Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1271

정보보호의 투자 집행 효과에 관한 연구

정 성 훈,† 윤 준 섭, 임 종 인, 이 경 호‡
고려대학교 정보보호대학원

Studies on the effect of information security investment executive

Seong-hoon Jeong,† Joon-sub Yoon, Jong-in Lim, Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

본 논문에서는 정보보호 관리체계를 구축하고 운영하고 있는 기업에서 외부감사(ISO27001)와 내부감사(보안전담조직에 의한)에 대한 결함 및 권고사항을 기술적 영역, 관리적 영역, 물리적 영역으로 분류하고 예산과 투자에 대한 상관관계를 확인하여 어떠한 영향이 있는지 분석하였다. 분석 결과는 시간의 흐름에 따라 관리적 보안영역과 기술적 보안영역에서 일관성 있는 연관관계를 확인하였으며 특히 미집행 예산(예산액-집행액) 규모와 감사 결함 및 권고사항의 수가 정(+)의 관계에 있음을 확인할 수 있었다. 이를 통해 상관분석 결과에 따른 유사도를 통계 분석하여 정보보호 투자의 효과성을 검증할 수 있는 모델을 제시한다. 그리하여 기업의 정보보호 투자에 대한 체계적인 방법론 접근과 정보보호 정책 수립 시 정확한 의사결정 방향에 도움이 되고자 한다.

ABSTRACT

This paper classifies technical, administrative and physical areas of defects and advices made by an external audit (ISO27001) and internal audit (performed by a security team) in a company which has the management system of information security. With the classified data it finds the correlation between the budget and investment of information security, and analyze the correlation. As a result of the analysis, it has been found that as time goes on there is a consistent correlation between a administrative area and technical area of security. Specially, it has been confirmed that the relation between the scale of the budget which is not executed and the number of the defects and advices made by the audit is in direct proportion. Therefore, in this paper, so as to provide a model that can be used for validating the effectiveness of the protective investment information by statistically calculating the similarity based on the results of correlation analysis. This research is intended to help that a company makes a precise decision when it establishes a policy of information security and systematic methodology of the investment in information security.

Keywords: Security Policy, ISMS, ISO27001, Risk Management, Information Security Investment

I. 서 론

정보보호 투자의 효과를 정량적으로 검증하기 위해서는 정보보호 투자에 대한 데이터 및 침해사고 건수, 피해액 등 정보보호 투자의 효과를 나타내는 데이터가 필수적이다. 하지만 정보보호 투자 및 침해사고에 대한 데이터가 대다수 기업의 대외비 정보이기 때문에 데이터 수집에 한계가 있다. 이처럼 정보보호라는 특수성으로 인해 정보보호 투자에 대한 효과를 정량적으로 산출해 내고자 하는 연구에 한계가 있고 체계적이지 않아 정보보호 투자에 대한 기업의 어려움이 있다. 또한 기업에서 정보보호에 대한 투자를 점차적으로 늘려가고 있으나 그 투자가 곧바로 가시적으로 확인되는 것도 아니며 투자 이후에는 오히려 정보보호 투자에

접수일(2014년 9월 24일), 수정일(1차: 2014년 11월 4일, 2차: 2014년 11월 17일), 게재확정일(2014년 11월 23일)
† 주저자, skkalsam@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

대한 성과 검증을 하지 못해 오히려 관련 투자가 위축되기도 한다. 이러한 정보보호에 대한 투자가 적시에 이루어지지 못하는 경영환경 속에서 정보보안 사고는 지속적으로 발생하고 있으며 단순히 기업 경쟁력의 문제가 아니라 때로는 〔Table 1.〕과 같은 보안사고로 인해 국가 안보의 문제로도 대두되고 있다.

최근 발생한 금융기관의 보안사고와 관련하여 금융감독원에 따르면 2013년 3월 농협 전산망 사고 시 농협의 IT예산 중 보안 예산 비중은 1.6%에 불가하였고 시스템 구축이 완료되었다는 이유로 보안예산을 71억원에서 23억원을 삭감한 것으로 알려졌다. 또한 김희정 새누리당 의원은 최근 1억4천만건에 달하는 개인정보를 유출한 3개 신용카드사의 정보보호 예산이 KB국민카드는 2012년 113억에서 2013년 76억원으로 40억원 이상 삭감되고, NH농협카드(농협은행 기준)는 2012년 1103억원에서 2013년 406억원으로 60% 이상 삭감되었으며 롯데카드의 경우 2012년 84억원에서 2013년 89억원으로 소폭 늘렸지만 IT예산 대비 정보보호 예산은 8.5%에서 7.48%로 오히려 떨어지는 등 전자금융감독 규정에 따라 7% 이상을 형식적으로 반영하고 있다고 지적했다〔1〕.

이러한 정보보안 사고가 사회적 이슈가 됨에 따라 각 기업은 정보보호 예산에 대한 고민이 깊어지고 최신 보안솔루션을 검토하고 도입을 고려하고 있지만 정작 해당 기업 또는 조직에 어떤 정보보호 효과가 있는지 검증하는데 있어 한계가 있다.

국내외 연구에서도 정보보호 투자에 대한 최적 모델을 제시하는가 하면 정보보호 투자의 비용회수에 대한 연구가 진행되고 있지만 정량적으로 정보보호 투자를 위한 의사결정의 도구로는 한계가 있는 것이 현실이다.

정보보호 예산 수립을 통한 보안투자는 정보보호 관리체계를 강화하는 방법 중의 한가지이고 관리체계가 향상되면 상대적으로 보안감사 결함수는 줄어든다. 따라서 본 연구에서는 정보보호 예산 및 투자와 내·외부 감사의 결함에 대한 자료를 분석하고 이들의 관계에 대해 다음과 같은 가설을 검증해보고자 한다. 정보보호 투자가 기술적, 관리적, 물리적 보안영역 중에서 어떤 분야의 보안감사 결함 수준에 영향을 미치는지 분석하고자 한다.

이를 통해 기업의 정보보호 투자에 대한 효과를 검증하고 정보보호 투자에 대한 현실적이고 실질적인 인식 변화를 도모하고자 한다.

Table 1. Information security incidents in korea (wikipedia, Since2008)

Time	Company	Accident type	Damage scale
July 2009	Government, portal, bank	7·7 DDoS Attack	
March 2011	Government, portal, bank	3·3 DDoS Attack	
April 2011	NHbank	Computer network attack	
October 2011	Election Commission	10·26 DDoS Attack	
March 2013	MBC, KBS, Shinhan Bank, NHbank	3·20 South Korea cyber attack	
June 2013	New Frontier Party, blue house, USFK	6·25 cyber-terror	2.9million people
January 2014	KBcard, lottecard, NHcard	Financial Information Disclosure	20million people

II. 정보보호 투자 현황 및 선행 연구 분석

2.1 정보보호 투자 현황

한국인터넷진흥원(KISA)의 2014년 국가정보보호 백서에 따르면 정보보호 전담조직을 설치, 운영하고 있는 업체는 9.8%로 전년 대비 1.3% 증가하였으며 정보관리 총괄 책임자(CIO, Chief Information Officer)를 임명한 사업체는 23.5%로 전년 대비 6.6% 증가하였으며 정보보호책임자 (CISO, Chief Information Security Officer) 임명은 4.2% 증가한 19.9%로 조사되었다. 또한 정보보호 투자는 국내 민간 사업체의 경우 45.9%로 전년대비 19.2% 증가한 것으로 나타났으나 5% 이상 정보보호에 지출한 업체는 여전히 3.2%에 불과하다〔2〕.

미래부의 정보보호 관련 산업 예산은 지식정보 보안산업 경쟁력 강화, 정보보호 대응능력 강화, 해킹바이러스 대응체계 고도화, 사이버 보안위협 예방체계 구축, 전자서명인증사업, 정보보호시스템 평가 및 인증기반 강화 등 분야별로 수립되고 있으며 2008년부터 점차적으로 증가해 2010년을 최고 기점으로 이후 다시 줄었다가 최근 보안 이슈로 점차적으로 늘려가고 있지만 3년 전 예산기준도 못 미치는 수준이다.

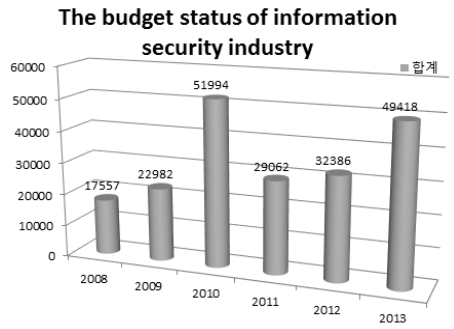

Fig. 1. The budget status of information security industry (Ministry of Science, ICT and Future Planning)

정보화예산과 비교해보면 2011년 6.2%까지 줄어든 정보보호예산은 2011년 발생한 3.4 DDoS 공격과 농협 전산시스템 마비사건을 계기로 12년 8.1%로 다시 증가하였다가 2013년 전년도 대비 0.8% 감소하였다[3].

대부분의 기업들이 보안의 중요성은 인식하고 있으나 여전히 투자가 아닌 비용으로 인식하고 있으며 사고가 발생하면 투자가 잠시 늘었다가 잠잠해지면 다시 금 줄어드는 예산 구조로 시장 확대가 둔화되고 있다.

또한 한국인터넷진흥원(KISA)의 2013년 정보보호 실태조사 자료에 따르면 정보보호 관련 지출이 없는 사업체를 대상으로 정보보호 관련 지출이 없는 이유를 조사해 보니 정보보안 사고로 인한 피해가 거의 없어 필요성을 느끼지 못하기 때문이라는 응답이 46.5%로 1위 였으며, 정보보호에 관심이 없다는 응답이 17.2%, 정보보호 예산이 없다는 응답이 15.8%이었다[4]. 정보보안 사고가 발생해야 관련 지출이 발생한다는 과반수에 가까운 응답이 국내 정보보호의 현주소를 알려주고 있다.

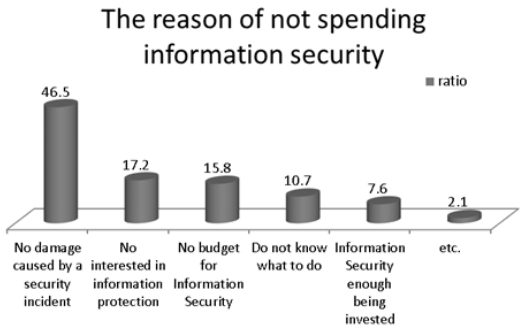

Fig. 2. The reason of not spending information security (%)

2.2 선행 연구 분석

정보보호 투자와 관련한 선행 연구는 크게 정보보호 투자 의사결정에 영향을 미치는 요인에 대한 연구와 정보보호 투자 효과에 관한 연구로 구분할 수 있다.

먼저 정보보호 투자 의사결정에 영향을 미치는 요인에 대한 선행연구로 Roper(1999)[5]는 정보보호 투자 시 비용 요인을 구매 비용, 유지보수 비용, 관리 및 운영 인력비용으로 분류하였고, Blakely(2001) [6]는 정보보호에 대한 투자효과를 정의하면서 투자 요인으로 초기 도입 비용, 갱신비용, 관리 비용 등을 포함하였으며, Harris(2001)[7]는 정보보호 투자에 대한 비용 요인을 제품 구매 비용, 설계 및 계획수립 비용, 환경 구축 비용, 연동 비용, 유지보수 비용, 테스트 비용, 갱신비용, 운영 및 관리 비용으로 분류하였다.

김정덕, 박정은(2003)[8] 및 이종선, 이희조(2007)[9]는 정보보호 투자에 대한 비용 산정 시 지속적 관리활동을 감안하는 것을 반영하여 TCO (Total Cost of Ownership)에 기반을 둔 개선된 ROSI를 제안하였고, 조영택(2014)[10]은 비용절감 및 효율을 위하여 통합 평가 항목이라는 개념을 제시하였다.

Witty(2001)[11]는 정보보안의 투자 요인을 크게 하드웨어, 인적자원, 소프트웨어, 외부 서비스 및 물리적 보안으로 분류하였다. 다섯 가지 영역을 세분화하여 인증, 권한관리, 코드보호, 사이버 재난대응, 컨텐츠 모니터링, 디지털 저작권 관리, 법적 책임준수, 암호화, 방화벽, 보험 가입, 인터넷 차단 통제, 침입 탐지, 인증 획득, 로깅, 감사, 악성코드 관리, 무결성 관리, 프라이버시 관리, 공개키 기반 구조, 레코드 기록 및 보관, 원격 접속, 위험 분석, 보안관리, 보안체계, 통합인증체계 등으로 구분하였다.

Gordon and Loeb(2002)[12]은 기밀성, 무결성, 가용성 등을 정보보호 목표로 하여 최적의 투자수준을 고려하는 경제적 모델을 제시하였다.

Cavusoglu et al. (2004a)[13], Cavusoglu et al. (2004b)[14]는 정보보호 투자 시 담당자가 고려해야 할 요인으로 정보보호침해 비용산정, 리스크 관리 기법, 비용 효과적 기술구성, 다양한 기술구성을 통한 가치들로 분류하였다.

김진(2014)[15]은 기업에서 투자 우선순위를 IT 재해복구, 접근통제, 물리적 보안 등의 순으로 진행한다고 통계 분석하였고, 장철환(2014)[16]은 규제가 투자에 가장 많은 영향을 미치며 다음으로 경쟁 우위

확보, 고객만족도 순으로 제시하였다.

다음으로 정보보호 투자 효과에 관한 연구에서

Table 2. Factors on Information Security Investment Decision

Analysis	Researcher	Content
Cost factors	Roper (1999) [5]	Classifying investment cost into purchase cost, maintenance cost, operating personnel cost
	Blakely (2001) [6]	Including initial introduction costs, renewal costs and administrative costs as investment factors
	Harris (2001) [7]	Classifying investment cost into purchase cost, design and planning cost, environmental construction cost, linkage cost, maintenance cost, renewal cost, operating cost
	Kim Jeong deok, Park Jeong Eun (2003) [8]	Presenting ROSI methods using TCO(Total Cost of Ownership)
	Lee Jong seon, Lee Hui Ho (2007) [9]	When calculating the cost of investments, Reflect the view of management activities continue
	Jo Young Tek (2014) [10]	Presented the concept of integrated assessment items for security assessment costs
Criteria for investment	Witty (2001) [11]	Classifying investment factor into HW, SW, Human resource, External service, Physical security
	Gordon and Loeb (2002) [12]	Presenting investment model considering the optimum level of investment
	Cavuso gluetal. (2004a, 2004b) [13],[14]	Investment decision applying game theory propose the factor investor should consider
	Kim Jin (2014) [15]	Analysis in corporate investment priorities
	Jang Chul Hwan (2014) [16]	Analysis for giving the most impact on investment

Scott(1998)[17]은 정보보호에 대한 투자는 보호 받는 자산의 가치를 기준으로 평가하는 것을 제시하였고 Gordon and Loeb(2002)[12]은 순현재가치(Net Present Values)모형을 이용하여 투자의 최적수준을 제시하면서 초기에 투자되는 비용에 비해 그 보안 수준의 향상은 완만하게 변화하는 것을 분석하였다.

Kim과 Leem(2002)[18]은 정보시스템 투자에 대한 효과를 운영적 효과와 경쟁우위를 달성시키는 전략적 효과로 분류하였다. 운영효율을 증대시켜주는 운영적 효과는 금전적 형태, 수치적 형태 또는 정성적 형태로 표현된다. 운영적 효과에는 비용절감, 이익 증대, 의사결정 수준 향상, 업무 기능 향상 등을 제시하고 있다.

Davis(2005)[19]는 ROSI를 정보보호 투자에 대한 재정적 수익의 비율로 정의하고, 운영비용의 감소와 순익의 증대를 포함하는 재무적 효용(financial benefits)과, 통제 비용과 사고(incidents) 비용을 포함하는 정보보호비용(cost of security)을 이용해 측정하였고, 선한길(2005)[20]은 정보보호 투자에 대한 성과를 정보보호 사고의 감소, 자산의 손실건수 감소, 비즈니스 기회손실 감소, 타사 경쟁 시 손해 감소, 이미지 실추건수 감소, 사고발생 시 신속한 처리 등으로 구분하였으며 Blatchford(1995)[21]는 정보보호 투자에 대한 비용(costs)과 효용(benefits)이 고객-공급자 기대심리 등을 통해 기업에 직간접적으로 지대한 영향을 미칠 수 있음을 지적하였다.

홍기향(2004)[22]은 정보보호 관리 수준을 측정하고 정보보호 노력이 조직에 미치는 영향을 분석하였으며, 인과관계와 적합관계 유형에 따라 정보보호 성과에 미치는 영향을 분석하였다.

남상훈(2005)[23]은 기업의 보안 사고가 주식가격에 미치는 영향을 통해 정보보호 투자효과를 분석한 반면 권영옥(2005)[24], 권영옥, 김병도(2007)[25]는 정보보안 사고에 따른 기업의 손실과 보안 투자로 인한 수익을 기업 시장가치의 변화를 이용하여 정량적으로 측정하였다.

정보보호 투자와 관련된 선행연구는 주로 정보보호 투자를 NPV, ROSI 등 경제학의 관점에서 접근하여 투자 효과를 측정하고 설문에 기반한 투자의 우선순위 도출에 제한되어 있었지만 본 연구는 보안감사의 결함을 기준으로 정보보호예산액과 정보보호집행액을 분석하여 실질적 데이터에 기반한 투자효과 검증모델을 제시하였다.

Table 3. Study on information security investment effect

Analysis	Researcher	Content
investment effect measurement	Scott (1998) [17]	Based on the value of the protected assets
	Gordon and Loeb (2002) [12]	Presenting optimal level of investment using NPV(Net Profit Value) model
	Kim & Leem (2002) [18]	Analysis classified as operational effectiveness and strategic effectiveness of investment
	Davis (2005) [19]	Defined ROSI as the ratio of the financial return on investment for information security
	Seon Han Kil (2005) [20]	Classifying performance metrics - Decrease in the security incidents - Decrease of business opportunity loss - Decrease loss of third party damage - Decrease of image suffersPrompt rocessing(accident)
Impact on the Company	Blatchford (1995) [21]	Point out impact how costs and benefits affect companies
	Hong ki Hyang (2004) [22]	Impact Analysis informationsecurity effort affect orgarnization
	Nam Sang Hoon (2005) [23]	Analyzing Impact enterprise security affect share price
	Kwon Young Ok (2005) [24], Kwon Young Ok, Kim Byung Do(2007) [25]	Measurement of changes in market value due to security incident and corporate investment

III. 분석 환경 및 분석 방법

3.1 분석 환경

A사의 매출 500억 규모인 데이터센터를 연구 범위로 하여 그 중 보안 감사 부분은 IT보안담당자 및 내부통제조직에 의해 수행되는 내부보안 감사결과와 정보보호 관리체계 국제 표준인 ISO27001 외부감사 심사결과를 연구 범위로 선정하였다.

마찬가지로 정보보호 예산액 및 정보보호 집행액 부분도 동기간에 걸쳐 자료 분석이 시행되었다. 정보보호 예산액은 연간보안예산을 기준으로 월단위로 구분하였고 유지보수예산도 포함시켰으며 정보보호 집행액의 경우는 집행 실적 금액과 유지보수비용을 합하여 산정하였다. 또한 보안감사영역과 예산 및 투자집행의 범위를 동일한 범위 내에서 선정하였다.

기간은 2009년부터 2014년 상반기까지 총 5년6개월 동안의 66차에 걸친 데이터를 기반으로 하였다. 연구대상 기간을 2009년부터 선정한 이유는 2008년을 전후로 정보보호전담조직의 변화 및 내부보안감사를 체계적으로 시행하게 되는데 주로 기인한다. 아울러 2009년도부터 5년6개월의 연구대상기간은 실증연구분석을 위한 적정수의 표본이라 판단된다. 상관관계분석을 위한 기초 데이터 자료는 아래 [Table 4.]와 같다.

특정 기업의 정보보호 예산과 투자집행 그리고 감사 결함수를 통계 분석하였으므로 매출 500억 규모의 IT서비스 외 업종에는 일반화하기에 제약사항이 존재한다.

Table 4. Selected analytical data

	selected item	details
security audit	ISO27001 audit results	divided into administrative, physical and technical section about external audit results half-yearly
	internal security audit results	divided into administrative, physical and technical section about internal audit results half-yearly
security budget and performance	planning and investment budget	classify into security budget semiannually

	maintenance costs	separate out security maintenance of the total maintenance
	investment executive performance	separate out information security investment executive performance on budget

3.2 분석 방법

STEP 1 : 정보보호 결함의 분류 기준 수립
STEP 2 : 정보보호 결함 내역 분석
STEP 3 : 정보보호 예산의 분류 및 분석
STEP 4 : 정보보호 투자 집행 내역 분석
STEP 5 : 분야별 결함과 예산 및 투자와의 상관분석
STEP 6 : 정보보호 투자효과 검증 모델 도출

3.2.1 보안감사 결함의 분류 기준

2009년도 상반기부터 2014년도 상반기 ISO27001 심사 결과보고서 상의 부적합사항(nonconformities) 및 권고사항(observations)과 내부보안 감사결과 보고서 상의 부적합사항을 통해 총 309개의 부적합사항 및 권고사항을 정리하였다.

내부보안 감사와 외부 보안감사에 중복되는 결함내역이라 하더라도 개별적으로 결함 개수에 반영하였다. 이후 부적합사항과 권고사항을 합쳐서 결함수(defects)라고 하겠다. 관리적 보안, 기술적 보안, 물리적 보안으로 구분하여 해당분야의 투자 성과를 측정하는데 있어 각 분야의 연관성이 존재하여 제약사항이 있지만 분야별로 보다 신뢰성 있는 결론에 도달하기 위해 해당 내역을 〔Table 5.〕 기준에 근거하여 관리적, 기술적, 물리적 분야로 분류하였다. 객관적인 데이터를 분류하기 위해 결함에 대한 개선방향이 아닌 결함자체의 근거를 기준으로 하여 분류하였으며 동일한 이유로 인해 부적합사항 및 권고사항에 대한 가중치는 별도로 고려하지 않았다.

3.2.2 보안감사 결함 분류

내부보안감사와 ISO27001 심사 결과에 대하여 부적합사항(nonconformities)과 권고사항(observations)의 개수 합으로 결함수(defects)를 측정하였다. 관리적 보안의 결함이 대체로 많은 편이며 물리적 보안의 결함은 3건 미만으로 분류되었다. 2010년도 상반기에 결함 수가 급격히 늘어난 이유는 2009년 7월 7.7

Table 5. Nonconformities and observations criteria for classification

Domain	ISO 27001	Internal Audit	classification			details
			adMinistrative	Technical	Physical	
Managing the ISMS	4,5,6,7,8	XX21 XX24 XX40	M1	T1	P1	Risk management, Internal Audit ISMS review
Security Policy	A5	XX21	M2	T2	P2	policy
Organization of information security	A6	XX22, 38	M3	T3	P3	responsibility
Asset management	A7	XX25, 36	M4	T4	P4	asset management
Human resources security	A8	XX23, 28	M5	T5	P5	training, personnel management
Physical and environmental security	A9	XX35, 30	M6	T6	P6	Facility, CCTV
Communications and operations management	A10	XX28, 32,37, 38,19, 01	M7	T7	P7	log, backup, document, media, vaccine
Access control	A11	XX29, 28,47	M8	T8	P8	account management, terminal
Information systems acquisition, development and maintenance	A12	XX31	M9	T9	P9	outsourcing program development
Information security incident management	A13	XX27	M10	T10	P10	vulnerability inspection
Business continuity management	A14	XX26	M11	T11	P11	BCP/DR
Compliance	A15	XX21, 24	M12	T12	P12	personal information

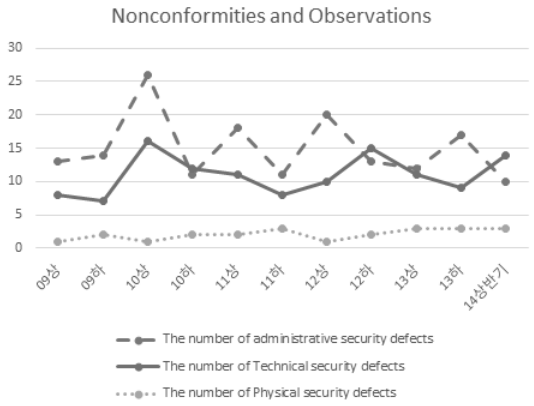

Fig. 3. The number of Nonconformities and Observations

DDoS 보안사고 이후 보안 감사가 강화된 것으로 추정해 볼 수 있다.

Table 6. The number of Nonconformities and Observations

	M(adMinistrative)	T (Technical)	P (Physical)
2009-1st half	13	8	1
2009-2nd half	14	7	2
2010-1st half	26	16	1
2010-2nd half	11	12	2
2011-1st half	18	11	2
2011-2nd half	11	8	3
2012-1st half	20	10	1
2012-2nd half	13	15	2
2013-1st half	12	11	3
2013-2nd half	17	9	3
2014-1st half	10	14	3

3.2.3 정보보호 예산의 분류

예산의 경우 기획예산과 투자예산 그리고 유지보수 예산 중 보안과 관련된 항목만 선정하였으며 주요 내용은 〔Table 7.〕과 같다.

3.2.4 분야별 예산 통계

정보보호 예산은 보통 연단위로 계획되며 예산집행 예정시기에 따라 월별로 분류하였다. 오차를 줄이기 위해서 교육과 같이 단기에 끝나는 항목을 제외한 나머지는 반기를 기본으로 해당기간만큼 분산해서 산정하였다.

Table 7. Budget classification

group	main contents
adMinistrative	security education security consulting fee auditing fee membership fee
Technical	server security solution network security solution application security solution PC security solution
Physical	access control systems parking control systems CCTV(closed-circuit television) Digital Video Recorder

대체로 관리적 보안예산과 물리적 보안예산에 비해 기술적 보안예산의 비율이 높은 편으로 확인된다. 2008년도 국내기업의 대형 개인정보 유출사고 및 개인정보보호법 개정을 통해 정보보호 예산은 2009년도에 최대치를 기록하고 이후 점점 줄어들다가 다시 최근 대형 보안사고 및 관련법 개정으로 보안투자의 필요성이 확대된 것으로 분석된다. 이는 미래부 예산 현황과 유사한 형태를 보이고 있다.

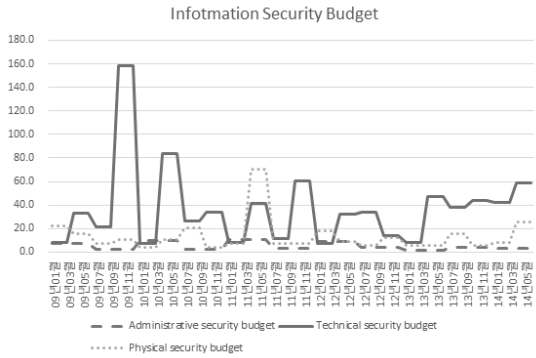

Fig. 4. Information security budget

3.2.5 보안투자 실적 통계

기술적 보안투자의 경우 2009년도 국내 7.7 DDoS 보안사고 이후 관련 보안솔루션 및 통합 보안 모니터링 시스템 구축으로 인해 예산이 많이 집행되었

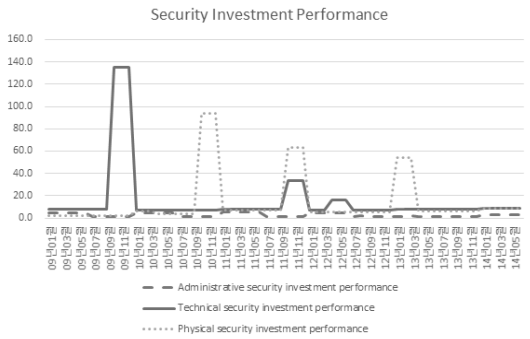

Fig. 5. Investment Performance

으며 물리적 보안 투자는 2010년도 하반기와 2011년도 하반기 그리고 2013년도 상반기에 주로 이루어 졌다.

IV. 정보보호 투자와 감사 결함과의 관계

4.1 유사도 분석

예산액과 집행액 그리고 결함수와 정량적 비교분석을 통해 연관성을 추정할 수 있었으며 표본은 지난 5년 6개월(66개월)간의 66차에 걸친 예산액과 집행액 그리고 결함수를 대상으로 하였다. 그 중 관리적, 기술적, 물리적 분야별로 분류된 집행액, 예산 미집행액 그리고 결함수를 선정하여 유사도 분석을 실시하였다.

각 변수간의 관련성을 구하기 위해 SPSS 21 (Statistical Packages for Social System) 통계 분석을 활용하였으며 상관분석시 사용된 계수는 Pearson 상관계수이다.

일반적으로 $-1 < r < -0.7$ 은 강한 음의 선형관계, $-0.7 < r < -0.3$ 은 뚜렷한 음의 선형관계, $-0.3 < r < -0.1$ 은 약한 음의 선형관계, $-0.1 < r < 0.1$ 은 거의 무시될 수 있는 선형관계, $0.1 < r < 0.3$: 약한 양의 선형관계, $0.3 < r < 0.7$ 은 뚜렷한 양의 선형관계, $0.7 < r < 1$ 은 강한 양의 선형관계를 나타낸다. 본 연구에서는 모델 산출을 위해 피어슨계수 0.7 이상의 강한 선형관계에 대해서 선정하였다.

앞서 설명한 바와 같이 정보보호 체계 강화를 목적으로 정보보호 투자를 집행하므로 대립가설은 정보보호 투자가 관리적, 기술적, 물리적 영역의 정보보호 감사 결함수 축소에 영향이 있다고 설정한다.

단순히 집행액만으로 보안결함수에 영향이 있는지 아니면 예산에 근거한 집행액과 관련이 있는지 확인하기 위해 '집행액과 결함수의 상관관계'와 '예산 미집행액과 결함수의 상관관계' 를 비교해보고 어떤 분야에서 유사도가 높은지 분석해보겠다.

4.2 집행액과 결함수의 상관관계

4.2.1 관리적 부분

관리적부분의 결함수와 집행액의 상관계수는 0.564이고 유의확률이 0.001이하로 유의수준 0.05에서 귀무가설은 기각되며 따라서 상관관계가 있다고 할 수 있다. 하지만 피어슨 상관계수가 0.7을 넘지 못하므로 채택하지는 않는다.

Table 8. Correlation analysis between the number of administrative security defects and administrative investment performance

Descriptive Statistics

	Mean	Std. Deviation	N
Administrative investment performance	2.5303	1.73240	66
The number of administrative security defects	15.0000	4.64758	66

Correlations

		Administrative investment performance	The number of administrative security defects
Administrative investment performance	Pearson Correlation	1	.564**
	Sig. (2-tailed)		8.05E-07
	N	66	66
The number of administrative security defects	Pearson Correlation	.564**	1
	Sig. (2-tailed)	8.05E-07	
	N	66	66

4.2.2 기술적 부분

기술적부분에서의 결함수와 투자 금액의 상관계수는 -0.531이고 유의확률이 0.001이하로 귀무가설은 기각되며 상관관계가 있다고 할 수 있다. 마찬가지로 상관계수 절대치가 0.7을 넘지 못하므로 채택하지는 않는다.

4.2.3 물리적 부분

결함수와 집행액의 상관계수는 0.405이고 유의확률이 0.001로 유의수준 0.05에서 귀무가설은 기각되며 따라서 약한 상관관계가 있다고 할 수 있다.

추이 통계를 분석해본 결과 관리적, 기술적, 물리적 분야별 단순 집행액과 결함과의 강한 상관관계는 없는

Table 9. Correlation analysis between the number of technical defects and technical security investment performance

Descriptive Statistics

	Mean	Std. Deviation	N
Technical security investment performance	15.1636	18.37779	66
The number of technical defects	11.0000	2.88231	66

Correlations

		Technical security investment performance	The number of technical defects
Technical security investment performance	Pearson Correlation	1	-.531**
	Sig. (2-tailed)		4.54E-06
	N	66	66
The number of technical defects	Pearson Correlation	-.531**	1
	Sig. (2-tailed)	4.54E-06	
	N	66	66

Table 10. Correlation analysis between the number of physical security defects and physical security investment performance

Descriptive Statistics

	Mean	Std. Deviation	N
physical security investment performance	14.1182	15.39072	66
physical security defects	2.0909	.79860	66

Correlations

		physical security investment performance	physical security defects
physical security investment performance	Pearson Correlation	1	.405**
	Sig. (2-tailed)		.001
	N	66	66
physical security defects	Pearson Correlation	.405**	1
	Sig. (2-tailed)	.001	
	N	66	66

것으로 확인되었다.

4.3 예산 미집행액과 결함수의 관계

4.3.1 관리적 부분

결함수와 미집행예산액의 상관계수는 0.857이고 유의확률이 0.001이하로 귀무가설은 기각되며 연구가설은 지지된다. 즉 관리적 영역의 결함수는 관리적 부분의 미집행된 예산액과 강한 상관관계(+)가 있다. 또한 그래프를 통해 관리적 보안 부분에서 예산(Bm) 대비 집행실적(Ipm)을 제외한 나머지 금액 즉 집행되지 않은 예산(Bm-Ipm)과 결함수(M)를 분석해 본 결과 대부분 정(+)의 비례관계에 있음을 확인할 수 있다.

관리적 보안의 경우 상반기에 투자집행이 많이 이루어지고 또한 연간활동의 미비사항을 상반기에 주로 확인하는 감사 특성상 예산과 결함의 변동이 급격함을 알 수 있다.

Table 11. Correlation analysis between the number of administrative security defects and not execution administrative budget

Descriptive Statistics

	Mean	Std. Deviation	N
not execution administrative budget	2.7061	1.76843	66
administrative security defects	15.0000	4.64758	66

Correlations

		not execution administrative budget	administrative security defects
not execution administrative budget	Pearson Correlation	1	.857**
	Sig. (2-tailed)		4.20E-20
	N	66	66
administrative security defects	Pearson Correlation	.857**	1
	Sig. (2-tailed)	4.20E-20	
	N	66	66

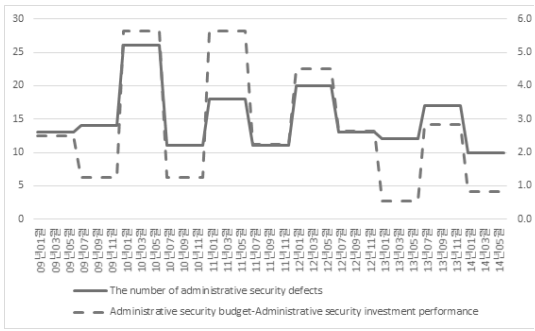

Fig. 6. The number of administrative security defects vs not execution administrative budget

4.3.2 기술적 부분

결함수와 미집행예산액의 상관계수는 0.767이고 유의확률이 0.001 이하로 유의수준 0.05에서 귀무가설은 기각되며 따라서 기술적 영역의 결함수도 기술적 부분의 미집행된 예산액과 강한 상관관계(+)가 있다.

기술적 보안 부분의 예산 대비 실제 집행된 실적을 제외한 나머지 금액과 기술적 부분의 결함수가 정(+)의 관계에 있음을 확인하였다.

기술적 분야에서 미집행 예산과 결함의 관계가 밀접하게 나타나고 있으며 11년 계획 대비 예산을 많이 집행한 시기에 감사 결함이 비교적 적게 나타났고 그 이후 최근 예산 집행이 제대로 이루어지지 않고 투자가 계속 줄어들자 감사 결함수가 늘어나고 있음을 확인할 수 있다.

Table 12. Correlation analysis between the number of technical security defects and not execution technical budget

Descriptive Statistics

	Mean	Std. Deviation	N
Not execution technical budget	25,5455	12,07181	66
Technical security defects	11,0000	2,88231	66

Correlations

		Not execution technical budget	Technical security defects
Not execution technical budget	Pearson Correlation	1	,767**
	Sig. (2-tailed)		6,17E-14
	N	66	66
Technical security defects	Pearson Correlation	,767**	1
	Sig. (2-tailed)	6,17E-14	
	N	66	66

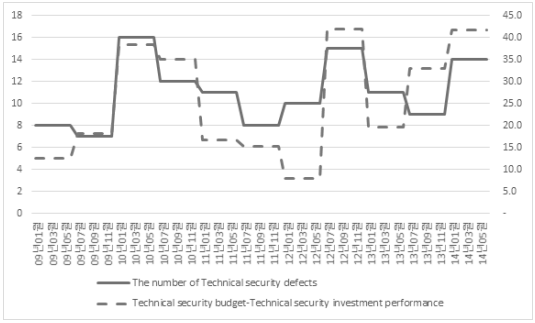

Fig. 7. The number of technical security defects vs not execution technical budget

4.3.3 물리적 부분

결함수와 미집행예산액의 상관계수는 -0.387이고 유의확률이 0.01로 귀무가설은 기각되나 유사도가 낮아 상관관계는 없다고 할 수 있다.

물리적 보안 부분의 예산 대비 집행실적을 제외한 나머지 금액과 물리적 부분의 결함수는 무관한 것으로 확인되었다. 그 원인을 분석해 본 결과 물리적 보안 부분의 감사는 결함수가 상대적으로 적으며(관리적 보안 결함에 비해 14%, 기술적 보안 결함에 비해 19%), 예산집행과 무관하게 긴급히 투자가 집행되는 경우가 많고 통계적 접근으로는 결함수 편차가 너무 좁아 분석이 어려운 부분인 것으로 확인되었다. 정리하면 결함수가 적고 예산과 무관하게 집행되는 경우가 많은 것이 원인으로 분석된다.

Table 13. Correlation analysis between the number of physical security defects and not execution physical budget

Descriptive Statistics

	Mean	Std. Deviation	N
Not execution physical budget	-,2727	19,61518	66
Physical security defects	2,0909	,79860	66

Correlations

		Not execution physical budget	Physical security defects
Not execution physical budget	Pearson Correlation	1	-,387**
	Sig. (2-tailed)		,001
	N	66	66
Physical security defects	Pearson Correlation	-,387**	1
	Sig. (2-tailed)	,001	
	N	66	66

4.4 정보보호 투자 효과성 분석 모델

각 분야의 상관도를 분석해 본 결과 피어슨 상관계수 기준으로 보안감사 결함수와 예산 미집행액에서의 관리적 부분이 0.857이고 기술적 부분이 0.767로 각각 강한 상관관계가 나타났다. 이는 정보보호에 대한 단순 투자 집행액의 규모보다는 수립된 예산을 충실히 이행하는게 결함수를 줄이는데 효과적인 것을 확인할 수 있다.

또한 유의확률이 0.001 이하인 결함수와 미집행예산에서의 관리적, 기술적 부분이 신뢰도가 높은 결과로 도출되었다.

Table 14. Significant Pearson coefficient

the number of defects VS	classification	Pearson coefficient (|r| 〉=0.7)	significant probability (p〈=0.05)
Not execution administrative budget	Bm-IPm	0.857	0.001
	Bt-IPt	0.767	0.001

6개 분야의 상관분석된 데이터 중 유사도 기준치(0.7)를 만족하는 분야를 선택하여 예산과 투자가 모두 반영된 영역의 효과 검증 모델을 도출하기 위해서 관리적 부분과 기술적 부분은 입력 값을 예산액과 집행액의 차액으로 하고 출력 값을 결함수로 하여 분야별로 회귀 분석하였다.

먼저 관리적 부분의 회귀분석 결과는 유의확률이 0.001 이하로 회귀식이 신뢰성을 가지며 관리적 보안의 검증 모델은 아래와 같다.

Table 15. Regression analysis among the number of administrative security defects and administrative security budget and administrative security investment performance

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1031,459	1	1031,459	177,197	,000[b]
	Residual	372,541	64	5,821		
	Total	1404,000	65			

a, Dependent Variable: The number of administrative security defects

b, Predictors: (Constant), Not execution administrative budget

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8,904	,546		16,315	,000
	Not execution administrative budget	2,253	,169	,857	13,312	,000

a, Dependent Variable: The number of administrative security defects

Table 16. The formula for administrative security vulnerability level validation

$$Y_m = 2.253(X_1 - X_2) + C$$

Y_m : $The\ number\ of\ administrative\ defects$
X_1 : $Administrative\ security\ budget$
X_2 : $Administrative\ security\ investment\ cost$
C : $constant\ (=8.904)$
(※X_1, X_2 $Unit$: $Million\ won$)

기술적 부분의 회귀분석 결과는 유의확률이 0.001 이하로 유의기준 0.05를 만족하여 회귀식이 타당하며 기술적 보안영역의 모델링을 제안한다.

Table 17. Regression analysis between the number of technical security defects and technical security budget and technical security investment performance

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	317,424	1	317,424	91,273	,000[b]
	Residual	222,576	64	3,478		
	Total	540,000	65			

a, Dependent Variable: The number of technical security defects

b, Predictors: (Constant), Not execution technical budget

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6,324	,541		11,697	,000
	Not execution technical budget	,183	,019	,767	9,554	,000

a, Dependent Variable: The number of technical security defects

Table 18. The formula for technical security vulnerability level validation

$$Y_t = 0.183(X_1 - X_2) + C$$

Y_t : $The\ number\ of\ technical\ defects$
X_1 : $Technical\ security\ budget$
X_2 : $Technical\ security\ investment\ cost$
C : $constant\ (=6.324)$
(※X_1, X_2 $Unit$: $Million\ won$)

위 두 가지 모델을 분석해 보면 미집행실적의 민감도가 관리적 영역에서 약 10배 이상 높다는 것을 확인할 수 있으며 이는 곧 관리적 보안 영역에서의 정보보호 투자가 다른 영역보다 결함수에 더 민감한 부분임을 알 수 있다.

단, 제한사항은 매출 500억 규모의 IT서비스 업종에서 정보보호 전담조직이 정보보호 관리체계를 운영하며 반기별 평균 20개에서 30개 정도의 결함수가 발생하는 기업이 기준이며 제안된 모델을 통해서 예산과 투자 정보만으로 기업의 정보보호 관리체계 취약성 정도를 예측할 수 있다.

V. 결 론

5.1 연구 결과 요약 및 시사점

점점 더 다양해지는 해킹 기법과 규제의 복잡성으로 인해 기관이나 기업들은 정보보호 투자에 골머리를 앓고 있다. 이러한 정보보호 책임자의 고민 속에서 최적의 정보보호 투자를 위한 의사 결정 기준이나 정보보호 투자의 효과 분석에 대한 연구가 국내외에서 진행되어 왔으나 이들 연구의 대부분은 가설과 설문에 기반한 통계학적 자료로 정보보호 산업에 대해 실질적인 효과를 증명하는데 있어 제약점이 있었다.

반면 본 연구는 정보보호 관리체계를 지속적으로 유지하고 정보보호 조직 또는 인력 변동 등의 다른 변수가 최소화되어 있는 환경에서 실질적인 정보보호 관련 재무수치와 감사 결함과의 관계를 관리적, 기술적, 물리적 분야별로 세분화하여 시간 추이에 따라 유사도 분석을 실시함으로써 정보보호 투자의 효과 및 상관계수를 정량적으로 실증 분석하고 정보보호 투자에 대한 효과를 검증하였다.

그리하여 다음과 같이 연구 분석결과를 요약하고 시사점을 제시하고자 한다.

첫째, 순수 정보보호 투자 집행액과 감사 결함수와의 관련성은 낮지만 예산 미집행액(예산액-집행액)과 감사 결함수의 상관관계는 높다. 즉 수립된 정보보호 예산을 임의로 조정하거나 삭감하게 되는 경우 뿐만 아니라 정보보호 예산을 예정된 시기에 집행하지 못하는 경우에도 정보보호 관리체계가 취약해 질 수 있다는 것을 알 수 있다.

둘째, 감사 결함수와 예산 미집행액 관계 중에서도 관리적 보안영역과 기술적 보안영역에서 강한 양(+)의 선형관계로 나타난다. 계획된 예산을 집행하지 못하였을 경우 물리적 보안영역 보다는 관리적 보안영역과 기술적 보안영역에 결함이 나타날 수 있다는 것을 확인하였다.

셋째, 관리적 보안영역의 예산 미집행액이 기술적 보안영역의 예산 미집행액보다 결함에 미치는 영향이 크다. 과거 보안 솔루션 중심의 정보보호 투자보다는 정보보호 교육, 보안컨설팅 등과 같은 관리적 보안투자에 더 비중을 높여야 전체 정보보호 관리체계 수준을 높이는데 효과적이다라는 의미이다.

따라서 예산에 기반한 정보보호 투자는 관리적/기술적 보안영역에서 정보보호 관리체계 수준 향상에 효과가 있으며, 예산집행시 관리적 보안영역을 우선 순위로 하는 것이 효율적일 것이다.

5.2 향후 연구 방향

본 연구에서 정보보호 관리체계를 운영하는 기업의 적절한 정보보호 투자는 정보보호 관리체계의 수준 향상에 긍정적 영향이 있다는 것을 실증분석을 통해 확인하였다. 향후에는 본 연구에서는 확인할 수 없었던 물리적 보안 부분에 대한 연구와 제안한 방법론을 보완하여 업종별 그리고 기업규모별로 그 특성을 반영하여 정보보호 투자 예산 마련과 투자 집행에 대한 효과 검증에 도움이 되는 연구가 지속되어야 할 것이다.

References

[1] Hankyoreh News, Jan. 23. 2014. http://www.hani.co.kr/arti/politics/assembly/621197.html

[2] KISA, "2014 National Information Security White Paper," Apr. 2014.

[3] Ministry of Science, "Information Security industrial development agenda of comprehensive plan," ICT Future Planning, Jul. 2013.

[4] KISA, "Information Security Survey 2013," Dec. 2013.

[5] Roper, C.A., "Risk Management for Security Professionals", Butterworth-Heinemann, Boston, MA, pp.83-96, 1999.

[6] Blakley, B., "Returns on Security Investment: an Imprecise but Necessary Calculation," Secure Business Quarterly, Vol. 1, No. 2, 2001.

[7] Harris, S., CISSP All-in-One Exam Guide, McGraw-Hill, New York, NY, 2001.

[8] Jeong-deok Kim and Jeong-Eun Park, "Based on information security ROI TCO (ROSI) study," The Society of Digital Policy & Management, Founding Conference, pp.251-261, Dec. 2003.

[9] Jong-seon Lee and Hui-Ho Lee, "Using the TCO-based Security ROI information security investment performance and evaluation method", Korea Information Processing Society, Conference, pp.1125-1128, Aug. 2007.

[10] Young-Tek Jo, "Study on Improving the information protection level by Integrated Evaluation Items(IEI)" pp.53-63, Aug. 2004.

[11] Witty R.J, et al., "The Price of Information Security," Gartner Inc., Stamford, CT, 2001.

[12] Gordon, L.A. and Loeb, M.P., "The Economics of Information Security Investment," ACM Transactions on Information and System Security, Vol.5, No.4, pp.438-457, Nov. 2002.

[13] Cavusoglu, H.(Hasan), Cavusoglu, H.(Huseyin) and Raghunathan S., "Economics of IT Security Management: Four Improvements to Current Security Practices," Communications of the

Association for Information System, Vol.14, pp.65-75, 2004.
〔14〕 Cavusoglu, H., Mishara, B. and Raghunathan, S., "A Model for Evaluating IT Security Investments," Communications of the ACM, Vol.47, No.7, pp.87-92, Jul. 2004.
〔15〕 Jin Kim, "Study on the Differences of Priority between Information Protection Importance and Security Investment," pp.34-43, Feb. 2014.
〔16〕 Chul-hwan Jang, "Factors that Affect Selection of Information Security Countermeasures," pp.28-30, Feb. 2014.
〔17〕 Scott, D., Security Investment Justification and Success Factors, Gartner Inc., Stamford, CT, 1998.
〔18〕 Leem, C.S. and Kim, S. "Introduction to an Integrated Methodology for Development and Implementation of Enterprise Information Systems," Journal of Systems and Software, Vol. 60 No. 3, pp.249-261, Feb. 2002.
〔19〕 Davis, A., "Return on Security Investment-Proving It's Worth It," Network Security, Vol. 2, pp. 8-10, 2005.
〔20〕 Han-kil Seon, "Study on the effect of information security policy and organization on the performance of information security," Korea Institute of Information Management, Conference pp.1087-1095, Aug. 2005.
〔21〕 Blatchford, C., "Information Security Controls-Are They Cost-effective," Computer Audit Journal, Vol. 3, pp. 11-19, 1995.
〔22〕 Ki-hyang Hong, "Study on the Effect of Information Security Controls and Processes on the Performance of Information Security," kookmin University Ph.D. paper, pp. 138-141, Feb. 2004.
〔23〕 Sang-hoon Nam, "Empirical Study on the Impact of Security events to the Stock Price in the Analysis method of Enterprise Security Investment Effect," Korea University Ph.D. paper, pp. 80-102, Feb. 2006.
〔24〕 Young-ok Kwon, "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Seoul University, paper of masters degree, pp.44-46, Aug. 2005.
〔25〕 Young-ok Kwon and Byung-do Kim, "The Effect of Information Security Breach and Security Investment Announcement on the Market Value of Korean Firms," Information Systems Review, 9(1), 1, pp.105-120, Apr. 2007.

〈저자소개〉

정 성 훈 (Seong Hoon Jeong) 정회원
2003년 2월: 부경대학교 기계자동차공학부 졸업
2009년 9월~현재: 고려대학교 정보경영공학과 석사과정
〈관심분야〉 정보보호 관리체계, 보안감사, 위험관리, 정보보호정책

윤 준 섭 (Jun Seob Yoon) 정회원
2014년 2월: 중앙대학교 컴퓨터공학부 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 관리체계, 위험관리, 정보보호정책

임 종 인 (Jong In Im) 정회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 안전행정부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

이 경 호 (Kyung Ho Lee) 정회원
1989년 8월: 서강대학교 수학학사
1997년 8월: 서강대학교 정보통신대학원 네트워크공학석사
2009년 7월: 고려대학교 정보경영대학원 박사
2011년 8월:~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험평가·관리, 정보보호 관리체계, 개인정보보호, 개인정보영향평가