 분을 일일 복제한다.



[그림 3] 대법원 전산정보센터 개요도

2.2.2 국외사례

국방엔터프라이즈컴퓨팅센터는 SMC(System Management Center)와 하부의 지역센터(Detachment)로 구성되어 있다. SMC는 재정/회계(Defense Finance and Accounting Service), 미해병대(United State Marine Corps), 해군, 인사(Defense Integrated Military Human Resources System), 군수(Defense Logistic Agency)를 지원하는 기능을 갖추고 있다[1].

연방준비은행(Federal Reserve Bank)는 연방준비제도(Federal Reserve System)에 따라 전국을 총12개 구역으로 나누고 각 구역마다 연방준비은행(Federal Reserve Bank)을 두어 해당 구역의 중앙은행으로서의 역할을 수행케 하고 있다.

연방저당권협회(Federal National Mortgage Association)는 워싱턴주에 본사를 두고 버지니아주에 백업센터를 두어 운영하고 있다. 외부 프로세스를 중심으로 복구시간을 실시간, 24시간, 3일, 5일 등으로 나누어 업무영향도 분석을 실시하여 손실로 인한 영향력을 분류하고, 전체 프로세스 중 10%에 해당하는 프로세스를 즉시 복구할 수 있는 체제를 구축하였다.

캘리포니아주정부의 비상서비스담당국(Office of Emergency Service)는 비상사태 시 주정부의 주요 기능을 수행하고 재해복구를 담당한다. 주정부는 각종 재해복구 및 방재업무, 재해복구 프로세스 등을 수행한다. 주요 기간시스템의 복구, 기능 백업 등을 유지하고 있으며 3개의 지역에 EOC(Emergency of Center)를 운영하여 센터간 상호백업을 실시하고 있다[2].

스위스 중앙은행은 취리히에 위치한 전산센터에서 모든 주 업무(회계, 지급결제 및 통계 등)를 관장하며 재해대비를 위하여 수도 베른에 백업센터를 운영하고 있다. 베른 백업센터는 취리히로부터 약 130Km 떨어진 지역에 위치하고 있으며 평상시에는 개발 및 테스트용으로 활용된다. 회계 및 통계 시스템은 2000년까지 IBM 메인프레임 환경에서 가동되었으나 IBM AIX환경으로의 전환작업을 2001년에 완료하였다.

프랑스 중앙은행은 Paris에 위치한 CETI와 Marne-la-Vallee에 위치한 CIMV 및 Paris로부터 약 350Km떨어진 Poitiers에 위치한 CEP가 있다. 3개의 센터에서 모든 주 업무(회계, 지급결제, TARGET 등)를 관장하고, 파업 등으로 인해 회계 및 지급결제 업무 등이 중단될 경우를 대비하여 파리의 주센터에서 5Km떨어진 곳에 위치한 지역에 백업센터를 두어 아웃소싱을 이용한 독자적 운영 및 관리를 하고 있다.

3. 기업의 재해 복구 현황 분석

이 절에서는 현재 기업이 운영하고 있는 전산망의 재해복구를 위한 효율적인 기업의 재해복구 현황을 분석한다.

3.1 기업의 재해복구 전략

재해의 정의와 관련하여 사전적 의미를 벗어나 정보시스템을 기반으로 하는 업무에 영향을 미치는 재해에 주안점을 두는 관점에서 광의의 재해는 다음과 같은 정의될 수 있다. J.W.Togo, Disaster Recovery Plannng : Strateges for Protectng Critcal Informaton, 2nd Ed.). 즉, 위의 정의에서는 업무에 영향을 미치는 정보시스템 중단사태를 모두 재해라고 통칭하고 있다.

〈표 1〉 재해 vs. 장애

구분	재해	장애
원인의 발생 위치	정보기술기반외부	정보기술기반내부
예방 및 통제	불가능	가능
정보기술 기반의 손상규모	한Site 전체	Site 내에서 부분적
대응 조직의 수준	전사적 수준	정보시스템 관리부서 수준
시스템복원 예상 소요시간	중·장기 수일 이상	단기수시간

정보시스템의 장애에 관한 광의의 개념은 정보시스템의 정상적인 운영을 방해하는 자연 재해, 시스템 장애와 기반구조 장애 (혹은 운영 장애와 설비 장애 등)를 모두 포함한다. 광의의 개념은 “정보시스템에 직·간접적으로 영향을 미치는 모든 요인들을 포함한다.”와 같이 정의하고 있어, 광의의 개념에서 볼 때에는 재해와 장애의 개념에는 차이를 두기 어렵다. 이에 따라, 동 지침에서는 협의의 개념으로서의 장애를 다음과 같이 정의하고 있다.

정보기술서비스관리의 통제 가능성 관점에서 협의의 장애 개념으로서, 통제 불가능한 재해(자연재해와 인적재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적 장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능저하, 오류, 고장. 즉, 정보시스템 장애관리지침에서는, 협의의 장애의 개념에서는 광의의 개념에서 포함한 자연 재해를 제외하고 직접적으로 정보시스템에 영향을 미치는 요인들 즉, 시스템 장애와 기반구조장애(혹은 운영 장애와 설비 장애 등)와 같은 요인들만을 포함하여, 정보시스템의 장애에 관한 광의와 협의의 개념을 그 직접적인 통제가능성으로 나누고 있다.

3.2 기업의 재해복구 전략

기업의 BCP 체계 수립을 위한 주요업무 및 자원 현황, 관련 법제도 등을 분석하기 위한 절차 및 체계를 수립하면 표 2와 같다. 현황분석은 사전준비, 조사계획수립, 인터뷰조사 및 업무 프로세스 분석 단계 등을 거쳐 기업의 현황을 종합적으로 분석하여 시사점 및 주요이슈를 도출한다. 현황분석 주요 절차 및 방법은 기업과 관련된 자료 및 선행사업 산출물 등의 내용 분석(자원정보 조사템플릿 활용), 주요업무 프로세스 및 요구사항 도출을 위한 분석, 내부협의 및 브레인스토밍 실시 등의 절차를 제시한다.

3.3 기업의 재해대비 현황 분석

본 논문에서는 기업의 재해대비 현황 분석을 현재 운영되고 있는 기업을 대상으로 재해위험도 및 재해복구 대비 현황을 분석하여 재해 복구 시스템 구축을 위한 재해복구 수준을 판별한다.

3.3.1 조사 개요

재해위험요소 분석은 재해 발생 가능성 현황을 분석하고 평가하여 취약 요인 도출하고 물리적 환경 요인 평가를 통해 향후 재해복구센터의 입지정보 제공 및 부문별 공통 취약 요인에 대한 대처 방안 제시와 분석 관점(지역, 규모)별 평가에 의한 조사 기관별 위험요소 제시한다.

위험 요소는 소재 위치별 환경 요인, 설비 현황 및 관리 절차와 입지에 따른 재해 발생 가능성과 재해복구 대비현황에 따른 재해 대처 가능성, 재해 위험 수준을 평가한다.

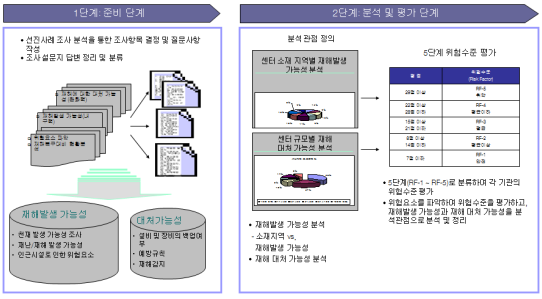
3.3.2 위험요소 분석절차

재해 위험요소 분석은 천재 발생 가능성 조사, 재난/재해 발생 가능성, 인근시설로 인한 위험요소의 재해 위

〈표 2〉 현황분석 절차

사전준비	현황분석	인터뷰조사	현황분석	요구사항도출
· BCP 사업수행범위 확인 – 목적 및 대상 – 수행범위 · 자료수집 및 분석 – 표준운영지침 – 표준운영절차 – 규정 – 비상대비계획서 – 조직 및 인력 구성 – ISP 보고서 – 기업환경 자료 ·손실데이터/통계자료	·현황조사계획수립 – 조사목적 – 조사항목 · 인터뷰계획 수립 – 인터뷰 대상 – 인터뷰 일정 – 인터뷰 시트 개발 – 자원정보조사템플릿 개발 · 현황조사 팀 구성 – 업무분장 – 역할 및 책임 분담	·업무담당자 인터뷰 – 보안운영 – 기획 – 서버운영 – 시설/인프라 – 통신망운영 ·인터뷰 결과 정리 및 검토 – 주요내용 공유 – 추가요청 자료 파악	· 기업운영환경 – 목표 – 재난관련 법 – 비상대비계획 현황 · 주요자원 현황 – 조직/인적자원 – 주요 업무 프로세스 – 운영시스템 – 기반환경 – 중요자료	·종합분석 – 분석내용 정리 – 통계분석 ·분석결과 검토 ·시사점 및 이슈도출

험요소와 설비 및 장비의 백업여부, 예방규칙, 재해감지 등 재해 대처 수준을 평가하여 위험요소를 파악하여 위험수준을 평가하고, 재해발생 가능성과 재해 대처 가능성을 분석관점으로 분석 및 정리 한다.



[그림 4] 위험요소 분석 절차

3.3.3 재해위험요소 분석 방법 및 기준

재해위험요소 분석 방법은 크게 재해위험요소 분석 도구를 사용하는 방법과 설문 문항을 통해 분석하는 방법 2가지가 있다.

① 재해위험요소 분석 도구

재해위험요소 분석 도구는 IBM 재해복구서비스(BRCS: Business Resilience & Continuity Services)팀에서 전세계적으로 전산센터의 물리적 환경을 설문조사를 통해 평가하는 도구로서 '재해발생 가능성'과 '재해에 대한 대처 가능성' 부문으로 구성되며 DB화된 재해 관련 통계를 근거로 문항 별 가중치를 적용한다.

② 설문 문항 구성

설문 문항 구성은 재해발생 가능성의 잠재적 인근 위험시설(10 문항), 자연 위협요소(9 문항), 시설/설비 위협요소(6 문항), 재해대처 가능성의 재해 발생 가능성 완화요소(8 문항)으로 구성하고 있다.

4. 평 가

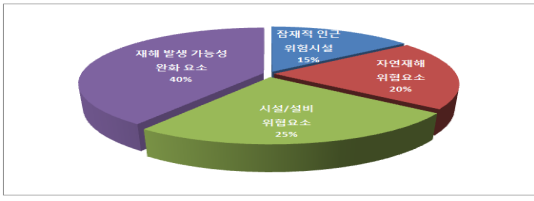
이 절에서는 기업의 정보시스템 재해위험요소의 평가 결과를 분석한다.

4.1 재해위험요소 평가

재해위험요소의 평가 항목은 재해위험요소와 재해대처가능성이며, 재해위험요소는 잠재적, 인근 위험시설, 자연재해위협요소, 시설/설비 위협요소 등이며 재해대처 가능성은 재해 발생 가능성 완화 요소로 평가하였다. 표 3은 재해위험요소 평가를 설문지를 통해 수집된 결과를 종합하여 평가 결과를 도출하였다. 표 3에서 재해위험요소의 평가 평점은 각 평가 영역을 25점으로 평가하여 총점을 100점으로 평가하고 있다.

〈표 3〉 재해위험요소 평가

구분	평가 영역	평점
재해위험요소	잠재적 인근 위험시설	12
	자연재해위협요소	16
	시설/설비 위협요소	20
	소계	48
재해대처 가능성	재해 발생 가능성 완화 요소	32
	소계	32
종합 평가 결과		16



[그림 5] 재해위험요소 분석

표 3의 재해위험요소를 분석한 그림 5의 재해위험요소의 분석 결과는 재해위험요소가 48점으로 비교적 높게 평가 되었으나 재해발생 가능성 완화요소가 32점으로 낮게 평가되어 종합평가 결과의 평점이 16점으로 평균 수준의 평가 결과가 나타났다. 이 같은 평가 결과는 현재 위험요소를 낮추어 경쟁력 있는 운영환경 확보가 필요하다.

4.2 재해 대비 준비율

현재 운영되고 있는 정보시스템의 재해복구 준비율을 분석하여 재해복구시스템 구축을 위한 재해복구 수준을 판별한다.

기업의 정보시스템 재해 준비율 평가결과 표 4처럼 재해복구 전략수립 부문 20점으로 일부 재해복구 전략수립은 되어있으나 재해복구체계 및 계획 그리고 재해복구를 위한 유지관리 절차에 대해서는 수립되어 있지 않아 재해복구 시스템 구축을 위한 계획수립이 필요하다.

〈표 4〉 재해 준비율

평가 구분	평점	비고
유지/관리 체계	20	일부 전략수립
재해복구계획	0	없음
재해복구체계	0	없음
재해복구 전략	20	없음
종합평가	20	

5. 결 론

정보화 진전에 따른 업무의 정보시스템 의존도가 심화되면서 국지전, 테러, 기상이변, 대규모 자연재난 등 재난위험으로부터 중요 IT자원의 보호가 필수적이다. 그러나 현재 기업들은 재난이 발생할 경우 기업 정보자원을 보호하고, 신속하고 체계적인 복구 및 운영할 수 있는 체계적인 복구준비가 되어 있지 않아 기업에 재난관 관련된 문제가 발생할 경우 체계적인 복구가 어려운 상황이다. 본 논문에서는 재해복구 종합 정책을 위하여 국내외 기관의 연구 동향 분석을 통해 기업의 IT자원에 대한 재해복구 현황을 분석하여 기업에 재해가 발생할 경우 신속하게 재해를 복구할 수 있는 내용을 다루었다. 향후 연구에서는 재해/재난 시 기업의 업무 서비스 연속성을 확보하기 위하여 재해복구시스템을 구축하고 이에 따른 업무영향분석(BIA)과 재해복구시스템 모델을 설계할 계획이다.

참 고 문 헌

[1] NFPA 1600:2004, Standard on disaster/emergency management and business continuity programs, National Fire Protection Association.

[2] INS 24001:2007, Security and continuity management systems . Requirements and guidance for use, Standards Institution of Israel.

[3] Business Continuity Guideline, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[4] 정보시스템 재해복구지침, 정보통신부, 2005.12. pp.15-16.

[5] 공공기관 정보시스템을 위한 비상계획 및 재해복구에 관한 지침서, 한국정보통신기술협회, 2000. 03. 28.

[6] 다기관통합전산센터의 재해복구체계 고도화 및 자동화 시스템 구축을 위한 선행연구, 한국전산원, 2003. 09.

[7] 국내외 재난관련 표준화 동향, TTA Journal, 2008.

[8] 정보시스템 재해복구 지침, 한국정보화 진흥원, 2009.

[9] 'ISO/TC223' 재난관리 기술위원회의 표준화 현황, 기술표준원.

[10] 김진환, 2002, Business Continuity Plan을 통한 중소기업형 재해복구 시스템의 구현 및 운영방안, 강원대학교 공학석사학위논문.

[11] 재해복구 전략 수립을 위한 5가지 제안, 시만텍코리아.

[12] 기업측면 재난관리 대책방안, 삼성웹진, 2007.

[13] 재난 관리 시스템 표준화 및 표준 활용방안 연구보고서, 한국기술표준원.

[14] 정부통합전산센터 재해복구시스템 모의훈련 및 유지관리 지침.

[15] 정병채, 2011, 한국 재난관리의 운영체계에 관한 연구, 한양대학교.

김 재 경

- 2005년 2월: 광운대학교 컴퓨터과학과(석사)
  2011년 3월~현재: 한국과학기술정보연구원기술원
- 관심분야: 정보보안, 개인정보보호, 포렌식
- E-Mail: kjk@kisti.re.kr

정 윤 수

- 2000년 2월: 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월: 충북대학교 대학원 전자계산학 박사
- 2009년 8월~2012년 2월: 한남대학교 산업기술연구소 전임연구원
- 2012년 3월~현재: 목원대학교 정보통신공학과 조교수
- 관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail: bukmunro@gmail.com

오 충 식

- 2009년 2월: 충북대학교 컴퓨터공학과 박사수료
- 2004년 2월: 충북대학교 전자계산학과 이학석사
- 1986년 3월~현재: 한국과학기술정보연구원 책임연구원
- 관심분야: 보안, USN, 개인정보보호, 재난관리
- E-Mail: ocs@kisti.re.kr

김 재 성

- 1999년 2월: 포항공과대학교 산업공학과석사
- 2003년 2월: 포항공과대학교 산업공학과 박사
- 2003년 3월~현재: 한국과학기술정보연구원 선임연구원
- 관심분야: 정보화, 슈퍼컴퓨터
- E-Mail : jaesungkim@kisti.re.kr