http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.2, May 2015, pp.27-36
http://dx.doi.org/10.7838/jsebs.2015.20.2.027

보안교육과 보안관리 역량의 상관관계 분석: 인가된 내부자 기밀유출사례를 중심으로

An Analysis of Relationship between Industry Security Education and Capability: Case Centric on Insider Leakage

이치석(Chi-Seok Lee)*, 김양훈(Yanghoon Kim)**

초 록

국가 상대로 한 국가기밀유출과 더불어 최근 산업 기술유출은 점점 늘어가고 유출의 범위가 기술유출 중심에서 정보통신, 전기전자, 방위산업, 전략물자 불법수출, 외국의 경제 질서교란, 지식재산침해 등 신 경제안보 분야로 다양화되는 추세로 유출 피해는 유출된 기업에 피해를 줄 뿐만 아니라 국가의 이익과 국내 산업 전반에 영향을 끼칠 수 있다. 국가정보원 산업기밀보호센터 통계에 따르면, 기술유출의 주된 원인은 해킹과 악성코드와 같이 외부에 의한 것뿐 아니라 전・현직직원 등 내부유출이 약 80%를 차지하며, 협력업체 의한 기술유출이 뒤를 이어 금전유혹과 개인의 이익으로 인한 기술유출이 계속해서 꾸준히 증가하고 있다.

그러나 그간의 연구들은 핵심자산 유출을 방지하기 위하여 기업의 보안역량을 측정하거나, 관리를 위한 측정지표를 개발하는 연구가 주를 이루고 있었으며, 가장 핵심이 되는 기업 구성원들의 보안활동에 대한 기초연구가 미흡한 상황이다. 따라서, 본 연구에서는 보안 활동에 가장 기초가 되는 보안교육이 기업의 보안역량에 미치는 영향에 대해 분석하였다. 그 결과, 보안교육은 보안역량에 양(+)의 상관관계를 나타내는 것으로 분석되었다.

ABSTRACT

Current leakage of industrial technologies with revealing state secret against nation is gradually increasing and scope of the spill is diversified from technology-oriented leakage to new economic security sector like information and communication, electrical and electronic, defense industry, illegal export of strategic material, economic order disturbance by foreign country, infringement of intellectual property, etc. So the spill damage can affect not only leaked company but also national interests and entire domestic industry. According to statistics from National Industrial Security Center of National Intelligence Service, a major cause of technology leakage is not only by external things about hacking and malignant code, but internal leakage of former and current employees account for about 80%. And technology leakage due to temptation of money and personal interests followed by technology leakage of subcontractor is steadily increased.

* First Author, Department of Knowledge Information Security Management, SangMyung University (sundolri5555@daum.net)
** Corresponding Author, Department of Cyber Security, Far east University(yhkim@kdu.ac.kr)
Received: 2015-03-11, Review completed: 2015-04-09, Accepted: 2015-04-10

Most studies in the field of security have tended to focus on measuring security capability of company in order to prevent leakage core assets or developing measurement Indicators for management rather than security activities of the company members that is most important. Therefore, this study analyzes the effect of most underlying security education in security activities on security capabilities of enterprise. As a result, it indicates that security education have a positive(+) correlation with security capabilities.

키워드 : 보안관리, 보안 역량, 교육훈련, 내부자 유출
Security Management, Security Capability, Education & Training, Insider Leakage

1. 서 론

급속히 변화하는 경영환경 속에서 기업들은 전략적 우위를 점하기 위한 선결조건으로 기업의 정보화를 수립하고 있다[1~3, 6]. 이는 단순한 기업 경영환경의 변화가 아니라 생산성 향상과 거래비용 절감을 통한 기업 경쟁력 확보의 한 수단으로써 자리매김하고 있다[4, 5]. 기업의 정보화는 순기능적으로 지식과 정보를 활용하는 경제사회 전반에 걸쳐 고 부가가치 화를 이루고 있는 핵심근본이며, 이를 통해 시장의 높은 불확실성을 대응할 수 있는 능력을 갖추게 된다[11]. 그러나 기업의 핵심자산이 정보화 되고, 사물인터넷 환경 및 융합 환경 등 새로운 환경의 도래로 인하여 안전하게 보호되어야 할 산업기술이 IT와 융합되어 경쟁기업이나 해외로 손쉽게 유출되고 있다[7, 8].

최근에는 기업뿐만 아니라, 국가 상대로 한 국가기밀유출과 더불어 산업기술유출은 점점 늘어가고 유출의 범위가 기술유출 중심에서 정보통신, 전기전자, 방위산업, 전략물자 불법수출, 외국의 경제 질서교란, 지식재산침해 등 신 경제안보 분야로 다양화되는 추세를 보이고 있다[10, 12]. 또한, 유출 피해는 유출된 기업에 피해를 줄 뿐만 아니라 국가의 이익과 국내 산업 전반에 영향을 미치고 있다[13~15]. 국가정보원 산업기밀보호센터 통계에 따르면, 기술유출의 주된 원인은 해킹과 악성코드와 같이 외부에 의한 사이버공격과는 별개로 전·현직직원 등에 의한 내부유출이 약 80%를 차지하며, 협력업체 의한 기술유출이 뒤를 이어 금전유혹과 개인의 이익으로 인한 기술유출이 계속해서 꾸준히 증가하고 있는 추세이다.

이러한 보안사고 문제를 해결하기 위한 기존의 보안활동은 보안 시스템의 도입·구축을 통한 기술적 측면의 보안대책이 주로 검토되었다. 그러나, 최근에 발생하고 있는 첨단 기술 활용을 통한 사고추적의 어려움과 내부자의 정보유출 등의 보안사고의 특성을 고려해 볼 때 이러한 접근방법은 한계성이 있다[16]. 특히, 아무리 첨단의 보안 시스템이 다중으로 구축되어 있다 하더라도 기업 내 구성원의 악의적인은 행동은 기업의 핵심자산을 쉽게 유출할 수 있다.

그러나 그간의 연구들은 핵심자산 유출을 방지하기 위하여 기업의 보안역량을 측정하거나, 관리를 위한 측정지표를 개발하는 연구가 주를 이루고 있었으며, 이와 별도로 보안 교육 프로그램에 대한 연구가 진행되고 있었다[9]. 이러한 연구들을 기반으로 기업의 보안 교육과 기업의 보안역량을 별개의 요소가 아닌 연계된 속성으로 인지하고, 기업의 보안역량을 구성하는 기본 속성에 대한 연구가 필요한 시

점이다.

따라서, 본 연구에서는 보안 활동에 가장 기초가 되는 보안교육이 기업의 보안역량에 미치는 영향에 대해 분석하고자 한다. 세부적으로, 중소기업청에서 발표한 중소기업 기술보호 역량 및 수준 조사 결과를 분석하고, 이를 기반으로 보안 교육에 따른 보안 역량의 상관관계를 분석하여, 보안 역량을 향상시키기 위한 제언을 하고자 한다.

2. 중소기업 보안 현황

2008년부터 2010년까지 기술유출 경험이 있다고 응답한 기업은 161개사로, 전체 표본기업 1,529개사 중 10.5%를 차지하였다. 기업유형별로는 대기업 11.1%, 중소기업 10.0%, 벤처기업 11.6%가 각각 기술유출을 경험했다고 응답하였다. 기술유출 경험이 있는 기업들을 대상으로 추가적인 설문을 진행한 결과, 1회성의 기술유출 사고를 경험한 기업은 64.0%이며, 2회 이상 반복적으로 기술유출 사고를 경험한 기업도 36.0%에 이르는 것으로 조사되었다. 기술유출 경험이 있는 기업들의 평균적인 기술유출 사고 횟수는 1.6건으로 산출된다. 기업유형별로는 대기업 2.2건, 중소기업 1.6건, 벤처기업 1.5건으로 분석되었다.

기술유출 사고 1건당 평균 피해금액은 16.6억 원이며, 대기업은 31.4억 원, 중소기업은 10.2억 원, 벤처기업은 24.7억 원으로 조사되었다. 기업규모에 비하여 상대적으로 피해손실이 큰 기업은 벤처 기업으로 조사되었다. 세부적으로, 기술유출 경험이 있는 중소기업과 벤처기업들의 평균 매출규모는 116.5억 원으로 조사되었다. 이에 따라, 전체 매출금액의 약 12%가 기술유출로 인한 피해손실금액인 것으로 추정된다. 또한 벤처기업 기업만의 매출규모는 82.7억 원으로 조사된다. 이에 따라, 전체 매출금액 대비 29.8%가 기술유출로 인한 피해손실 금액으로 추정된다.

중소기업의 기술유출 관계자는 퇴직임직원(74.5%)의 비중이 압도적으로 높았으며, 경쟁업체 종사자(15.5%), 협력업체 종사자(14.9%) 순으로 조사되었다.

이러한 기술유출 관계자들의 기술유출 수단은 핵심인력 스카우트(42.2%), 복사 및 절취(38.5%), 휴대용 저장장치 분실, 합작사업 및 공동연구(11.2%) 순으로 조사되었다. 인력자체 이동을 통한 기술유출 방법이 도구에 의한 기술유출 방법보다 상대적으로 높은 것으로 분석되었다.

중소기업의 기술유출 발생 후에 보안관리 개선이 되었다는 비율이 과반수 이상(57.8%)으로 높게 나타나, 기업들이 기술유출 사고에 대한 중요성 인식 및 경계심 등이 확산된 것으로 조사되었다.

기술유출 사후조치로서 관계자(사) 고발 37.9%로 조사되었으며, 연구소 내 보안관리 시스템의 강화도 26.7% 수행된 것으로 조사되었다. 그러나 특별한 조치를 실시하지 않은 기업도 여전히 33.5% 수준으로 조사되었다. 부가적으로 최근 2년 이내에 퇴직자가 경쟁업체에 전직했다는 응답비율은 14.7%로 나타났다. 대기업의 퇴직자 전직비율은 37.0%로 타 기업유형에 비해서 상대적으로 높은 것으로 조사되었다.

기업들은 기술유출 발생 원인으로 보안관리 및 감독체계 허술이 56.3%, 임직원 보안의식 부족이 52.4%, 개인적인 재산상 이익추구가

27.6% 순으로 응답하였다. 세부적으로 중소기업 및 벤처기업의 경우 영세성으로 인한 보안 비용 투자곤란이 각각 20.7%, 17.6%로써 이에 대한 애로가 대기업에 상대적으로 높게 나타났다. 따라서 별도의 고비용의 보안 시스템 구축보다 상대적 저비용의 기업 구성원들에 대한 보안의식 강화 및 보안관리 체계 구축이 경영자원이 부족한 중소/벤처기업에게는 효율적인 보안 전략으로 채택될 수 있을 것으로 기대된다.

기술유출 방지에 투자하고 있다고 응답한 기업은 63.4% 수준이었다. 벤처기업(68.5%), 중소기업(61.7%), 대기업(51.9%)인 것으로 조사되었다. 그리고 기술유출 방지를 위한 평균 투자금액은 19.5백만 원으로 조사되었다. 세부적으로 대기업 128.8백만 원, 중소기업 17.7백만 원, 벤처기업 13.4백만 원으로 조사되었다.

3. 보안 교육과 보안관리 역량의 상관관계 분석

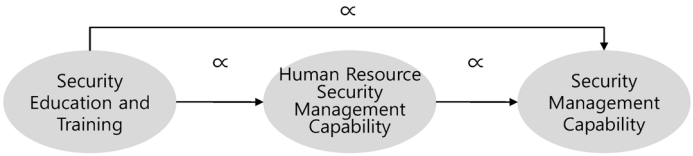
3.1 상관관계 분석 조사설계 및 모형설계

본 연구에서는 보안 교육과 보안관리 역량의 상관관계 분석을 위하여, '중소기업 산업기밀관리 실태조사' 결과보고서에서 제시하는 산업보안 역량평가 Framework의 모형과 문항별 점수표를 참조하고 조사 대상을 중소기업군과 대기업 군으로 분류하여 내부자 기밀유출 경험이 일부 있는 기업들을 포함한 100개의 기업들을 대상으로 조사·분석하였다. 교육 현황은 내부인원과 외부인원으로 분류하여, 내부인원은 신규 입자사, 재직자, 퇴사자에 대한 교육실시 현황을 확인하였고, 외부인원은 협력업체 및 외국인들의 교육실시 현황에 대해 조사하여 100점 환산으로 구성하였다. 인적자원관리 역량은 10개 문항으로 구성하여 인적자원들의 보안활동, 보안서약서, 지침 이행, 퇴직자 관리에 대하여 조사하여 100점 환산으로 구성하였다. 마지막으로 보안역량은 선행연구를 통해 조사된 보안 규정, 보안 조직, 사고 및 대응, 인적자원관리, 자산관리, 시설관리, IT 보안관리를 대분류 기준[11]으로 조사하여 총 100점으로 구성하였다. 이와 같은 구성을 기반으로 본 논문에서는 아래의 내용을 기반으로 하여 <Figure 1>과 같은 상관관계를 규명해보고자 한다.

가설 1: 보안교육의 빈도와 시간이 많을수록 인적자원관리역량이 높을 것이다.

가설 2: 인적자원관리역량이 높을수록 보안관리역량이 높을 것이다.

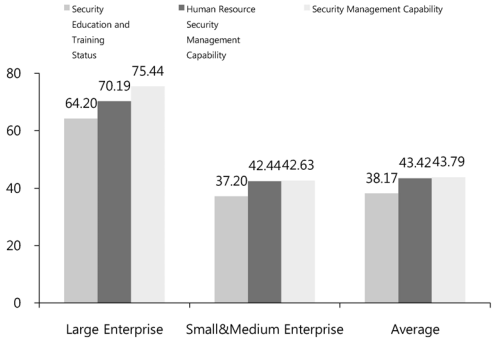
가설 3: 보안교육의 빈도와 시간이 많을수록 보안역량이 높을 것이다.



〈Figure 1〉 Correlation Analysis Model on Between Security Education & Training and Security Capability

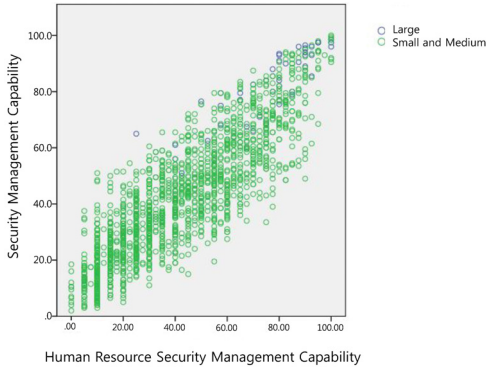
3.2 중소기업 보안 현황 분석

<Figure 2>에서 제시된 바와 같이, 대기업은 전반적으로 보안교육 현황이 중소기업에 비해 우수한 것으로 조사되었다. 기업 별 보안 역량에서 보여지는 것처럼, 대기업 군은 전반적으로 풍부한 보안교육을 운영하고 있으며, 이에 따라, 높은 인적자원관리 및 보안 역량을 보유하고 있는 것으로 조사되었다. 그러나, 높은 보안 역량 수준에 비하여 조금은 낮은 수준으로 인적자원을 관리하고 있으며, 이보다 더 부족한 보안교육을 운영하고 있는 것으로 분석되었다. 중소기업은 인적자원관리 역량과 비슷한 보안역량을 보유하고 있는 것으로 조사되었으나, 인적자원관리역량 및 보안역량에 비하여 조금은 부족한 보안교육을 운영하고 있는 것으로 조사되었다.



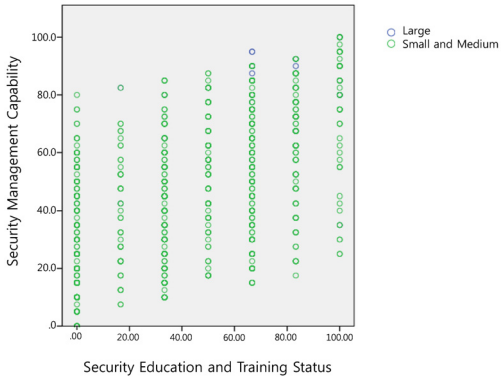
〈Figure 2〉 Enterprise Security Capability

우선, 인적자원관리 역량에 따른 보안역량 분포를 살펴보면, 대기업의 경우 일부 기업들이 낮은 인적자원관리 역량을 보유하고 있으며, 이에 따라 낮은 보안역량을 보유한 것으로 분석된다. 그리고, 중소기업의 경우에는 인적자원관리역량이 전무한 기업들부터 100점의 역량을 보유한 기업들까지 편차를 보이고 있지만, 분포도만을 고려하였을 때 대부분의 기업들이 인적자원관리 역량에 따라 보안역량을 형성하고 있는 것처럼 보인다.



〈Figure 3〉 Enterprise Security Capability according to Human Resource Management (Distribution)

다음으로 교육현황을 살펴보면, 재직자, 퇴직자, 제3자 모든 이해관계자들에게 교육을



〈Figure 4〉 Human Resource Security Management Capability according to Security Education & Training

실시하지 않은 중소기업들이 다수 있는 것으로 조사되었으며, 모든 교육을 철저하게 수행하는 기업들도 분포하고 있는 것으로 분석되었다. 교육현황이 전무하여 인적자원관리역량이 0인 기업부터 모든 보안교육훈련을 수행하여 인적자원관리가 100인 기업까지 다양한 분포를 보였다.

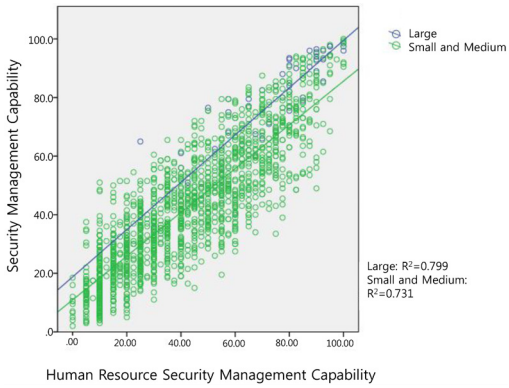
3.3 보안 교육과 보안 역량의 상관관계 분석

보안 교육과 보안 역량의 상관관계를 분석하기 위하여, 우선, 인적자원관리역량과 보안역량의 상관관계를 분석하였다. 종속변수를 보안역량으로 하여, 독립변수를 인적자원관리역량과 교육현황으로 투입한 회귀분석에서, R^2 값은 0.746으로 보안역량은 인적자원관리역량과 교육현황으로 설명력이 충분한 것으로 분석되었다.

〈Table 1〉 Regression Result: Human Resource Security Management Capability - Security Education & Training

R	R^2	d	F	p
.864a	.746	2	2243.863	.000

세부적으로는 인적자원 보안관리 역량(B = 0.724)이 보안교육현황(B = 0.051)에 비하여 보안역량에 많은 영향을 미치는 것으로 분석되었다. 가장 설명력이 큰 인적자원관리역량과 보안역량의 상관관계를 기업 규모에 따라 분석해보면, <Figure 5>와 같이 대기업의 경우 R^2값이 0.799로써 중소기업의 R^2값 0.731보다 설명력이 더 큰 것으로 분석되었다.



〈Figure 5〉 Human Resource Security Management Capability-Security Management Capability: Large Enterprise and Small Medium Enterprise

인적자원관리역량과 비교하여 보안역량에 영향력이 적은 보안교육 현황을 다시 인적자원관리역량에 어떠한 영향을 미치는지 분석해보면 <Table 2>와 같이 분석되었다. 그 결과 교육현황은 인적자원관리역량에 대하여 R^2 값이 0.421만큼 설명할 수 있는 설명력을 가지고 있으며, 0.649만큼 영향을 미치는 것으로 분석되었다.

〈Table 2〉 Regression Result: Human Resource Security Management Capability-Security Management Capability

R	R^2	d	F	p
.649	.421	1	1111.283	.000

4. 결론 및 제언

최근에는 기업뿐만 아니라, 국가 상대로 한 국가기밀유출과 더불어 산업기술유출은 점점 늘어가고 유출의 범위가 기술유출 중심에서 정보통신, 전기전자, 방위산업, 전략물자 불법 수출, 외국의 경제 질서교란, 지식재산침해 등 신 경제안보 분야로 다양화되는 추세를 보이고 있다.

최근에 발생하고 있는 첨단 기술 활용을 통한 사고추적의 어려움과 내부자의 정보유출 등의 보안사고의 특성을 고려해 볼 때 이러한 접근방법은 한계성이 있다.

그러나 그간의 연구들은 핵심자산 유출을 방지하기 위하여 기업의 보안역량을 측정하거나, 관리를 위한 측정지표를 개발하는 연구가 주를 이루고 있었으며, 이와 별도로 보안 교육 프로그램에 대한 연구가 진행되고 있었다.

따라서, 본 연구에서는 보안 활동에 가장 기초가 되는 보안교육이 기업의 보안역량에 미치는 영향에 대해 분석하였다. 그 결과 모든 가설이 채택되었으며 세부적으로 다음과 같이 4가지 의미를 정리하였다.

1. 기업의 보안역량수준을 향상시키기 위하여 기업 구성원(이해관계자) 관리수준의 상관관계와 보안교육의 상관관계를 살펴본 결과 해당 구성요소가 양(+)의 연관성이 있는 것으로 분석되었다. 따라서, 기업의 보안교육과 인적자원관리역량은 보안관리역량수준에 영향을 미치는 것으로 분석되었다.
2. 중소기업은 대기업에 비하여 매우 낮은 보안역량 수준을 보유하고 있으나, 인적자원관리역량에 있어서는 대기업은 평균에 못 미치는 결과를 가져왔지만, 중소기업은 균형잡힌 역량을 보유한 것으로 분석되었다.
3. 기업의 보안역량수준을 향상시키기 위하여 기업의 보안역량수준을 향상시키기 위하여 보안교육활동만으로는 조금 부족한 상황이며, 기업의 인적자원에 대한 체계적인 관리가 필요한 것으로 분석되었다.
4. 높은 수준에 올라와있는 대기업들의 인적자원관리 역량에 대해 향상시킬 필요가 있으며, 그 단초는 다차원적인 보안 교육 실시에서부터 찾을 수 있다.

본 연구에서 진행한 연구를 바탕으로 다음과 같은 보안교육을 위한 제언을 하고자 한다.

1. 가장 기본적으로 국내의 보안은 기술적 보안 위주로 구성되어있다. 이러한 구성에 따라 교육의 많은 부분이 기술적인 보안, 즉, 해킹, 바이러스 등에 대한 위협을 주로 학습한다. 이러한 단방향성 교육을 지양하고 보안교육에 맞는 다차원의 교육 콘텐츠 개발이 시급하다.
2. 해외의 보안 메가 트랜드는 '융합보안'의 형태로 진화하고 있다. 융합보안에는 기존의 기술적, 물리적, 관리적 보안 외에도 기업 간 협업, 커뮤니케이션, 법과 윤리, 범죄 등의 다양한 학문분야를 융합하고 있는 실정이다. 따라서 국내 보안교육을 위해서 기술적, 물리적, 관리적, 인적 보안교육 외에도 학습자들이 근무하는 직종에 맞는 형태의 '산업에 적합한' 형태의 다채로운 교육이 필요하다.

3. 국내의 보안과 관련된 직무 분야인 공학 교육은 혁신적인 '창의 교육', '문제해결중심 교육'으로 변화하고 있다. 기존의 서류 중심의 이해와 학습을 탈피하여, 보안을 무의식/의식적 행동윤리에 스며들 수 있도록 행동하는 보안교육 콘텐츠 개발이 필요하다.

References

[1] Ahn, J. H., Park, J. H., Sung, K. M., and Lee, J. H., "Impacts of Punishment and Ethics Training on Information Security Compliance: Focus on the Moderating Role of Organizational Type," Information Systems Review, Vol. 12, No. 1, pp. 23-42, 2010.

[2] Albrechtsen, E., "A qualitative study of users' views on information security," Computers and Security, Vol. 26, No. 4, pp. 276-289, 2007.

[3] Bae, Y. S. and Chang, H. B., "A Qualitative Research on ICT Policy Design for Small and Medium Business," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 57-70, 2013.

[4] Cha, I. H., "Development of Personnel Security Management for Protection against threat," The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 3, No. 4, pp. 221-232, 2008.

[5] Chang, H. B. and Kim, K. K., "Design of Inside Information Leakage Prevention System in Ubiquitous Computing Environment," Lecture Notes in Computer Science, Vol. 3483, pp. 128-137, 2005.

[6] Cho, M. K., Kim, S. C., Hwang, J. M., and Kim, S. C., "A Study on the Effect of Institutionalization of the Security Education: Survey of National R&D Projects," The Journal of Korean Association of Computer Education, Vol. 17, No. 2, pp. 21-29, 2014.

[7] Choi, J. H., "A Study on the Institutional Improvement Directions of Industrial Security Programs: Focused upon Policies and Practices in the U.S," Korea Security Science Association, Vol. 22, pp. 197-230, 2010.

[8] Choi, M. G., Jeong, J. H., and Kim, J. H., "A Study on the Effects of the Security Perceptions of Top Managers and the Education on the Business Performances," Asia Pacific Journal of Small Business, Vol. 36, No. 2, pp. 209-226, 2014.

[9] Choi, S. T. and Yu, H. C., "A Study on the Establishment of Industrial Security Education Programs in Korea," Korea Security Science Association, Vol. 25, pp. 185-208, 2010.

[10] Kang, J. G., Lim, J. H., Lee, H. J., and Chang, H. B., "A Study on Classification of Information Asset Considering Business Process Characteristics for Small IT Service Organization," The Journal of Society for e-Business Studies, Vol. 16,

No. 4, pp. 97-108, 2011.

[11] Kim, Y. H. and Chang, H. B., “Human centric security policy and management design for small and medium business,” Security and Communication Networks, Vol. 7, No. 10, pp. 1622-1632, 2014.

[12] Kim, Y. H., Moon, J. W., Hwang, S. H. Chang, H. B., “A study on Method of Security Management in the ICT Outsourcing Environment,” Review of Korea Institute of Information Security and Cryptology, Vol. 24, No. 1, pp. 23-31, 2014.

[13] Moon, H. J., “A study on the system and problems of educational training for developing competency of small & medium enterprise in Korea,” Review of Korea Institute of Information Security and Cryptology, Vol. 19, No. 1, pp. 29-39, 2009.

[14] National Intelligence Service, “Industrial technology protection: trace for 5 years gone by,” High Industrial Technology Trend, Vol. 9, pp. 8-145, 2008.

[15] No, M. S. and Lee, S. Y., “Explaining Industrial Security of SMEs in Korea: An Ordered Logit Analysis,” The Journals of Korean Public Administration Review, Vol. 44, No. 3, pp. 239-259, 2014.

[16] Yoo, J. H. and Chang, H. B., “Public IT service strategy for social information security in the intelligence all-things environment,” Electronic Commerce Research, Vol. 14, No. 3, pp. 293-319, 2014.

저 자 소 개

이치석	(E-mail: sundolri5555@daum.net)
1997년	한양대학교 외교안보학전공 (석사)
1998년~2000년	국가정보대학원 부교수 (국가방첩학, 국제범죄)
2012년~2013년	한국산업기술보호협회 상임부회장(총괄 단체장) 및 한국산업보안연구학회 부회장
2012년~현재	한국산업기술대학교 기술정보보호학과 겸임교수 (산업보안학)
관심분야	산업보안, 국가정보, 보안관리

김양훈	(E-mail: yhkim@kdu.ac.kr)
2011년	대진대학교 소프트웨어공학 전공 (박사)
2012년~2013	상명대학교 소프트웨어·미디어 연구소 박사 후 연구원
2014년~현재	극동대학교 사이버안보학과 조교수
관심분야	보안관리, 유출방지, 보안 인식, 소프트웨어 프레임워크