경영정보학연구
제8권 제2호
1998년 9월

정보시스템의 위험도 분석에 관한 연구: 통합적인 분석 틀을 중심으로

김 영 걸*, 이 종 만**, 이 재 남**

Risk Analysis for Information Systems: An Integrative Framework

Kim, Young-Gul, Lee, Jong-Man, Lee, Jae-Nam

This study attempts to draw a blueprint of risk analysis for Information Systems (IS). We introduce two main variables for measuring IS risk - business-impact intensity and IS-vulnerability index - through the investigation of information characteristics, business processes and human-related factors. IS-vulnerability index consists of two factors such as degree of openness and degree of preparedness to the threats. Based on these factors, we built two integrative frameworks for risk analysis and management: One is a conceptual framework to enhance the understandability of IS risk itself; the other is an integrative framework to improve the managerial insight of overall IS risk. We then conducted a field study to empirically validate the proposed framework using a structural equations modeling method. We found that IS maturity and business-impact intensity were positively correlated to degree of openness to the threats, while IS maturity was negatively correlated to degree of preparedness to the threats.

* 한국과학기술원 테크노경영대학원 부교수
** LG-EDS 시스템

Ⅰ. 서 론

최근 급격한 경영환경의 변화와 무한 경쟁 구도에 직면하고 있는 많은 기업들은 정보기술의 도입을 통하여 새로운 돌파구를 모색하고 있다. 정보기술의 활용을 통해 경쟁우위를 확보하기 위한 기업들의 이러한 노력은 조직과 정보기술의 관계를 더욱 밀착시켰으며, 결국 정보시스템이 기업내에서 더욱 중요한 위치를 점하게 되는 계기가 되었다.

그러나 이 과정에서 각 기업들은 다음과 같은 문제에 직면하게 되었다. 첫째는 기업이 정보기술에 대한 전략적/운용적 의존도가 높아지면서 정보 자산의 손실이 기업 활동에 직접적인 영향을 미치게 되었다는 것이다. 따라서 이에 대한 체계적인 대비가 필요하게 되었다. 두번째 문제는 새로운 정보 기술들의 출현에도 불구하고 이에 대한 관리 능력이 부족하다는 것이다. 즉, 사용자 중심의 전산화와 분산컴퓨팅 환경의 확산으로 관리 영역이 확대되었음에도 불구하고 정보시스템 관리자들의 성향은 여전히 기존의 해법 만을 고집하고 있다. 하지만, 해커나 바이러스와 같은 신규 위협들도 자연재해처럼 치명적인 손실을 초래할 수 있다는 것을 인식해야만 한다.

최근 국내의 정보시스템 범죄나 정보 유출 사건들은 정보화 사회의 역기능으로써 기업에게 많은 위협을 주고 있다. 특히 최근에 두드러진 현상으로 컴퓨터 네트워크의 확대는 자유로운 정보의 교환이라는 정보화 사회의 이점은 있지만, 이를 통한 정보시스템의 위협은 증가하게 되었고 결과적으로 기업의 정보시스템 위험관리에 대한 필요성이 대두되었다. 그러나 대부분의 기업들은 이에 대한 체계적인 대책보다는 부분적인 하드웨어 또는 소프트웨어의 도입을 통해 해결하려는 경향이 있다. 더군다나 다른 경쟁기업이나 타 업종에서 성공한 기업의 보안 설비 및 대책을 그대로 도입하기도 한다. 이러한 경향은 기업의 문화, 환경 및 전산수준 등과 같은 상황적 요인을 고려하지 않기 때문에 효율적인 위험관리를 기대하기란 쉽지 않다. 결국, 효과적인 정보시스템의 위험관리는 기업이 이에 대한 중요성을 인식하는 것에서부터 시작되어야만 하는 것이다.

이러한 문제의식을 전제로 하여 본 연구에서는 정보시스템에 대한 제반 위험을 산출하는 변수들을 도출하고, 이를 기반으로 위험에 대한 종합적인 분석 틀을 개발하여 정보시스템 위험에 대한 개념적 이해를 돕고자 한다. 다음 장에서는 정보시스템의 위험에 대한 기존 연구들을 살펴보고, 3장에서는 문헌연구를 기반으로 정보시스템의 위험 뿐만 아니라 조직 차원에서의 위험을 포함한 통합적인 분석 틀을 제안하며, 4장에서는 연구모형과 가설을 제시한다. 5장은 연구방법을 소개하고 6장에서는 제안한 위험분석의 통합 모형을 설문조사와 구조방정식 모형을 이용하여 검증하는 과정을 다룬다. 마지막으로, 7장에서는 본 연구의 결론 및 향후 연구과제에 대하여 논의하고자 한다.

Ⅱ. 문헌 연구

정보기술의 환경적 특성과 해결방안 관점에서 재난 및 위험관리와 관련된 선행 연구들을 <표 1>과 같이 분류하였다. 첫번째는 대형컴퓨터를 중심으로 한 대규모 데이터 센터의 백업 및 복구 활동에 대한 선행연구 들이다[Kahane, Neumann and Tapiero, 1988; Post and Diltz, 1986]. 이 연구들은 주로 백업 데이터 존재의 필연성과 복구를 위한 백업의 구체적인 대안들을 제시하는데 초점을 두고 있다. 따라서 전반적인 재난복구계획(Disaster Recovery Planning)과 절차로서 제반 문제를 풀려고 하였으나, 제안된 계획과 절차에 대한 검증작업의 미비로 인하여 효과성이 미흡하다는 문제를 가지고 있다[Lee and Ross, 1995; Rohde and Haskett,

1990; Wong, Monaco and Sellaro, 1994].

두번째 연구 범주는 기술적으로 문제를 해결하려고 하는 접근이다. 이들은 중앙집중식 컴퓨팅 환경 뿐 아니라 분산컴퓨팅 환경에 대해서도 실질적인 해결방안을 제시하고자 하였다[Clark and Hoffman, 1994; Moad, 1990; Rodrigues and Verissimo, 1993]. 그러나 이 연구들 역시 위협을 방어하기 위한 보안 측면의 제안들이 주를 이루고, 분산컴퓨팅 환경 하에서의 연구들은 아직 성숙되지 않은 상태에 있다는 난제를 지니고 있다.

따라서, 선행 연구의 마지막 범주인 위험관리에 대한 연구가 정보시스템의 제반 위협에 대처하기 위한 효과적인 접근 방안으로 대두되었다[Anderson, 1994; Ross, 1995; Miller and Engemann, 1996; Rainer, Snyder and Carr, 1991]. 즉 업무절차의 재구성 문제라든지, 관련된 조직 구성원에 대한 합리적인 책임부여와 체계적인 교육을 통한 관리효율의 증대 또는 효과적인 위험분석 활동을 위한 복합적 방법론의 적용 등이 경영층 및 조직 구성원의 인식 전환을 통하여 비용 대비 효과를 높일 수 있는 방안으로 간주되고 있다.

본 연구의 차원은 세번째 선행연구의 범주에 속하며, 특히 위험관리의 기초가 되는 위험분석에 중점을 두고 있다. 따라서 위험의 결과물인 재난(Disaster)이란 용어부터 자세히 살펴보도록 하겠다. 일반적으로 재난이라 하면 홍수나 태풍 등 천재지변을 의미한다. 그러나 정보시스템에 대한 새로운 위협들이 자연재해의 수준에 이를 정도로 커지고 있다. 따라서 본 연구에서는 Rohde와 Haskett[1990]의 재난에 대한 정의 - 정보시스템 운영상의 막대한 지장으로 인하여 기업경영의 존립이 위협 받는 하나의 사건 - 에 근거하여 재난을 자연재해와 인재(人災)로 재분류하고자 한다. 여기서 인재는 우발성 또는 고의성 재난(위협)을 모두 포함하고 있다.

<표 2>는 앞에서 재분류한 재난을 바탕으로 유형별 분석작업의 결과를 보여주고 있다. 이와 같은 유형별 분석작업은 인재가 가지고 있는 논리적 또는 잠재적 특성으로 인하여 자연재해에 비해 문제를 해결하는데 많은 어려움이 있음을 보여주고 있다. 따라서 합리적인 위험관리 활동은 재난에 대한 논리적인 원인을 포함하여 제반 위협에 대한 포괄적인 분석에 기초하여야 한다.

<표 1> 위험 관리에 관한 선행 연구의 분류

선행연구의 분류	정보시스템 환경	접근방향
1. 재난복구계획(DRP)	중앙 집중식 컴퓨팅 환경	재난복구
2. 기술적인 해법		
3. 위험관리 방안	분산 컴퓨팅 환경	보 안

<표 2> 재난에 대한 유형별 분석

구 분	자연 재해	인재
재난 발생 원인	물리적인 원인: (예) 화재, 지진 등	논리적인 원인: (예) 해커, 바이러스 등
재난 발생 특징	급진적	점진적
재난 발생부터 발견까지의 시간	짧다	길다
복구 절차의 특성	명확	불명확
접근 방향	재난 복구	보안

<표 3> 정보시스템 환경에 따른 분석

구 분	중앙 집중식 컴퓨팅 환경	분산 컴퓨팅 환경
자연재해 발생시 손실비용	크다	적다
인재 발생시 손실비용	적다	크다
백업 및 복구의 용이성	높다	낮다

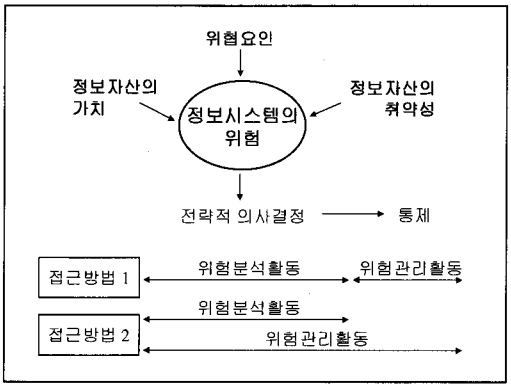
또한, <표 3>은 정보시스템 환경, 즉 중앙집중식 컴퓨팅 환경과 분산컴퓨팅 환경에 대한 분석을 보여주고 있다. 이와 같은 분석작업은 컴퓨팅 환경의 고유 특성에 따라서 재난에 대한 대비가 달라져야 한다는 것을 의미하며, 이는 결국 정보시스템의 환경적 특성에 지배되지 않는 통합적인 접근방법이 필요하다는 것을 의미하는 것이다.

Ⅲ. 정보시스템의 위험에 대한 통합적 접근

3.1 정보시스템의 위험산정 변수

<그림 1>에서 보듯이 정보시스템의 위험은 정보자산의 가치, 이에 대한 위협요인들 그리고 정보자산의 취약성으로 구성되어 있으므로, 위험분석은 정보자산의 기밀성, 무결성, 가용성 등을 저하시킬 수 있는 제반 위협들 및 그와 같은 위협들에 대한 정보자산의 취약성에 근거를 둔다. 또한 위험분석은 경영층의 전략적 의사결정에 의한 통제 메커니즘을 조직에 이행하고 유지하는 위험관리의 기초가 된다[김기윤·김정덕, 1994; Rainer, Snyder and Carr, 1991].

그러나 합리적인 위험분석 활동에는 몇 가지 어려움이 있다. 첫번째 문제는 위험이란 용어 자체의 추상성에서 기인한다. 용어의 추상성으로 인해 정확하고 계량화된 위험산정이 어렵기 때문이다. 물론 많은 연구자들이 체계적인 위험분석을 위하여 구조적 접근방법을 시도하였다.



<그림 1> 위험 분석 및 관리에 대한 개념

이 구조적 접근방법은 (1)위협 발생확률과 손실크기의 곱으로 산출되는 기대가치에 근거하는 정량적 분석방법(예: ALE, LRAM, Stochastic Dominance 등), (2)기술 변수(Descriptive Variables)에 의한 정성적 분석 방법(예: scenario, analysis, fuzzy metrics, questionnaires 등)으로 대별된다[김기윤·김정덕, 1994]. 최근에는 자동화된 도구(예: CRAMM 등)에 대한 연구도 행해지고 있다[김법진·한인구, 1996]. 정량적 분석방법이 정확한 위험산정이 가능하다는 장점은 있지만, 많은 자원이 필요하며 사용 가능한 과거자료가 부족하기 때문에 본 연구에서는 위험관리 포토폴리오의 전반적 약점을 비교적 빠르게 파악할 수 있는 정성적 위험분석 방법을 채택하고자 한다.

두번째 문제는 기업의 정보자산을 중복이나 누락 없이 완벽하게 파악하는 것이 어렵다는 것이다. 선행 연구자들은 자료의 특성이나 가치사슬에 근거하여 정보자산을 인식하는 절차를 개발하려고 노력하였다. 그럼에도 불구하고 이들 방법들은 자산 인식 주체의 불명확성과 복잡한 절차 등으로 인하여 실제 활용에는 회의적인 요인들이 많았다. 따라서 본 연구에서는 애플리케이션을 중심으로 하여 그와 관련된 정보자산을 인식하는 방법을 사용하고자 한다.

1) 위험변수 설정

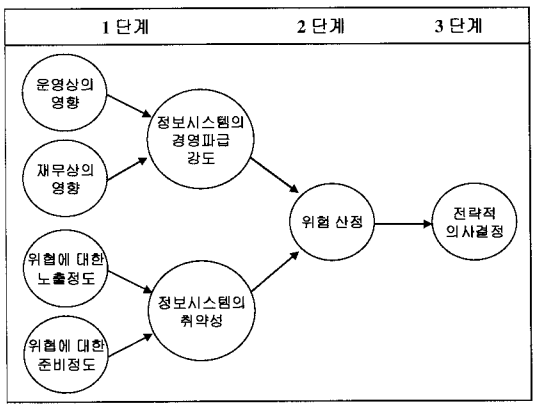
정보시스템의 위험산정 변수는 <그림 1>에서 보듯이 정보자산의 가치에 근거한 정보시스템의 경영파급 강도와 정보자산의 취약성에 근거한 정보시스템의 취약성으로 분류할 수 있다.

정보시스템의 경영파급 강도. 정보시스템의 경영파급 강도란 "정보시스템의 운영이 기업 경영상의 제반 활동 및 성과에 미치는 영향의 정도"라고 정의할 수 있다. 그러나 실제로 정보시스템이 기업경영에 미치는 영향의 정도를 측정하는 것은 매우 어렵다. 또한 그 영향을 측정하고자 노력한 선행 연구자들의 관심은 주로 재무적인 손실과 같은 유형적 요소에 집중되어 있었다. 다행히 최근 몇몇 학자들이 비재무적이며 무형적인 요인에 대해 관심을 가지기 시작했으며, 이는 본 연구의 변수 선정작업에 좋은 동기가 되었다[Drucker, 1995; Erickson, 1995; Smith and Sherwood, 1995]. 본 연구에서는 선행연구를 근거로 하여 정보시스템의 경영파급 강도를 측정하는 변수로서, (1)정보시스템의 운영상 장애가 기업활동에 미치는 영향(관리활동의 상실 정도, 노동생산성의 저하 정도, 기업 활동에 대한 장애 정도 등)과 (2)그로 인한 재무적인 손실가능성(정보자산의 손실, 제반 장애에 대한 위약금 정도 등)을 사용하고자 한다.

정보시스템의 취약성. 정보시스템 취약성이란 "재난 또는 제반 위협에 대하여 정보시스템의 취약한 수준"을 의미한다. 본 연구는 앞에서 정의한 재난을 정보시스템의 취약성을 찾아내는 시발점으로 삼았다. 재난에 대한 원인을 살펴봄으로써 정보시스템의 취약성을 (1)위협에 대한 노출정도[Banes, 1995; Lee and Ross, 1995]와 (2)위협에 대한 조직의 준비정도[김종기, 1994; Nevola, 1995; Straub, 1990; Smith, 1993]로 구분할 수 있다. 위협에 대한 노출정도는 데이터센터의 분산정도, 데이터 처리 로직의 복잡도, 신기술의 적용정도, 타 시스템과의 연계정도, 네트워크 인터페이스 정도 등으로 나타낼 수 있으며, 위협에 대한 준비 정도는 교육훈련 정도, 하드웨어 또는 소프트웨어의 사용정도, 정책(절차)의 정규화 정도, 담당자의 유무 또는 활동정도, 공급자와의 협약 정도, 문서화 정도 등을 포함하고 있다.

2) 정보시스템 위험에 대한 개념적 틀

본 연구에서 제안하는 정보시스템의 위험산정 절차는 정보시스템의 경영파급 강도와 정보시스템의 취약성을 근간으로 하고 있다. 이를 토대로 정보시스템의 제반 위험에 대한 분석과정을 크게 3단계로 구분하였다. <그림 2>에서 보듯이 1단계와 2단계에서는 정보시스템의 위험을 산정하며, 산정된 위험에 대한 대처방안의 창출은 3단계에서 이루어 진다.



<그림 2> 위험 분석의 과정

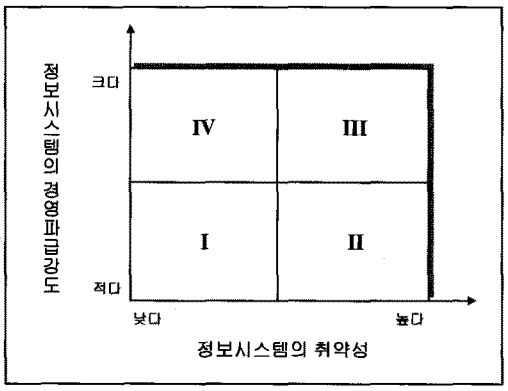
앞에서 도출된 정보시스템 위험에 대한 변수들(1단계)에 근거하여 정보시스템의 제반 위험을 다음과 같은 함수(2단계)로 정의할 수 있다.

정보시스템의 위험 = f (정보시스템의 경영파급강도, 정보시스템의 취약성)

위의 함수를 바탕으로 정보시스템 위험에 대

한 전략적 의사결정을 지원하기 위하여 <그림 3>과 같은 정보시스템 위험에 대한 개념적 분석 틀을 사용할 수 있다. <그림 3>에서의 I 방안은 정보시스템의 경영파급 강도가 매우 낮음에도 불구하고 제반 위협에 대한 준비정도는 상대적으로 큰 경우로써 제반 위험에 대하여 가장 안정한 경우이다. 이 방안은 일상생활에서 건강한 사람이 주기적으로 정기검진을 받는 것에 비유될 수 있다.

II 방안은 제반 위협에 대한 정보시스템의 취약성이 높은 반면, 정보시스템이 경영에 미치는 파급강도는 상대적으로 낮은 경우이다. 즉, 치명적이지 않은 지병을 가진 사람이 치료를 위하여 외래진료를 받는 경우처럼, 기업의 위험회피 성향에 따라 정보시스템의 취약성을 줄이려는 노력이 신축성 있게 결정될 수 있는 방안이다.



<그림 3> 정보시스템 위험에 대한 개념적 분석 틀

III 방안은 정보시스템의 취약성 뿐만 아니라 정보시스템의 경영파급 강도가 매우 높은 경우로써, 가장 먼저 제반 위험에 대한 대책을 마련해야 하는 긴급한 경우이다. 분산컴퓨팅 환경하에서 여러 부분에 걸친 기능적 업무를 처리하는 정보시스템이 이에 해당된다.

마지막으로, IV 방안은 정보시스템이 기업에 미치는 경영파급 강도가 매우 높음에도 불구하고 제반 위협에 대한 준비정도가 높아서 정보시스템의 취약성이 상대적으로 낮은 경우이다. 이 경우는 마치 일상생활에서 장래에 발생할지도 모르는 재난에 대비하여 보험에 드는 경우처럼 위험 회피도가 높은 조직에서 좀더 높은 안정성을 확보하기 위하여 각종 대책을 마련하는 경우가 될 수 있다.

3.2 조직의 위험산정 변수

정보시스템의 위험 분석에 관한 선행 연구들을 살펴보면, 정보시스템의 취약성에 영향을 미치는 변수를 (1)조직의 유형, (2)위험에 대한 관리자의 의식, (3)정보시스템 부서의 크기, (4)불확실성 회피 정도, (5)정보시스템의 성숙도, 그리고 (6)정보시스템의 경영파급 강도로 구분하고 있다. 이중에서 (1), (2), (3) 변수는 정보시스템의 취약성에 명확히 영향을 미치는 것으로 밝혀졌다[김종기, 1994]. 따라서 본 연구에서는 정보시스템 취약성과의 연관성이 불명확한 (4), (5), (6)을 바탕으로 조직 관련 변수를 설정하였다.

불확실성의 회피 정도. 위험에 대한 의사결정자의 주관적인 성향은 효용이론(Utility Theory) 또는 선호도 이론(Preference Theory)에 의하여 어느 정도 파악될 수 있다. 이 이론들은 위험산정 근거를 관련 자산의 크기와 통계적 확률치로 보고 있다. 즉, 관련 자산의 크기와 재무적 요소에 대한 일련의 값을 근거로 위험을 산정할 수 있으며, 비재무적인 변수도 위험을 나타내는 간접 지표로써 활용될 수 있다. Straub [1994]의 불확실성 회피 지수는 비재무적인 변수에 대한 예가 될 수 있다. Straub[1991]는 "불확실성 회피"를 "불확실과 애매모호함에 대한 사회 구성원들의 감지정도"라고 정의하고, 이를 측정하기 위하여 업무에 대한 스트레스 정도, 규칙 준수에 대한 성향, 장기 근속에 대한 성향을 사용하였다. 본 연구에서도 Straub[1991]가

사용한 3개의 변수를 이용하여 불확실성의 회피정도를 측정하고자 한다.

정보시스템의 성숙도. 유기체를 포함한 모든 시스템은 시간의 경과에 따라 끊임없이 변화하며 성숙하게 된다. 이러한 시스템의 매카니즘은 경영정보 분야에서 단계별 성장 이론(Stage Theory)의 모태가 되었다. Nolan과 Gibson[1974]은 기업의 전산 예산 집행에 대한 연도별 추이 곡선이 시간의 경과에 따라 S모양을 그린다고 주장하면서, 이 곡선을 4단계(차후에 6단계)로 구분하여 정보시스템의 단계별 성장 이론으로 발전시켰다[Nolan, 1979]. 또한 트랜잭션의 배치/온라인 처리와 데이터베이스 기술에 근거한 Nolan의 이론은 시간이 지나면서 정보시스템 역할의 변화와 새로운 정보기술의 출현을 계속적으로 반영함으로써 단계별 성장 이론의 완성도를 높일 수 있다[Earl, 1993; Porter, 1984; Ward, 1995]. 비록 단계별 성장이론에 대한 검증이 불충분하기는 하지만, 지금도 많은 연구에서 자주 인용되고 있는 이유는 이론이 제공하는 직감적인 통찰력 때문이다[Drury, 1983].

이와 같은 성장이론을 바탕으로 본 연구에서는 정보시스템의 계획과 개발에 대한 성숙도를 <표 4>에서와 같이 5단계로 구분하였다[Earl, 1989]. 도출된 정보시스템의 성숙도는 "설사 동일한 성숙도를 가진 기업이라 할지라도 각각의 애플리케이션 성숙도는 다른 분포를 가질 수 있다"는 것을 전제로 하고 있다. 이는 McFarlan et al.[1983]이 제시한 기술확산 단계와도 그 맥락을 같이 하는 것이다.

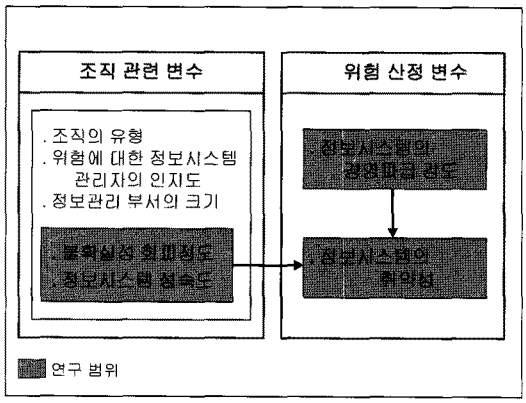
Ⅳ. 연구의 모형 및 가설의 설정

4.1 연구 모형

본 연구에서는 정보시스템의 위험분석에 대한 통합적인 틀을 제시하기 위하여 문헌 연구로 부터 조직관련 변수들과 위험산정 변수들을 도출하였다. <그림 4>는 이를 토대로 설정한 개념적인 연구 모형을 보여주고 있다. 한편 조직관점의 이슈는 위험에 대한 대처 수준에 있으므로 본 연구에서는 정보시스템의 취약성 정도를 다시 위협에 대한 노출정도와 위협에 대한 준비정도로 세분하여 구체적인 연구 범위를 설정하였다.

<표 4> 정보시스템의 계획과 개발에 대한 성숙도

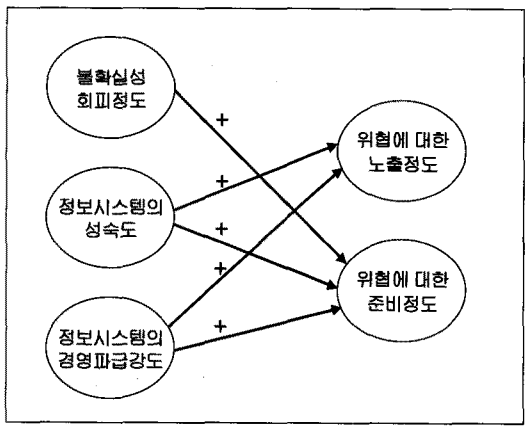
구 분	1단계	2단계	3단계	4단계	5단계
정보시스템 사용목적	기술	방법론	관리	핵심업무	전체조직
	학습	정보시스템 계획	커스터마이즈된 정보시스템 계획	신규 기회 창출	단위업무별 전략간 연계성 추구
정보시스템 계획과 통제	자유 방임	하향식 통제	상향식 통제	정보 공유	외부조직과의 표준화 추구
지향하는 방향	기술 주도	상위관리자 주도	사용자와 전산부서간 공조체제	사용자그룹 전체주도	관련부서들간 긴밀한 협조체제



<그림 4> 개념적인 연구 모델

4.2 가설의 설정

지금까지 살펴본 바와 같이 정보시스템의 취약성은 조직(또는 구성원)의 특성과 정보시스템의 환경에 의존한다[김종기, 1994]. 본 연구에서는 불확실성의 회피정도와 정보시스템의 성숙도를 정보시스템의 취약성에 영향을 미치는 조직 변수로 선정하였으며, 정보시스템의 경영파급강도를 정보시스템의 취약성에 영향을 미치는 위험산정 변수로 설정하였다. 따라서 앞에서 제시한 정보시스템의 위험에 대한 개념적 틀과 이론적 배경에 근거하여 다음과 같은 연구 가설을 제시하고자 한다<그림 5>.



<그림 5> 연구의 모형

H: 불확실성 회피 정도, 정보시스템의 성숙도, 그리고 정보시스템의 경영파급 강도는 정보시스템 취약성 정도와 상관관계가 있다.

또한, 본 연구에서는 정보시스템의 취약성 정도를 위협에 대한 노출정도와 위협에 대한 조직의 준비정도로 구분하였다. 조직측면에서는 이 두가지 요소에 대한 적절한 대응을 통하여 정보시스템에 대한 위험 관리의 효과성을 향상시킬 수 있다. 따라서 위에서 제시한 기본 가설에 대한 세부 가설로써, 첫번째는 정보시스템 취약성 정도와 불확실성 회피 정도간의 관계를, 두번째는 정보시스템 취약성 정도와 정보시스템의 성숙도간의 관계를, 마지막으로 정보시스템의 취약성 정도와 정보시스템의 경영파급 강도간의 관계를 설정하였다. 하지만 조직 또는 구성원들의 특성을 나타내는 불확실성의 회피 정도는 정보시스템이 위협에 노출되는 정도와는 무관하기 때문에 세부 가설에서 제외하였다.

H1a: 불확실성 회피 정도와 위협에 대한 준비정도는 양의 상관관계를 가진다.
H2a: 정보시스템의 성숙도와 위협에 대한 노출 정도는 양의 상관관계를 가진다.
H2b: 정보시스템의 성숙도와 위협에 대한 준비정도는 양의 상관관계를 가진다.
H3a: 정보시스템의 경영파급 강도와 위협에 대한 노출 정도는 양의 상관관계를 가진다.
H3b: 정보시스템의 경영파급 강도와 위협에 대한 준비정도는 양의 상관관계를 가진다.

V. 연구의 방법

5.1 자료 수집

본 연구는 앞에서 제시한 연구모형을 바탕으로 조직 변수와 위험 변수 간에 설정된 연구 가설들을 검증하기 위하여 국내의 상장 기업들 중에서 비교적 정보강도가 높다고 판단되는 금

융권 및 제조회사들을 주된 표본으로 추출하였다. 각 회사의 애플리케이션 운영자 또는 관리자와 인터뷰를 실시하였으며, 일부는 팩스나 전자 메일을 이용하여 자료를 조사하였다. 약 2개월에 걸친 조사결과 총 73부의 자료를 수집하였다. 그 중 3부는 자료가 불충분하여 분석에서 제외하고 최종적으로 70부를 통계처리에 사용하였다. <표 5>는 설문대상 기업 및 응답자의 일반적인 특성을 보여주고 있다.

<표 5> 설물 기업 및 응답자의 일반적 특성

구 분		빈 도	비율 (100%)
업종	제조업	43	58.9
	금융업	16	21.9
	서비스업	13	17.8
	기타	1	1.4
직위	평사원	15	20.5
	대리/계장	45	61.6
	과장/차장이상	13	17.9
합 계		73	100

5.2 연구 변수

본 연구에서는 종속변수를 위협에 대한 노출정도와 위협에 대한 준비정도로 구분하였으며, 위협에 대한 노출정도는 Lee와 Ross[1995]의 연구를, 그리고 위협에 대한 준비정도는 Nevola [1995]의 연구를 바탕으로 측정도구를 개발하였다. 한편 종속변수에 영향을 미치는 독립변수를 크게 불확실성 회피정도, 정보시스템의 성숙도, 정보시스템의 경영파급강도로 구분하였다. 불확실성 회피정도는 1991년 Straub가 제시한 변수를 그대로 사용하였으며, 정보시스템의 성숙도는 Earl[1989; 1993]과 Nolan[1979]이 제시한 단계별 성장 이론을 바탕으로 측정도구를 개발하였다. 그리고 정보시스템의 경영파급강도를 측정하기 위하여 Drucker[1995]와 Erickson[1995]이 제시한 개념을 사용하였다.

모든 변수들의 측정도구는 선행연구에서 살펴본 바와 같이 기존연구에서 이미 검증된 것

<표 6> 변수의 측정항목, 평균, 표준편차 및 신뢰도 계수

연구변수	측정항목	평균	표준편차	Cronbach Alpha
불확실성 회피정도	업무에 대한 스트레스 정도	3.41	0.99	0.66
	규칙 준수에 대한 성향 정도	3.63	0.73	
	장기 근속에 대한 성향 정도	3.67	1.30	
정보시스템 성숙도	정보시스템의 기술습득정도	2.87	0.85	0.76
	정규화된 방법론의 활용정도	2.90	0.77	
	개발 및 운영조직 간의 협조정도	3.67	0.56	
	정보시스템의 표준화 정도	3.24	0.65	
정보시스템 경영파급 강도	관리활동의 상실 정도	3.55	0.96	0.71
	노동생산성의 저하 정도	3.99	0.89	
	기업 활동에 대한 장애 정도	3.03	1.04	
	정보자산의 손실 정도	3.36	0.78	
	제반 장애에 대한 위약금 정도	3.07	1.04	
위협에 대한 노출정도	데이터 센터의 분산 정도	3.63	1.00	0.68
	데이터 처리 로직의 복잡도	3.46	0.76	
	신기술의 적용 정도	3.63	0.94	
	타 시스템과의 연계 정도	3.70	1.42	
	네트워크 인터페이스 정도	3.76	0.84	
위협에 대한 준비정도	교육훈련 정도	2.61	0.82	0.83
	하드웨어,소프트웨어 등의 사용정도	2.40	0.89	
	정책(절차)의 정규화 정도	2.69	0.91	
	담당자의 유무 또는 활동정도	3.10	0.95	
	공급자와의 협약 정도	3.07	0.69	
	문서화 정도	2.39	0.80	

을 위주로 활용하였으며, 개발되었거나 사용된 적이 없는 변수들은 관련문헌을 참조하여 새롭게 정리하였다. 본 연구에서 사용된 독립변수와 종속변수는 모두 리커트 5점척도로 측정하였다. 다항목으로 구성된 척도의 타당성을 검증하기 위하여 항목분석과 요인분석을 실시하였다. 여기서 얻어진 결과를 가지고 요인분석의 절차에 따라 집중타당성, 판별타당성 및 단일 차원성을 검사하였다. 단일차원성이 규명된 후에 Cronbach Alpha를 사용하여 각 변수의 내적 일관성을 계산하였다. <표 6>에 측정된 변수들의 평균, 표준편차 및 신뢰도 계수를 정리하였다.

5.3 자료 분석 방법: 구조방정식 모델

본 연구에서는 LISREL 7.1.6을 이용한 구조방정식 모델을 통하여 제시한 가설을 검증하였다[Joreskog and Sorbom, 1989]. 구조방정식 모델은 데이터의 공분산 및 상관관계의 구조를 분석하는 기법으로써, 추상적인 개념을 많이 다루는 심리학 등 사회과학이나 마케팅 분야에서 주로 사용되어 왔다. 구조방정식 모델이 짧은 역사에도 불구하고 특정 연구 분야에서 선호되는 이유는 추상적인 개념들에 대한 합리적인 계량화와 더불어 구성개념간 관계에 대한 직감적인 이해를 도모하는 유용성 때문이다.

수학적 모형인 구조방정식 모델을 지원하는 도구는 스칼라 방식과 매트릭스 방식이 있다. 이중에서 매트릭스 방식의 LISREL 패키지가 광범위하게 사용되고 있으며, 이는 탐색적 모형보다는 확정적 모형의 분석 작업에 특히 용이하다. LISREL을 이용한 분석 방법에는 측정 하부 모형과 구조 하부 모형을 동시에 평가하는 단일 접근법과 각 하부모형을 분리하여 접근하는 2단계 접근법이 있다[김종기, 1994]. 하지만 단일 접근법은 모형 구조에 문제가 있을 경우 해석적 혼동을 초래할 수 있기 때문에, 2단계 접근법이 좀 더 합리적이라고 말할 수 있다. 한편, LISREL은 제시된 모형의 검증을 위하여 전반적인 적합도 지수(Chi-square, Goodness-of- Fit Index, Adjusted Goodness-of-Fit Index, Root-Mean-Square-Residual)와 개념들간의 회귀계수 등을 제공해 준다[임종원, 1996].

Ⅵ. 자료 분석 및 해석

6.1 연구 모델의 전반적인 적합도

본 연구의 목적이 전체적인 모형의 검증보다는 변수들 간의 관계를 도출하는데 중점을 두고 있으므로 공분산보다는 상관관계 행렬을 이용하여 제시한 연구모형을 검증하였다[Hair et al., 1995]. <표 7>은 변수들간의 상관관계를 보여주고 있다.

처음에 제시한 구조 하부 모형의 적합도는 <표 8>에서 보듯이 만족스럽지 못했다. 따라서 본 연구에서는 이 단계 접근법에 따라서 (1)연구 모형의 설명 변수 23개를 각 요인별로 나누고, (2)구성 개념간 어떠한 구조관계도 설정하지 않은 측정 하부 모형을 구성하여 LISREL을 수행하였다. 그리고 각 변수의 추정치가 0.5 미만이거나 또는 t-값이 |2.0| 보다 작은 설명 변수들을 중심으로 수정지수와 잔차를 살펴본 후, 문제가 있다고 판단되는 3개의 측정변수(위협에 대한 노출정도에 대한 하나의 측정변수; 위협에 대한 준비정도에 대한 2개의 측정변수)를 제거하였다. <표 8>에서 보듯이 수정된 측정 하부 모형의 전반적인 적합도가 약간 향상되었다. 비록 수정된 구조 하부 모형의 적합도가 만족스럽지는 못하지만 Straub[1990]의 연구결과(GFI = .680, AGFI = .597) 보다는 높게 나타났다.

<표 7> 변수들의 상관관계 행렬

변 수	(1)	(2)	(3)	(4)	(5)
(1) 불확실성 회피정도	1.000				
(2) 정보시스템의 성숙도	-.178	1.000			
(3) 정보시스템의 경영파급강도	.022	.289**	1.000		
(4) 위협에 대한 노출정도	.126	.061	.204*	1.000	
(5) 위협에 대한 준비정도	-.101	.317***	.237**	-.009	1.000

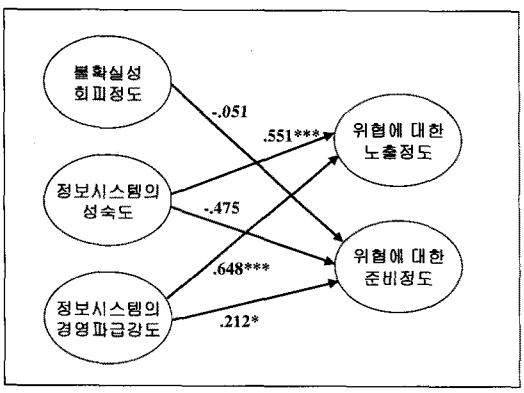
*p<0.10, **p<0.05, ***p<0.01

<표 8> 모델의 전반적인 적합도

측정치	초기 모델	수정 모델
Chi-Square (DF)	318.84(224)	205.06(164)
p-value (>= 0.05)	.000	.016
GFI (>= 0.90)	.722	.786
AGFI (>= 0.80)	.658	.725
RMSR (=< 0.05)	.122	.128

6.2 가설의 검증

정보시스템의 제반 위협에 대한 준비 정도와 조직 구성원의 불확실성 회피 정도에 대한 가설 H1a에 대한 검증 결과는 회귀계수가 -.051로 상관관계가 매우 미약하고 t-값이 -.434로 유의하지 않은 것으로 밝혀졌다.



*p<0.10, **p<0.05, ***p<0.01

<그림 6> 구조방정식 모델의 분석 결과

가설 H2a, 즉 제반 위협에 대한 노출 정도와 정보시스템 계획과 개발의 성숙도간의 관계는 <그림 6>에서 보듯이 회귀계수가 .551으로 상당한 양의 관련성이 있을 뿐 아니라, t-값이 2.415로 매우 유의적이었다. 하지만, H2b에서 제시한 가설과는 반대로, 제반 위협에 대한 준비 정도와 정보시스템의 계획과 개발 성숙도의 관계는 회귀계수가 -.475로 음의 상관관계가 있으며 t-값이 -2.667로 매우 유의적이었다.

제반 위협에 대한 노출 정도와 정보시스템의 경영파급 강도의 관계, 즉 H3a는 회귀계수가 .648로 양의 관련성이 상당히 있을 뿐 아니라 t-값이 2.976로 매우 유의적이었다. 또한, 제반 위협에 대한 준비 정도와 정보시스템의 경영파급 강도의 관계에 대한 가설 H3b도 유의적으로 조사되었다. 회귀계수는 .212로 양의 상관관계가 있으며 t-값이 1.441로 유의적이었다.

6.3 자료 해석

본 연구에서 제시한 가설들을 검증하는 과정에서 매우 흥미로운 결과가 발견되었다. 즉, 구성 개념인 정보시스템 성숙도와 정보시스템의 경영파급 강도가 제반 위협에 대한 노출정도와 양의 상관관계를 있는 반면에, 정보시스템의 성숙도와 제반 위협에 대한 준비정도는 음의 상관관계가 있다는 것이다. 이는 기업의 정보시스템 발전 방향이 네트워크를 기반으로 한 분산화를 지향하고 있는데 반하여, 정보시스템 계획과 개발의 성숙도가 높을수록 오히려 제반 위험에 대한 준비 정도는 낮아지고 있다는 것을 의미한다. 결국, 계획과 개발에 대한 정보시스템의 성숙도는 제반 위협에 대한 준비 수준과 관련이 없음을 말해주고 있는 것이다.

그렇다고 해서 각 기업들이 정보시스템에 대한 위협을 무시하거나 간과하고 있다고 볼 수는 없다. 왜냐하면 정보시스템의 경영파급 강도와 제반 위협에 대한 준비정도가 양의 상관관계를 가지고 있기 때문이다. 다시 말해, 각 기업들은 정보시스템의 경영파급 강도가 높은 정보시스템에 대하여 제반 위협에 대한 준비 수준을 높이려는 노력 대신 정보시스템에 대한 외부에서의 접근 통로 자체를 차단하는 것으로 해석할 수 있다.

Ⅶ. 결론 및 향후 연구과제

최근 들어 인터넷의 대중화와 컴퓨터 2000년 연도 표기문제(밀레니엄 버그) 등으로 인하여 정보시스템에 대한 위험관리가 새로운 연구 분야로 대두되고 있으며, 인재로 인한 위험은 점점 증가하고 있는 추세이다. 하지만, 인재로 인한 정보시스템의 위험을 정확히 분석한다는 것은 매우 어려운 일이다. 더군다나 실제 기업들의 위험관리는 재무관리와 같은 전통적인 관리 활동에 비하여 상당히 미약하다는 사실이 본 연구를 통하여 발견되었다. 이러한 연구 결과와 더불어 본 연구에서 제안한 정보시스템 위험에 대한 통합적인 시각은 기업들의 초기 위험관리 활동에 대한 투자의 중요성을 강조하고 있다. 또한, 본 연구에서는 정보시스템 위험에 대한 새로운 시각을 제시하였다. 즉, 정보시스템 자체의 위험과 더불어 업무절차와 인적요인을 변수로서 고려하였으며, 위험에 대한 이해를 도모하기 위한 개념적, 통합적인 분석 틀을 제시함으로써 위험에 대한 통찰력을 향상시키고자 하였다.

그러나 본 연구는 다음과 같은 한계를 가지고 있다. 첫번째는 자료수집을 위하여 인터뷰를 실시하였기 때문에 인터뷰 대상자의 주관적인 편견이 반영되었을 가능성이 있다는 것이다. 두번째는 본 연구에서 사용한 70개의 유효 응답자 수는 LISREL의 합리적인 요구수준을 충족시키지 못하고 있다는 것이다.

본 연구를 통하여 다음과 같은 향후의 연구 방향을 제시할 수 있다. 첫째는, 보다 합리적인 연구를 위하여 본 연구에서 제시한 상호관계 모델은 인과관계 모델로 발전시킬 수 있다. 예를 들어, 제반 위협에 대한 노출 정도를 정보시스템의 경영파급 강도의 선행변수로 설정할 수 있다. 둘째는, 본 연구는 유효 응답자 수와 인터뷰 방법 자체가 가지는 제약점으로 인해 연구결과를 일반화하는데 다소 무리가 있었다. 따라서, 본 연구에서 제시한 통합 모델에 대하여 좀더 포괄적인 연구를 수행할 필요가 있다. 마지막으로, 본 연구의 위험분석 틀을 위험관리 분야로 확장하여 적용할 수 있다. 예를 들어, 우선순위에 의한 위험관리 전략과 통제 아키텍처의 개발 등이 이에 포함될 수 있다.

〈참 고 문 헌〉

[1] 김기윤, 김정덕, "정보시스템의 위험분석과 관리," *한국경영정보학회 추계학술대회 논문집*, 1994, pp. 277-297.

[2] 김법진, *한인구, CRAMM을 이용한 정보시스템을 위한 위험분석과 관리*, 석사학위논문, 한국과학기술원 테크노경영대학원, 1996.

[3] 김종기, "정보시스템 보안의 상황적 모형," *한국경영정보학회 추계학술대회 논문집*, 1994, pp. 299-312.

[4] 임종원, *마케팅 조사 이렇게*, 법문사, 1996.

[5] Anderson, R. J., "Why Cryptosystms Fail," *Communications of the ACM*, Vol. 37, No. 11, November 1994, pp. 32-40.

[6] Clark, P. C. and Hoffman, L. J., "BITS: A Smartcard Protected Operating System," *Communications of the ACM*, Vol. 37, No. 11, 1994, pp. 66-70.

[7] David Banes, "Security and the Enterprise Network," *Intrernational Journal of Network Management*, July-August 1995, pp. 198-206.

[8] Drucker, P. F., "The Information Executives Truly Needs," *Harvard Business Review*, January-February 1995, pp. 54-62.

[9] Drury, D. H., "An Empirical Assessment of the Stages of DP Growth," *MIS Quarterly*, June 1983, pp. 59-70.

[10] Earl, M. J., "Experiences in Strategic Information Systems Planning," *MIS Quarterly*, March 1993, pp. 1-20.

[11] Erickson, J., "Integrated Risk Assessment Part One: The Methodology," *IS Audit & Control Journal*, Vol. 3, 1995, pp. 20-29.

[12] Hair, J. F., Anderson, R. E., Tatham, R. L. and Black, W. C., *Multivariate Data Analysis with Readings, 4th ed.*, Prentice-Hall, Inc. 1995.

[13] Kahane, Y., Neumann, S. and Tapiero, C. S., "Computer Backup Pools, Disaster Recovery, and Default Risk," *Communications of the ACM*, Vol. 31, No. 1, 1988, pp. 78-83.

[14] Joreskog, K. G. and Sorbom, D., *LISREL 7 Users Reference Guide*, Scientific Software, Inc., 1989.

[15] Lee, S. U. and Ross, S., "Disaster Recovery Planning for Information Systems," *Information Resources Management Journal*, Summer 1995, pp. 18-23.

[16] McFarlan, F, W., McKenney, J. L. and Pybum, P., "The Information Archipelago-plotting a Course," *Harvard Business Review*, January-February 1983, pp. 145-156.

[17] Miller, H. E. and Engemann, K. J., "A Methodology for Managing Information-Based Risk," *Information Resources Management Journal*, Spring 1996, pp. 17-24.

[18] Moad, J., "Disaster-Proof Your Data," *Datamation*, November 1990, pp. 87-93.

[19] Nevola, J. E., "How Safe is Your Data Center?," *International Journal of Network Management*, July-August 1995, pp. 185-188.

[20] Nolan, R. L., "Managing the Crisis in Data Processing," *Harvard Business Review*, Vol. 57, No. 1, January-February 1979, pp. 115-126.

[21] Nolan. R. L. and Gibson, "Managing the Four Stages of EDP Growth," *Harvard Business Review*, Vol. 52, No. 1, 1974, pp. 76-88

[22] Porter, M. E. and Millar, V. E., "How

information gives you competitive advantages," *Harvard Business Review*, 1984, pp. 149-160.

[23] Post, G. V. and Diltz, J. D., "A Stochastic Dominance Approach to Risk Analysis of Computer Systems," *MIS Quarterly*, December 1986, pp. 363-374.

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

[25] Rodrigues, L. and Verissimo, P., "Replicated Object Management using Group Technology," *IEEE*, 1993, pp. 54-61.

[26] Rohde, R. and Haskett, J., "Disaster Recovery Planning For Academic Computing Centers," *Communications of the ACM*, Vol. 33, No. 6, 1990, pp. 652-657.

[27] Ross, S. J., "Is It Security or Disaster Recovery? Who Cares?," *International Journal of Network Management*, July-August 1995, pp. 193-197.

[28] Smith, M., *Commonsense Computer Security*, McGraw-Hill Book Company, 1993.

[29] Smith, M. and Sherwood, J., "Business Continuity Planning," *Computers & Security*, Vol. 14, 1995, pp. 14-23.

[30] Straub, D. W., "Effective IS Security: An Empirical Study," *Information Systems Research*, September 1990, pp. 255-276.

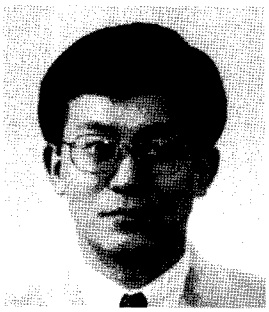
[31] Straub, D. W., "The Effect of Culture on IT Diffusion: E-Mail and FAX in Japan and the U.S.," *Information Systems Research*, March 1994, pp. 23-47.

[32] Ward, J., *Principles of Information Systems Management*, Routledge London and New York, 1995.

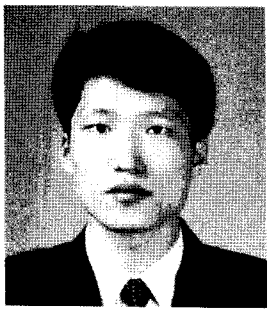
[33] Wong, B. K., Monaco, J. A. and Sellaro, C. L., "Disaster Recovery Planning: Suggestions to Top Management and Information Systems Managers," *Journal of Systems Management*, May 1994, pp. 28-33.

◈ 이 논문은 1998년 6월 8일 접수하여 1차 수정을 거쳐 1998년 8월 26일 게재확정되었습니다.

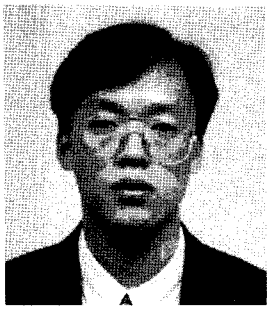
◆ 저자소개 ◆



김 영 걸 (Kim, Young-Gul)
현재 KAIST 테크노경영대학원 부교수로 재직중이다. 서울대 산업공학과 및 동 대학원을 졸업하고 미국 University of Minnesota에서 박사학위(MIS 전공)를 취득하였다. 1990년부터 3년간 미국 University of Pittsburgh의 Katz Graduate School of Business에서 조교수로 재직하였다. 주요 연구관심분야는 정보시스템 아키텍쳐, 데이타/프로세스 모델링, 지식 관리, 정보시스템 관리, 고객정보시스템 등이다.



이 종 만 (Lee, Jong-Man)
현재 LG-EDS 시스템에 재직중이다. 한양대학교 공과대학을 졸업하고 KAIST 테크노경영대학원 경영공학과에서 석사학위를 취득하였다. 주요 관심분야는 정보시스템 관리, 클라이언트-서버 컴퓨팅, Hypertext 기술, Data Mining 등이다.



이 재 남 (Lee, Jae-Nam)
현재 LG-EDS 시스템에 재직중이며 한국과학기술원 테크노경영대학원 박사과정에 있다. 성균관대학교 공과대학을 졸업하고 KAIST 테크노경영대학원 경영공학과에서 석사학위를 취득하였다. 주요 관심분야는 정보시스템 아웃소싱, 정보시스템 관리, 프로젝트 관리, 데이타/프로세스 모델링 등이다.