AHP를 이용한 정보보호투자 의사결정에 대한 연구

공 희 경* · 전 효 정** · 김 태 성***

A Study on Information Security Investment by the Analytic Hierarchy Process

Hee-Kyung Kong* · Hyo-Jung Jun** · Tae-Sung Kim***

Abstract

Recently organizations identify information security as one of essential means for gaining competitive advantage. However, they do not actively increase investment in this area because they consider spending for information security as a cost rather than an investment. This is because organizations don't have a clear understanding of information security objectives which can be achieved through investment, and they don't have criteria for alternatives which can be considered in information security investment decision-making. In this paper we propose to model the decision-making process of information security investment by the AHP (Analytic Hierarchy Process). The results will show that availability is the most important criterion for the decision of information security alternatives, and intrusion detection is the most important information security alternative. We hope that the results of this paper provide a guideline for clear decision-making in information security investment.

Keywords : Information Security Investment, Decision-making, AHP

논문접수일 : 2007년 11월 26일 논문게재확정일 : 2008년 03월 07일

※ 이 논문은 2007년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음.

* 충북대학교 경영정보학과 박사과정 수료

** 충북대학교 경영정보학과 박사과정

*** 교신저자, 충북대학교 경영정보학과 부교수, BK21 사업팀

1. 서 론

최근 기업들의 정보기술 투자비중이 지속적으로 확대되는 가운데, 정보보호는 기업 활동의 연속과 고객신뢰를 보장하는 필수요소로 그 중요성이 지속적으로 증가하고 있다. 그러나 한정된 정보기술 투자예산 중 정보보호에 대한 투자는 그 규모가 매우 작다. 우리나라기업의 정보화 대비 정보보호투자 예산 비율은 평균 약 5% 이하로 선진국인 미국 기업의 정보보호투자 비율인 10.6%의 절반 수준에 그치고 있다[한국전산원, 2006; 한국정보보호진흥원, 2003]. 이는 기업의 대표이사 등의 투자관련 의사결정자들이 정보보호의 필요성은 인식하고 있지만 정보보호에 대한 투자가 기업의 매출이나 가시적인 이익으로 연결될지에 대한 확신이 없기 때문이다. 또한 정보보호투자에 대한 효과를 사전에 객관적으로 예측할 수 있는 분석체계도 부족하다. 따라서 기업의 정보보호투자 의사결정 시 정량적 효과와 정성적 효과를 체계적으로 측정할 수 있는 평가기준의 도출이 필요하다.

기업의 정보보호투자에 대한 확신은 '정보보호 제품'의 선택에서부터 시작된다. 기업의 정보보호를 효율적으로 수행하기 위해서는 무엇보다도 경제적, 기술적 측면의 고려가 중요하다. 기업의 정보보호 현황에 적합하고, 전체적인 조직운영과 기업윤리 및 정책에 부합하면서 조직의 운영비용을 최소화할 수 있는 정보보호 제품의 선택이야말로 적정투자 수준을 결정하기 위한 기반을 제공한다. 본 논문에서는 기업이 정보보호 제품을 선택하여 투자할 때 고려해야 할 기준들을 제시하고, 적합한 정보보호 제품에는 어떠한 것들이 있는지에 대한 정보를 제공함으로써, 최적의 정보보호 제품 선택을 위한 가이드라인을 제공하고자 한다. 연구방법은 다기준 의사결정시 널리 사용되는 계층분석기법(Analytic Hierarchy Process, AHP)을 사용하여, 정보보호분야의 전문가들을 대상으로 설문조사를 실시하고 그 결과를 분석 및 제시하고자 한다.

정보보호투자의 효과에 대해서는 비교적 최근부터 연구가 시작되었다. 정보보호에 대한 사회적, 경제적 연구의 필요성에 대해 Soo Hoo [2000]는 보험 산업과 기업에서 정보보호 문제에 대한 연구의 필요성을 분석하고 효율적인 투자 규모와 효과 등에 대한 논의의 필요성을 제기하였다. Gordon and Loeb[2002]는 정보의 취약성과 잠재적 손실을 매개변수로 이용해 기업의 정보보호에 대한 최적의 투자수준을 고려하는 경제적 모델을 제시하여 기밀성, 무결성, 가용성 등의 정보보호 목표를 효율적으로 달성할 수 있도록 적합한 투자모델을 제시하였다. Cavusoglu et al.[2004a, 2004b]는 정보보호투자 시 관리자가 고려해야 할 여러 요소들을 분류하였다.

Bodin et al.[2005]의 연구에 따르면 AHP기법을 이용하여 CFO(Chief Financial Officer)를 대상으로 정보보호투자 평가안을 도출하고 정보보호관리자가 평가 측정할 수 있는 정보보호 수준을 제시하였다. 또한 Tanaka et al.[2005]는 정보보호투자와 정보보호 취약성의 관계를 일본의 e-local 정부의 실증 데이터를 바탕으로 비용효과 대비 접근방법과 내쉬균형이론을 적용하여 분석하였다.

이러한 연구에도 불구하고, 정보보호투자로 정보보호제품을 도입할 경우에 고려해야 할 평가기준과 도입효과에 대한 실무적인 연구는 이루어지지 않았다. 이를 테면, 어떠한 정보보호 제품을 왜 선정해야 하는지에 대해 실무자들이 참고할 수 있는 자료들을 찾기가 어렵다. 정보보호투자 의사결정과정에 대한 가이드라인이나, 정보보호투자의 효과를 측정할 수 있는 체계적인 방법론이 개발되어 있지 않은 것이 현실이

다. 정보보호투자 의사결정에 영향을 미치는 변수들이 열거될 뿐 어떤 기준이 어느 정도 영향을 미치는 지에 대한 분석과 검증이 이루어지지 않은 상황이다. 본 연구에서는 정보보호 제품 도입 시에 투자의사결정과정에서 고려해야 하는 평가기준을 도출하고, 도출된 평가기준을 사용하여 정보보호제품을 선정하는 과정을 AHP 기법으로 모델링하고 실증자료를 통해 수치 예를 제공하여, 실무적으로 유용하게 사용될 수 있는 평가모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 AHP 방법론을 소개해고, 정보보호투자 시 고려해야할 평가기준과 투자대안을 포함한 연구모델을 제시한다. 제 3장에서는 연구결과를 분석하고, 마지막으로 제 4장에서는 본 연구의 결론 및 시사점을 제시한다.

2. AHP 모형

2.1 계층분석기법

AHP기법은 Saaty에 의해 개발된 다기준 의사결정모델(multi-criteria decision making model)이며 의사결정 프로세스를 체계적으로 분석하고, 여러 평가항목의 가중치를 쌍별비교(pairwise comparison)에 의하여 단계적으로 도출함으로써 대안들에 대한 합리적 평가를 지원한다[Saaty, 1980]. AHP 방법론은 복잡한 의사결정 문제를 계층적으로 구조화하여 부분적으로 하나씩 단계적으로 접근하여 최종적으로 종합하는 과정을 거쳐 의사결정을 마무리한다[Saaty, 1980]. 즉, AHP는 계층(hierarchy)의 개념을 통해 의사결정에 필요한 여러 요소들을 계층화시켜 각 요소별, 요소간의 관계를 보다 상세히 논리적으로 보여준다. AHP 방법론만이 갖는 타 의사결정 방법론에 대한 고유의 특성은 일관성 비율(Consistency Ratio, CR)을 기준으로 하여 설문에 대한 응답 즉 판단 결과의 신뢰도를 측정할 수 있다는 점이다[Saaty, 1980]. 이를 통해 의사결정자의 논리적 일관성 유지 여부를 확인하고 의사결정의 합리성과 논리성을 높일 수 있게 된다. AHP 방법론의 개발자인 Saaty는 이러한 일관성비율의 값은 일반적으로 0.1(10%) 이하가 되어야 판단의 일관성이 있고 각 항목별 가중치가 의미있는 것으로 간주한다[Saaty, 1980]. 일부 사회과학 분야의 연구 조사에서는 설문 문항의 특성상 각 상·하위 기준간의 독립성 확보가 어렵다는 점을 감안하여 0.2(20%) 이내까지를 허용범위로 하고 있다[Saaty, 1980; Saaty, 1990; Saaty, 1998].

2.2 모형설정

본 연구모형 설정의 목적은 기업이 정보보호투자 시 고려해야 하는 기준과 투자대안에 대한 의사결정을 돕는 모델을 제시하는 것이다. 최적의 정보보호 제품 선택을 위한 가이드라인이 필요한 이유는 정보보호에 대한 한정된 투자 하에서 그 투자의 효용성을 최대한 높일 수 있는 방법을 제공하기 위한 것이다.

(1) 평가기준

이 절에서는 국내외의 연구에서 정의된 평가기준에 대해 고찰하고, 고려해야 할 평가 기준을 도출하고자 한다. 지금까지 정보보호투자의 효과를 분석하고 정보보호투자 시 고려해야 하는 기준에 대한 다양한 연구가 제시되어 왔다.

Blatchford[1995]는 비용(costs)과 효용(benefits)이 고객-공급자 기대심리 등을 통해 기업에게 직간접적으로 지대한 영향을 미칠 수 있음을 지적하였다. Davis[2005]는 ROSI(Return on Security Investment)를 정보보호투자에 대한 재

정적 수익의 비율로 정의하고, 운영비용의 감소와 순익의 증대를 포함하는 재정적 효용(financial benefits)과, 통제비용과 사고(incidents) 비용을 포함하는 정보보호비용(cost of security)을 이용해 측정하였다. Blatchford[1995], NIST[1996], TSO[1999], Lee[2003], Davis[2005], Bodin et al.[2005]는 적절한 보안통제를 위한 접근방법의 선택을 가능하게 해주는 컴퓨터 보안에 대한 기초자료를 제공하면서 컴퓨터 보안의 핵심으로 무결성, 가용성, 기밀성을 제시하였다. NIST[1996]는 기밀성은 비 인가된 사용자의 사적인 자료 또는 기밀 자료에 대한 접근을 막아내기 위한 요구사항이라고 정의하였다. 한편, 시기에 적절하고 내용이 정확하고 일관성이 유지된 경우 정보가 무결성을 가지는 것이라 정의하면서, 컴퓨터는 이러한 요구사항을 제대로 제공할 수 없음을 지적하였다. 이에, 컴퓨터 보안 차원에서의 무결성은 데이터 무결성과 시스템 무결성으로 나눠 살펴봐야 한다고 제시하고, 데이터 무결성은 특정한 경우 인가된 사용자에 의해서 정보나 프로그램이 변경되는 경우의 요구사항으로, 시스템 무결성은 시스템의 일관성을 유지하는 것이라고 정의하였다. 마지막으로, 가용성은 시스템의 신속한 처리·반응을 보장하기 위

〈표 1〉 연구의 평가기준 선정을 위한 문헌조사

연구자	선행연구의 평가기준	본 연구의 평가기준
Blathchford [1995]	비용(costs)	경제(제품가격)
	효용(benefits)	경제(기대매출)
	정보시스템 운영비용(cost of the controls)	경제(IS운영비용)
	기밀성(confidentiality)	기술(기밀성)
	무결성(integrity)	기술(시스템 무결성/데이터 무결성)
	가용성(availability)	기술(가용성)
	인증성(authenticity)	×
	공익성((Utility)	×
Davis[2005]	ROSI(return on security investment)	경제(기대매출)
	재정적 효용(financial benefits)	경제(기대매출)
	정보보호 비용(cost of security)	경제(제품가격)
NIST[1996]	기밀성(confidentiality)	기술(기밀성)
	데이터무결성(data integrity)	기술(데이터 무결성)
	시스템무결성(system integrity)	기술(시스템 무결성)
	가용성(availability)	기술(가용성)
Lee[2003]	가용성(availability)	기술(가용성)
	무결성(integrity)	기술(가용성)
	기밀성(confidentiality)	기술(시스템 무결성/데이터 무결성)
Bodin et al. [2005]	기밀성(confidentiality)	기술(기밀성)
	무결성(integrity)	기술(시스템 무결성/데이터 무결성)
	가용성(availability)	기술(가용성)
Cavusoglu et al. [2004b]	금전적 손실(monetary damage)	경제(제품가격)
	회사적 책임(corporate liability)	경제(기업 이미지)
	신뢰도 하락(loss of credibility)	경제(기업 이미지)

한 요구사항으로서 인가된 사용자에 대한 서비스가 거부되지 못하도록 하는 것이다. Lee[2003]은 정보보호에 대한 투자는 기술, 인력, 교육, 정책 및 컨설팅과 같은 정보자산의 가용성, 무결성, 기밀성을 보호하기 위한 것이라고 정의하였다. Lee[2003]는 기밀성은 인가된 사용자들만이 데이터베이스와 정보시스템에 접근할 수 있도록 하는 것으로, 데이터 무결성은 시스템내의 정보가 정확하고 명확하며 일관적이며, 인가된 사용자들만이 변경할 수 있음을 보장하는 것으로 정의하였다. 가용성은 시기적절한 때에 인가된 사용자가 사용 가능한 것으로 정의하였다. 한편, Bodin et al.[2005]는 AHP를 이용한 정보보호에의 투자평가를 위한 점수모델을 개발하였다. Bodin et al.[2005]는 모델에서 기밀성, 데이터 무결성, 가용성을 그 평가기준으로 설정하였으며, 가용성은 인증(authentication), 부인방지(non-repudiation), 접근성(accessibility)으로 세분화하였다. Cavusoglu et al.[2004b]는 정보보호침해로 인해 금전적 손실(monetary damage), 회사적 책임(corporate liability), 신뢰도 하락(loss of credibility)등이 발생한다고 가정하고 정보보호 담당자가 경제적 측면에서 관리할 수 있는 주요 요소를 정보보호침해 비용산정(estimation of security breach cost), 리스크 관리 기법(risk management approach), 비용 효과적 기술구성(cost effective technology), 다양한 기술구성으로부터 오는 가치(value from deployment of multiple technologies)들로 정의하였다.

본 연구모형에서는 문헌조사에서 도출한 정보보호 제품의 도입기준에 대한 여러 선정기준들을 재분류하고 중복되는 항목들을 제거하여, 이를 바탕으로 전문가를 대상으로 선정된 기준에 대해 델파이 조사를 실시하여 보다 객관적인 정보보호 제품의 도입기준을 도출하였다. 델파이 설문조사는 2006년 8월 31일 부터 2006년 9월 8일 까지 정보보호분야 관련 전문가 7명을 대상으로 문헌조사에서 도출된 정보보호 제품 도입기준에 대해 전문가들의 의견수렴을 목적으로 실시하였다. 설문에 참여한 전문가는 공공기관의 최고정보책임자 2명, 정보보호 관련기업의 최고정보보호책임자 및 최고의사결정자 4명, 정보보호 관련학과의 대학교수 1명으로 정보보호 분야의 이론적, 실무적 경험을 보유하고 있을 뿐만 아니라 정보보호 투자 의사결정에서 영향을 줄 수 있는 전문가들로 구성하였다. 이러한 델파이 조사를 통해 다음과 같은 평가기준을 도출하였다.

〈표 2〉 연구모형의 평가기준

상위 기준	하위 기준	조작적 정의
경제적 측면	제품 가격	투자규모 대비 제품 가격의 적정한 정도
	정보시스템 운영비용	정보시스템 운영비용 절감에 기여할 것으로 기대되는 정도
	기대매출	매출증가에 기여할 것으로 기대되는 정도
	기업 이미지	잠재적 자산인 기업이미지 향상에 기여할 것으로 기대되는 정도
기술적 측면	기밀성	기밀성 확보에 기여할 것으로 기대되는 정도
	데이터 무결성	데이터 무결성 확보에 기여할 것으로 기대되는 정도
	시스템 무결성	시스템 무결성 확보에 기여할 것으로 기대되는 정도
	가용성	가용성 확보에 기여할 것으로 기대되는 정도

평가기준은 크게 '경제적 측면'과 '기술적 측면' 두 가지로 범주화하였다. '경제적 측면'은 투자비용과 경제적 효과에 대한 관심의 정도로서, 일반적인 제품 및 시스템의 기업 내 도입 기준이다. 이는 비용 대비 효용으로 대표되는 제품 구매 자체에 초점을 맞춘 평가기준이다. '기술적 측면'은 정보보호 수준 제고에 대한 관심의 정도로서, 정보보호의 특성을 반영한 제품 또는 시스템 도입 기준이다. 이는, 정보보호 자체의 특성에 맞춰진 제품의 도입으로 기업이 보호하고자 하는 정보보호의 특성에 방향을 맞춘 평가기준이다.

본 연구모형에서는 '경제적 측면'의 세부기준으로 제품 가격, 정보시스템 운영비용, 기대 매출, 기업 이미지를 제시하였으며, '기술적 측면'의 세부기준으로는 기밀성, 데이터 무결성, 시스템 무결성, 가용성을 제시하였다.

(2) 평가대안

대안은 이미 시장에 상용화된 정보보호 제품들을 기준으로 하였다. 그러나, 제품 자체의 종류가 매우 다양하고 이미 시장에 상용화된 제품 위주로만 분류되어 있어, 개발은 되어 있으나 아직 기업이 사용하지 않고 있는 제품을 고려할 수 없기 때문에 각 제품들의 기술적 특성 및 보호의 대상특성 등을 기준으로 한 분류가 필요하다. 이에 적합한 정보보호 제품들의 분류를 제시하고 있는 문헌으로는 Finne[1996], NIST [2003], 국가정보원, 정보통신부[2006]이 있다.

Finne[1996]는 조직의 정보보호대책을 컴퓨터 보안, 운영보안, 도난방지, 화재방지, 수해방지, 전력배분(단전, 누전, 자기장 등), 내부·외부 위협(태업, 스파이 등), 통신보안, 비상계획, 인적 보안(채용, 통제 등), 정보보안이슈에 대한 태도, 기타 사항 등으로 분류하였으며, NIST[2003]에서

〈표 3〉 연구모형의 평가대안(정보보호 제품)

평가대안	정 의
식별 및 인증. (Identification and uthentication)	기능 : 책무성 확보와 식별 기반 접근통제를 위한 기반 형성 제품 : 생체인식, 보안 토큰, 인증프로토콜 등
접근 통제 (Access control)	기능 : 정보자원에 대한 인가된 접근만을 허가 제품 : 스마트 카드, ACL (Access Control List) 등
침입 탐지 (Intrusion detection)	기능 : 침입 모니터링 및 분석 프로세스 지원을 위한 SW 및 HW 제품 : 네트워크 기반 IDS, 호스트 기반 IDS, 침입 방지제품 등
방화벽 (Firewall)	기능 : 네트워크 간 또는 호스트와 네트워크 간의 네트워크 트래픽의 흐름을 통제하는 장치 또는 시스템 제품 : 패킷 필터 방화벽, NAT (Network Address Translation) 등
PKI (Public key infrastructure)	기능 : 문서(데이터)의 전자교환을 가능하게 해주는 암호기술 제품 : 키 보호 및 암호 모듈, 키 복구, 리포지터리 등
악성코드방지 (Malicious code protection)	기능 : 다양한 기법을 이용하여 프로그램에 내재된 악성코드 탐지 제품 : 스캐너, 취약성 모니터, 안티 바이러스, 바이러스 백신 등
취약성 분석 도구 (Vulnerability scanners)	기능 : 호스트(서버, 방화벽 등)를 검사하여 알려진 취약성을 밝힘 제품 : 네트워크 취약성 분석도구, 호스트 취약성 분석도구 등
포렌식 (Forensics)	기능 : 컴퓨터 메모리에서 삭제된 패스워드, 로그인 정보 등을 식별 제품 : 증거 보호 및 수집 도구, 분석 툴 등
데이터 무결성 도구 (Media sanitizing)	기능 : 삭제된 기밀데이터의 복구, 재설계 등을 불가능하도록 함 제품 : 겹쳐쓰기, 문서파기 기록삭제(degaussing) 등

는 식별 및 인증, 접근 통제, 침입 탐지, 방화벽, PKI, 악성코드방지, 취약성 분석도구, 포렌식, 무결성 도구 등으로 분류하였다. 국가정보원과 정보통신부가 공동으로 발간한 2006 국가정보보호백서에서는 정보보호 제품을 침입탐지·차단 및 방지 제품군, 컴퓨터 바이러스 및 스팸방지 제품군, 기타 제품군(백업제품, 인증·암호화 제품, 보안서비스 등)으로 분류하였다[국가정보원, 정보통신부, 2006]. 한국정보보호산업협회는 정보보호 제품을 PC보안, 가상사설망(VPN), 공개키기반구조(PKI), 데이터보안(encryption), 리눅스보안, 바이러스 백신, 보안관리 ESM, 패치관리 PMS, 보안취약점 분석도구(스캐너 외), 전자우편보안, 침입차단시스템(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS), 서버보안, DRM, DB 보안, 바이오인식 정보보안, 무선인터넷 보안 등으로 분류하였다[한국정보보호산업협회, 2006].

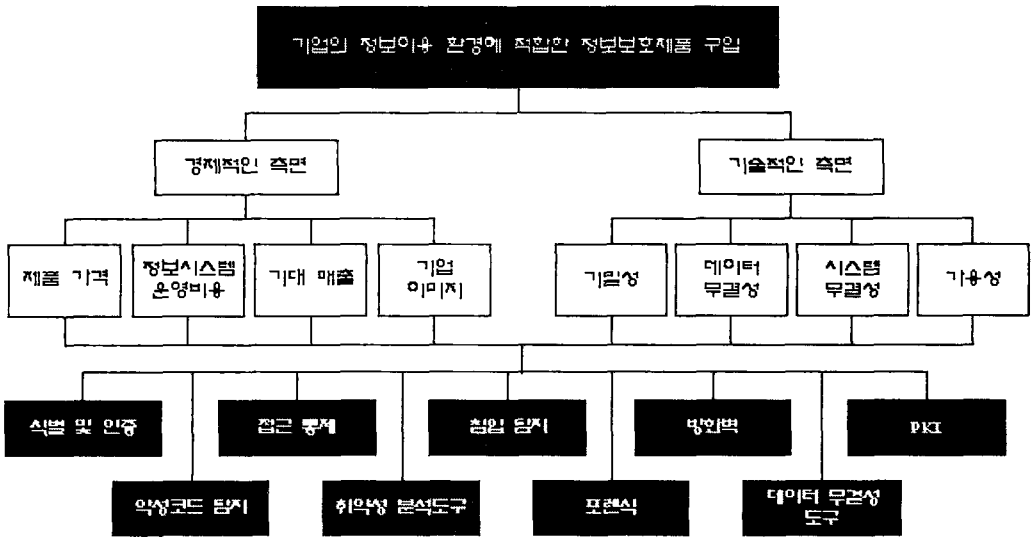
정보보호제품은 각 분류별로 SW, HW와 함께 정보보호서비스까지 포함한다. 본 연구모형의 평가대안과 정의는 가장 보편적으로 채택되고 있는 NIST[2003]의 분류를 따랐다<표 3>. 그러나 본 연구에서는 평가대안 사이의 상호 종속성을 배제하지 못하였다. 이로 인해 정보보호의 민감성에 따라 유사한 기능의 제품을 중복으로 선택하거나, 정보보호 제품을 패키지로 도입하는 경우 본 연구에서 제시하는 평가대안으로는 평가대안의 독립성에 한계가 있다. 따라서 정보시스템 이용환경의 특성을 고려하여 독립성이 보장되는 평가대안 도출에 대해 추가로 고려해야 한다.

3. 실증분석

제 3장에서는 연구모형을 토대로 정보보호분야 전문가들을 대상으로 실시한 설문조사 결과를 분석하고자 한다.

본 연구모형은 제 1계층에 모델의 목표, 제 2계층에 2개의 상위평가기준, 제 3계층에는 8개의 하위평가기준, 제 4계층에는 9개의 평가대안으로 구성하였다.

<그림 1>의 계층도를 기반으로 정보보호분



〈그림 1〉 최적의 정보보호제품 선정을 위한 계층도

야 전문가들을 대상으로 설문조사를 통하여 중요도를 산출하였다. 설문조사는 2006년 9월 15일 부터 2007년 4월 20일 까지 정보보호분야 관련 전문가 9명을 대상으로 실시하였다.

설문에 응답한 전문가는 대학교수 2명, 정보보호 관련기업의 최고정보보호책임자 3명, 공공기관의 최고정보책임자 1명, 정부출연연구소 팀장급 연구원 2명, 정보보호 관련분야 연구원 1명으로 정보보호 분야의 이론적, 실무적 경험을 보유하고 있을 뿐만 아니라 정보보호 투자 의사결정에서 영향을 줄 수 있는 전문가들이다.

AHP 기법에서 분석자료에 대한 신뢰도를 판단하기 위해 응답자 개개인의 판단상 오차정도를 측정하여 일관성 비율로 산출한다. 본 연구에서는 9부의 응답지를 회수하였으며, 이 중에서 결손치가 있는 응답지와 AHP 일관성 비율이 0.2이상인 응답지 3부를 제외하고 총 6부를 유효 데이터로 판단하였다. 유효설문 응답자의 일관성 비율은 각각 0.01, 0.06, 0.06, 0.12, 0.12, 0.13으로 나타났다. 중요도 평가과정에 집단이 참가하여 그 의견을 취합하는 방법은 집단의 동의를 구하여 단일의 중요도를 산출하는 방법과 개별적으로 중요도를 평가한 후 통합하는 방법이 있으나, 본 연구에서는 후자의 방법을 택하였고 6명 전문가의 의견을 기하평균(geometric mean)을 사용하여 집단의견의 중요도를 산출하였다[Saaty, 1998]. 본 연구는 하나로 통합된 중요도를 AHP 분석 프로그램인 Expert Choice 2000을 이용하여 분석하였으며, 그룹의사결정 분석 기능을 이용하여 일관성 비율을 분석한 결과 CR = 0.01로 유의한 수준의 응답을 얻음을 알 수 있다.

<표 4>는 상위기준(main criteria) 및 하위기준(sub criteria)간 우선순위(priority)에 대한 정보보호분야 전문가들의 의견을 보여주고 있다. 우선 상위기준 간 쌍별 비교 결과는 기술적 측면의 중요도와 경제적 측면의 중요도가 각각 43%와 56%로 거의 동일한 것으로 나타났다. 상위기준 대비 하위기준 간의 상대적 중요도는 경제적인 측면에서 기업이미지가 34%로 1위를, 정보시스템 운영비용이 30%로 2위를, 제품 가격이 21.3%로 3위를, 기대매출이 14.7%로 4위를 각각 기록했다. 연구결과, 흥미로운 것은 기업 이미지의 기준이 가장 중요한 제품 선정 기준으로 나타났다. 이는 정보보호 투자에 필요한 제품 선정 시 저가 제품보다는

〈표 4〉 상위기준 및 하위기준간 우선순위 분석 결과

상위기준	상위기준 간 상대적 중요도	하위기준	상위기준 대비 하위기준 간 상대적 중요도	전체 하위기준 간 상대적 중요도	하위기준 우선순위
경제적 측면	0.433	제품 가격	0.213(3순위)	0.092(7순위)	7
		정보시스템 운영비용	0.300(2순위)	0.130(4순위)	4
		기대 매출	0.147(4순위)	0.064(8순위)	8
		기업 이미지	**0.340(1순위)**	0.147(2순위)	2
기술적 측면	0.567	기밀성	0.163(4순위)	0.092(7순위)	7
		데이터 무결성	0.244(2순위)	0.138(3순위)	3
		시스템 무결성	**0.368(1순위)**	**0.209(1순위)**	**1**
		가용성	0.225(3순위)	0.128(5순위)	5
총 합	1.000		2.000	1.000	

〈표 6〉 대안간 하위기준별 우선순위 분석 결과

대안	경제적인 측면				기술적인 측면				전체 순위
	제품 가격	정보 시스템 운영 비용	기대 매출	기업 이미지	기밀성	데이터 무결성	시스템 무결성	가용성	
식별 및 인증	0.108 (5순위)	0.114 (6순위)	0.079 (7순위)	0.093 (5순위)	**0.176 (1순위)**	0.106 (3순위)	0.079 (9순위)	**0.152 (1순위)**	0.111 (6순위)
접근 통제	0.149 (2순위)	0.131 (3순위)	0.120 (3순위)	0.120 (3순위)	0.146 (2순위)	0.097 (7순위)	0.089 (8순위)	0.102 (6순위)	0.114 (3순위)
침입 탐지	0.132 (3순위)	0.121 (4순위)	0.099 (4순위)	0.099 (4순위)	0.127 (4순위)	0.131 (2순위)	0.103 (7순위)	0.144 (2순위)	0.120 (3순위)
방화벽	0.125 (4순위)	0.119 (5순위)	0.089 (6순위)	0.089 (6순위)	0.113 (5순위)	0.103 (4순위)	0.107 (5순위)	0.133 (4순위)	0.113 (2순위)
PKI	0.066 (8순위)	0.074 (8순위)	0.079 (8순위)	0.079 (8순위)	0.127 (4순위)	0.097 (7순위)	**0.140 (1순위)**	0.097 (7순위)	0.101 (8순위)
악성코드 방지	**0.174 (1순위)**	**0.153 (1순위)**	**0.242 (1순위)**	**0.242 (1순위)**	0.095 (6순위)	0.097 (7순위)	0.131 (2순위)	0.134 (3순위)	**0.148 (1순위)**
취약성 분석도구	0.105 (6순위)	0.097 (7순위)	0.122 (2순위)	0.122 (2순위)	0.075 (8순위)	0.080 (8순위)	0.130 (3순위)	0.111 (5순위)	0.108 (7순위)
포렌식	0.044 (9순위)	0.052 (9순위)	0.069 (9순위)	0.069 (9순위)	0.054 (9순위)	0.072 (9순위)	0.106 (5순위)	0.069 (8순위)	0.073 (9순위)
데이터 무결성 도구	0.097 (7순위)	0.139 (2순위)	0.086 (7순위)	0.086 (7순위)	0.086 (7순위)	**0.217 (1순위)**	0.114 (4순위)	0.057 (9순위)	0.112 (5순위)

기업이미지 제고에 도움이 될 수 있는 안정적인 제품을 선호하는 것으로 판단된다. 그 다음으로 중요한 정보보호 제품의 선정기준은 정보시스템 운영비용이다. 정보보호제품에 대한 투자 시 조직에서 운영하는 정보시스템이 정보보호 침해로 인해 비효율적으로 운영되는 것을 방지할 수 있고 기존의 정보시스템과 효율적으로 운용될 수 있는 제품을 선택하는 것이 중요한 기준임을 알 수 있다. 그 다음으로 중요한 정보보호 제품의 선정기준은 적정한 제품 가격과, 조직의 투자효과를 가장 가시적으로 판단할 수 있는 매출에의 기여도이다. 이들 기준들의 순위를 보면, 정보보호투자라는 것이 매출에의 직접적인 기여를 통한 효과성

〈표 5〉 대안간 상위기준별 우선순위 분석 결과

대 안	경제적 측면	기술적 측면	전체 순위
식별 및 인증	0.103(7순위)	0.116(4순위)	0.111(6순위)
접근 통제	0.131(2순위)	0.102(8순위)	0.114(3순위)
침입 탐지	0.118(3순위)	**0.122(1순위)**	0.120(2순위)
방화벽	0.112(4순위)	0.114(6순위)	0.113(4순위)
PKI	0.073(8순위)	0.120(3순위)	0.101(8순위)
악성코드 방지	**0.189(1순위)**	0.120(3순위)	**0.147(1순위)**
취약성 분석도구	0.108(6순위)	0.108(7순위)	0.108(7순위)
포렌식	0.058(9순위)	0.083(9순위)	0.073(9순위)
데이터 무결성 도구	0.108(6순위)	0.115(5순위)	0.113(5순위)

의 측면보다는 기업 이미지 향상과 정보시스템 운영비용의 감소를 통한 효율성의 측면이 더 강조되고 있는 것을 알 수 있다.

기술적인 측면에서의 상위기준 대비 하위기준 간의 상대적 중요도는 시스템 무결성이 36.8%로 1위, 데이터 무결성이 24.4%로 2위, 가용성이 22.5%로 3위, 기밀성이 16.3%로 4위를 각각 기록했다. 시스템 무결성 기준은 전체 8가지 하위기준 간 비교에서도 가장 높은 순위를 기록하여, 정보보호의 가장 중요한 목적이 조직의(주로 조직의 정보시스템의) 시스템 무결성을 확보하는 것임을 보여주는 결과이다. 시스템 무결성이 달성되지 못하면 데이터 무결성과 가용성이 보장될 수 없으므로 시스템 무결성과 데이터 무결성, 가용성은 상호 밀접한 관계가 있다. 실제 설문결과에서도 가용성 기준은 정보보호 제품 선정 시 데이터 무결성 기준과 근소한 차이를 보이는 것으로 나타났다. 그 다음으로, 일반인들이 '정보보호' 라는 용어로 쉽게 떠올리게 되는 기밀성이 상대적으로 낮은 중요도를 기록했다. 이러한 결과는, 최근의 정보보호 침해가 기밀성을 달성하지 못하게 하는 전통적인 형태보다는 정보시스템의 운영을 방해하여 시스템 무결성과 데이터 무결성, 그리고 가용성을 저해하는 것이 더 빈번하게 발생하기 때문인 것으로 판단된다.

전체 하위기준 간의 상대적 중요도는 시스템 무결성이 20.9%로 1위를, 기업 이미지가 14.7%로 2위를 나타내고 있다. 이는 기술적 측면에서의 시스템 무결성이 정보보호 제품 선정 시의 가장 중요한 기준으로 인식되고 있음을 나타낸다. 또한 기업이 정보이용환경에 적합한 정보보호 제품을 도입함으로써 정보화의 역기능들로부터 기업의 정보시스템을 보호하고, 정보시스템을 효율적으로 관리함으로써 향후 잠재적 자산인 기업 이미지 향상에 기여할 수 있을 것으로 기대하고 있기 때문으로 해석된다.

<표 5>와 <표 6>에서는 상위 기준 및 하위 기준 별로 각 대안간의 상대적 중요도를 보여주고 있다. 결과적으로, 기업에서 정보보호 목적을 달성하기 위해 투자를 하는 경우 경제적인 측면과 기술적인 측면을 모두 고려하면 '악성코드 방지' 제품군의 상대적 중요도가 가장 높은 것으로 나타났다. 정보보호 전문가들은 '악성코드 방지' 제품군의 도입을 통해 악성코드의 공격으로 인한 경제적 피해와 기술적 문제들에 대한 중요성을 높게 인식하는 것으로 여겨진다.

정보보호관련 전문가들은 경제적 측면에서는 '악성코드 방지' 제품군, 기술적 측면에서는 '침입 탐지' 제품군을 강조하는 것으로 나타났다. 경제적 측면에서 '악성코드 방지' 제품군의 중요도가 높게 나타난 것은 악성코드의 공격으로 인한 네트워크 위협의 실제 피해가 발생할 경우 그 규모가 클 것으로 예상하고 그 중요성을 높게 인식하고 있는 것으로 판단된다. 반면, 기술적 측면의 대안들은 상대적 중요도가 큰 차이를 보이고 있지 않지만, 그 중 '침입 탐지' 제품과 ' 악성코드 방지' 제품, 그리고 'PKI' 제품이 강조되는 것으로 나타났다. 이는 이러한 제품의 도입을 통해 기업의 정보자산의 침해에 신속하게 대응하여 필요한 조치를 취함으로써 피해규모를 최소화하고 수반되는 기술적 문제를 발생시키지 않게 하는 것이 가장 기초적이고 시급한 문제로 여겨지는 것을 알 수 있다.

<표 7>은 각 응답자별 대안선정 결과이다. 공통적으로는 많은 응답자가 '포렌식' 제품군을 가장 낮은 순위로 인식하는 것으로 나타났다. '포렌식'이 컴퓨터 수사를 위한 디지털 증거분석이라는 기술적 특성상 법과 가치를 반영하는 복잡하고 특성화된 분야이기 때문에 기업의 효율적인 정보시스템 운영측면에서는 중요성이 낮게 인식된 것으로 판단된다.

〈표 7〉 대안간 응답자별 우선순위

구 분		응답자 1	응답자 2	응답자 3	응답자 4	응답자 5	응답자 6	집단의견
일관성 비율(CR)		0.06 (6%)	0.12 (12%)	0.01 (1%)	0.12 (12%)	0.13 (%)	0.06 (%)	0.03 (3%)
대안별중요도	식별 및 인증	0.094 (6순위)	0.134 (2순위)	0.117 (4순위)	0.076 (5순위)	0.073 (8순위)	0.151 (1순위)	0.111 (6순위)
	접근 통제	0.124 (3순위)	0.102 (6순위)	0.117 (4순위)	0.070 (6순위)	0.100 (6순위)	0.150 (2순위)	0.114 (3순위)
	침입 탐지	0.124 (4순위)	0.142 (1순위)	0.098 (7순위)	0.062 (9순위)	0.141 (2순위)	0.138 (4순위)	0.120 (2순위)
	방화벽	0.066 (7순위)	0.136 (4순위)	0.098 (7순위)	0.068 (7순위)	0.131 (3순위)	0.144 (3순위)	0.113 (5순위)
	PKI	0.156 (2순위)	0.096 (7순위)	0.130 (2순위)	0.064 (8순위)	0.049 (9순위)	0.101 (7순위)	0.101 (8순위)
	악성코드 방지	**0.228 (1순위)**	0.126 (3순위)	**0.143 (1순위)**	**0.269 (1순위)**	0.115 (4순위)	0.112 (5순위)	**0.147 (1순위)**
	취약성분석도구	0.048 (8순위)	0.107 (5순위)	0.113 (5순위)	0.219 (2순위)	0.104 (5순위)	0.073 (8순위)	0.108 (7순위)
	포렌식	*0.056 (9순위)*	*0.076 (9순위)*	0.096 (8순위)	0.088 (3순위)	0.094 (7순위)	*0.027 (9순위)*	*0.073 (9순위)*
	데이터무결성도구	0.103 (5순위)	0.080 (8순위)	0.087 (9순위)	0.084 (4순위)	0.193 (1순위)	0.103 (6순위)	0.113 (5순위)

4. 결 론

본 연구의 결과가 정보보호제품 도입 의사결정과 관련하여 제시하고 있는 시사점은 다음과 같다. 첫째, 기업에서 정보보호 목적을 달성하기 위해 투자하는 경우 기술적 측면의 시스템 무결성을 가장 중요한 기준으로 인식하는 것으로 나타났다. 이는 기업의 외부 네트워크와의 정보교환 요구증가와 재택근무 등의 증가로 인해 네트워크 범위가 확대되어감에 따라 정보시스템 무결성 유지를 위한 투자비용과 운영 및 관리가 커다란 문제로 인식되고 있기 때문이다. 이러한 환경에서 기업의 보안을 유지하고 정보시스템의 무결성 확보를 위해 기술적 측면의 시스템 무결성 확보가 가장 중요한 기준으로 인식되고 있다. 둘째, 시스템 무결성 다음으로 기업이미지의 중요도가 높게 인식되고 있는 것으로 나타났다. 정보보호에 대한 투자효과는 정보시스템에 대한 투자와 다르게 기대 매출 증가나 정보시스템 운영비용 절감 등의 재무적 수치로 나타나기 보다는 비가시적이고 정량적으로 산출하기 어려운 기업의 이미지 향상 같은 정성적인 효과로 나타나기 때문에 이러한 효과들을 합리적으로 산출할 수 있는 평가기법의 개발이 필요하다는 점이다. 셋째, 경제적인 측면의 고려사항 중에서 제품가격의 중요도가 낮게 나타난 것은 정보보호제품 및 정보보호시스템에 대한 투자의 당위성과 투자비용의 타당성을 기업의 의사결정자들이 이미 인식하고 있다고 볼 수 있다. 넷째, 정보보호제품 및 시스템 도입을 결정하는 기업의 다양한 이해관계자의 의견에 일관성을 검증함으로써 의사결정의 질을 높이고, 상호간의 공감대를 형성할 수 있는 기준을 제시하였다. 마지막으로, 본 논문의 실무적 시사점은

다음과 같다. 기업경영의 전반에서 이루어지는 정보보호투자에 대한 의사결정 시 일반적인 경우의 적용사례를 제시하여 분석하였으며, 정보시스템 이용 특성을 반영한 평가기준 및 평가대안으로 수정 보완하여 적용할 수 있다.

본 연구에서 사용된 설문 응답자는 정보보호 기술 전반에 대해 폭넓게 이해하고 있고 조직의 투자관련 의사결정에 영향을 미칠 수 있는 최고정보책임자나 최고정보보호책임자이어야 하므로 설문결과를 확보하는데 많은 어려움이 있었다. AHP 방법론에서는 설문 응답자의 수 보다는 설문 응답자의 전문성이 더 중요시되기는 하지만, 본 연구에서는 설문 대상이 다양하지 않아 폭넓은 분석이 제한된 측면이 있었다. 또한 본 연구에서 제시된 정보보호 제품의 평가대안은 대안들 사이의 관계가 상호 독립적이거나 대체가능성을 지니고 있지 않으며, 일반적인 평가대안과는 차이가 존재한다. 추후 연구에서는 조직의 규모와 유형별, 또는 업종별로 도입 목적에 적합한 정보보호 제품을 선정할 수 있는 모형을 제시하고자 한다. 또한 향후연구에서 정보보호의 효과를 계량화할 수 있는 측도의 개발을 통해 다양한 하위기준들을 제시하고, 기준들 사이의 독립성을 강화하여 보다 가시적이고 객관적인 정보보호투자 의사결정을 지원할 수 있도록 할 계획이다. 또한 정보시스템측면과 정보보호측면에서의 평가기준 비교를 통해 보다 정보보호측면에서 특성화된 하위기준들을 도출하고자 한다. 이러한 연구를 바탕으로 정보보호에 대한 투자 의사결정시 작용하는 원리와 의사결정에 미치는 영향을 체계적으로 분석할 수 있을 것이다.

참 고 문 헌

[1] 국가정보원, 정보통신부, *2006 국가정보보호백서*, 2006.

[2] 김태성, 전효정, "AHP를 이용한 정보보호 인력 양성 정책 분석", *한국통신학회논문지*, 제31권 제5호, 2006, pp. 485-493.

[3] 권민영, 구본재, 이국희, "AHP 기법을 적용한 IT프로젝트 사전타당성 평가항목의 가중치 산출", *Information Systems Review*, 제8권 제1호, 2006, pp. 265-285.

[4] 한국정보보호진흥원, *2003 국내정보보호산업실태조사*, 2003.

[5] 한국전산원, *2006 국가정보화백서*, 2006.

[6] Blatchford, C., "Information Security Controls-Are They Cost-effective", *Computer Audit Journal*, Vol. 3, 1995, pp. 11-19.

[7] Bodin, L. D., Gordon, L. A., Loeb, M. P., "Evaluating Information Security Investments Using the Analytic Hierarchy Process", *Communications of the ACM*, Vol. 48, 2005, pp. 79-83.

[8] Cavusoglu, H.(Hasan), Cavusoglu, H. (Huseyin), Raghunathan S., "Economics of IT Security Management : Four Improvements to Current Security Practices", *Communications of the Association for Information System*, Vol. 14, 2004a, pp. 65-75.

[9] Cavusoglu, H., Mishra, B. and Raghunathan, S., "A Model for Evaluating IT Security Investments", *Communications of the ACM*, Vol. 47, No. 7, 2004b, pp. 87-92.

[10] Davis, A., "Return on Security Investment-Proving It's Worth It", *Network Security*, Vol. 2, 2005, pp. 8-10.

[11] Finne, T., "The Information Security Chain in a Company", Computers and Security, Vol. 15, 1996, pp. 297-316.

[12] Gordon, L. A., Loeb, M. P., "The Economics of Information Security Investment",

ACM Transactions on Information and System Security, Vol. 5, No.4, 2002, pp. 438-457.

[13] Kim, Snagkyun, Lee, Hongjoo, "Cost-Benefit Analysis of Security Investments : Methodology and Case Study", *International Conference on Computational Science and its Applications*, Vol. 3482, 2005, pp. 1239-1248.

[14] Lee, Vicent C. S., "A Fuzzy Multi-criteria Decision Model for Information System Security Investment", *Intelligent Data Engineering and Automated Learning*, Vol. 2690, 2003, pp. 436-441.

[15] NIST, An Introduction to Computer Security, *NIST Special Publication 800-12*, 1996.

[16] NIST, Guide to Selecting Information Technology Security Products, *NIST Special Publication 800-36*, 2003.

[17] Saaty, T. L., "How to Make a Decision : The Analytic Hierarchy Process", *European Journal of Operation Research*, Vol. 48, 1990, pp. 9-26.

[18] Saaty, T. L., The Analytic Hierarchy Process, *McGraw Hill, New York*, 1980.

[19] Saaty, T. L. and Luis, G. V., "Diagnosis with Dependent Symptoms : Bayes Theorem and the Analytic Hierarchy Process", *Operations Research*, Vol. 46, No. 4, 1998, pp. 491-502.

[20] Soo Hoo, K. J., How much is enough? A Risk-Management Approach to Computer Security, *CISAC*, 2000.

[21] Tanaka H., Matuura K., Sudoh O., "Vulnerability and Information Security Investment : An Empirical Analysis of E-local Government in Japan", *Journal of Accounting and Public Policy*, Vol. 24, 2005, pp. 37-59.

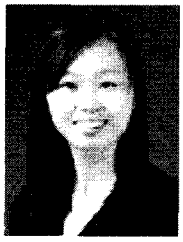
[22] TSO, Best Practice for Security Management, *ITIL Series*, 1999.

[23] http://www.kisia.or.kr(한국정보보호산업협회).

저자소개

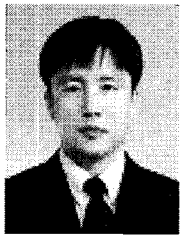
공 희 경

충북대학교에서 회계학을 전공하였고, 충북대학교 대학원 정보산업공학과에서 공학석사를 취득 후 현재 동 대학원 경영정보학 박사과정에 재학중이다. 주요 관심분야는 정보보호경영 및 정책, 정보자원관리, 경제성 분석, 시스템다이내믹스 등이다.



전 효 정

충북대학교 경영정보학과에서 학사, 석사를 마치고 한국전자통신연구원 기획본부 사업기획팀에서 4년간 근무하였다. 현재에는 동대학원 박사과정에 재학중이다. 주요 관심분야는 정보자원관리, 정보시스템 정보보호, 정보시스템 및 정보보호인력 관련 연구 등이다.



김 태 성

한국과학기술원 경영과학과에서 학사, 석사, 박사를 취득하고, 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 부교수로 재직중이다. 국내외 경영과학, 정보통신, 정보보호 관련 학술지 및 학술대회에 논문을 발표하였으며, 주요 관심분야는 정보통신과 정보보호에 관련된 경영 및 정책 이슈에 대한 분석이다.

◈ 이 논문은 2007년 11월 26일 접수하여 1차 수정을 거쳐 2008년 03월 07일 게재확정되었습니다.