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

The Journal of Society for e-Business Studies
Vol.20, No.3, August 2015, pp.1-10
http://dx.doi.org/10.7838/jsebs.2015.20.3.001

로지스틱 회귀분석을 이용한 중소기업 기술보호 요인 분석

Small Business Technological Assets Protection Factors Analysis Using Logistic Regression Analysis

홍준석(Jun Suk Hong)*, 박원형(Won Hyung Park)**,
김양훈(Yanghoon Kim)***, 국광호(Kwang Ho Kook)****

초 록

본 연구는 중소기업청에서 실시한 2013년 중소기업 기술보호 역량 및 수준조사를 바탕으로 중소기업의 기술유출 경험유무와 기술보호 요인을 분석하여 정부지원을 통한 기술유출방지 효과를 극대화 할 수 있는 핵심 요인을 도출하고자 한다. 중소기업 기술보호 역량 및 수준조사 대상 1,561개 기업 중 대기업 43개를 제외한 1,518개 중소기업 중 기술유출 중소기업 155개와 미유출 중소기업 1,363개 중소기업에 대해 기술보호 요인을 로지스틱 회귀분석 하였다. 기술유출 관련 요인을 분석한 결과, 출입자 통제 시스템 운영, 보안감사 실시여부, 임직원 부재 시 보안활동, 중요자료 보호대책 마련이 핵심요인으로 도출되었으며, 이들 사항에 대해 정부차원에서 집중적인 지원이 이루어진다면 기술보호 효과가 극대화 될 수 있을 것으로 사료된다.

ABSTRACT

The main objective of this study was to identify the factors that can maximize the effect of preventing technology leakage by government support. Therefore we used the 2013 small business technology protection capabilities and level of research which is conducted by the Small and Medium Business Administration, and have analyzed the presence of small business technological assets leakage protection eand skills. Multiple logistic regression analysis was performed to identify 1,518 small companies (43 big companies are excluded) which are divided into 155 technological assets leaked small business and non-leaked 1363 small business. The most important factors associated with technology leakage were entrant control system, security audit, employee absence of security activities and important data protection measures. This result shows that if the government can support more for these details, technological asset leakage prevention effect is expected to be maximized.

키워드 : 중소기업, 기술유출, 기술보호, 로지스틱 회귀분석
Small Businesses, Technology Leakage, Technology Protection, Logistic Regression

* Fist Author, Graduate School of Public and Information Technology, Seoul National University Of Science & Technology(hjsjun0817@naver.com)
** Co-Author, Department of Cyber Security, Far East University(whpark@kdu.ac.kr)
*** Co-Author, Department of Cyber Security, Far East University(yhkim@kdu.ac.kr)
**** Corresponding Author, College of Business and Technology, Seoul National University Of Science & Technology(khkook@seoultech.ac.kr)
Received: 2015-04-13, Review completed: 2015-06-29, Accepted: 2015-07-07

1. 서 론

2013년 우리나라의 세계 수출시장 점유율 1위 품목은 65개이고 세계 순위도 12위로 조사됐다. 1위 제품은 메모리 반도체, 자동차 부품, 탱커 등 65개로 조사되었다. 그러나 2013년 우리나라가 세계 수출시장 점유율 1위를 기록하고 있는 제품 65개 중 세계 수출시장 점유율 2위를 차지하고 있는 중국, 미국, 일본 등과 1위 제품 중 절반인 37개 제품에서 상위 3개국이 우리와 경쟁하고 있는 것으로 나타났다. 이처럼 해외시장에서 1위를 지키기 위한 치열한 경쟁이 이루어지고 있다[13]. 이러한 기술발전을 해 나가기 위해서 정부와 기업차원에서 많은 R&D 투자가 이루어지고 있다. OECD 국가 중 우리나라는 전체 R&D 투자의 국내총생산(GDP) 대비 비중은 4.03%로 이스라엘(4.38%)에 이어 2위(핀란드 3.78% 3위, 일본 3.39% 4위)이며, 민간 R&D 투자의 GDP 대비 비중도 3.09%로 이스라엘(3.51%)에 이어 2위를 기록(핀란드 2.66% 3위, 일본 2.61% 4위)하였다[17]. 우리나라가 이처럼 지속적인 R&D 투자로 끊임없는 기술개발을 통해 우리나라 대기업 및 중소기업의 기술력도 나날이 높아지고 있다. 특히 중소기업은 우리경제에서 많은 역할을 하고 있다. 2013년 기준으로 우리나라 중소기업 사업체 수는 약 341만 개이며 전체 사업체의 99.9%이며, 1,342만 명이 근무하고 있어 전체 사업체 근로자의 87.5%에 해당되며, 2012년 중소제조업의 부가가치는 239.3조 원이며 생산액은 717.2조 원으로 전체의 45.7%를 차지하고 있다[2]. 이처럼 중소기업이 우리나라에서 경제 측면의 비중이 커지는 것과 다르게 중소기업 기술보호 수준은 매우 취약하다. 국가정보원에 따르면 2009년부터 2013년까지 전체 기술유출 발생 209건 중 중소기업에서 151건이 발생하여 73%를 차지하고 있고[15], 기술유출 피해규모도 2008년 건당 9.1억 원에서 2013년에는 16.9억 원으로 증가하였다[20]. 이러한 중소기업의 기술유출이 심각해지면서 정부 차원에서 여러 가지 기술보호 지원을 하고 있다. 산업자원통상부에서는 산업기술유출방지법을 제정하여 산업기술보호 실태조사, 산업보안 교육 및 인력양성 등을 지원하며, 공정거래위원회에서는 하도급거래 실태조사 시 기술탈취 여부에 대해 조사하고 있으며, 경찰청에서는 산업기술유출수사 지원팀을 신설하여 운영하고 있다. 특허청에서는 영업비밀보호법과 원본증명제도, 표준관리시스템 보급 사업을 추진하고 있다. 중소기업청에서는 중요자료의 기술임치, 상담・컨설팅, 온라인 보안관제, 기술 유출방지시스템 지원 사업 등 다양한 사업을 추진하고 있다.

그러나 지금까지 기술유출 방지 대응전략은 주로 사후 대응 측면이 강하므로, 현재 시행되고 있는 정부차원의 기술유출방지사업의 성과를 높이기 위해서는 중소기업 기술보호 수준에 대한 정확한 평가를 바탕으로 기술유출방지 효과를 증대할 수 있는 부분에 지원 해줌으로써 기술보호 효과를 극대화 할 수 있을 것이다.

중소기업청에서는 중소기업 및 대기업을 대상으로 중소기업 기술보호 역량 및 수준조사를 통해 해마다 중소기업의 기술유출 실태 및 기술보호 수준을 파악하고 있으며, 이 결과를 활용하여 기술보호정책 개발, 지원 방안 마련에 이용하고 있다. 본 연구는 2013년 중소기업 기술보호 역량 및 수준조사를 바탕으로 로지스틱 회귀분석을 이용하여 중소기업의 기술유

출 유무와 관련된 기술보호 요인을 분석하여 정부지원을 통한 기술보호 효과를 극대화 할 수 있는 요인을 도출하고자 한다.

2. 관련 연구

2.1 이론적 배경

2013년 중소기업 기술보호 역량 및 수준조사에서는 1,518개 중소기업의 보안담당자를 대상으로 기술보호 역량 수준조사를 실시하였다. 중소기업의 기술보호 역량 수준은 43.3점으로 취약 수준으로 나타났으며, 최근 3년간 기술유출 경험은 평균 10.2%로 조사되었으며, 건당 피해금액은 16.9억 원으로 조사되었다. 유출자의 74.8%는 퇴직임직원이며, 기술유출 후 56.1%는 국내 중소기업으로 이직하였고 37.4%는 창업을 하는 것으로 조사되었다. 기술유출 유형은 생산중인 제품 52.9%, 설계도면 36.8% 등이 유출빈도가 높았고, 기술유출에 대한 사후 대응으로는 관계자의 고소, 고발이 36.8%로 가장 많았으며, 특별한 조치를 미실시 한다는 답변도 35.5%로 나타나 많은 중소기업에서는 사후 대응을 전혀 못하고 있는 것으로 조사되었다[20].

2009년부터 2013년까지 경찰청에서 발표한 산업기술 불법유출 검거 실적을 보면 총 검거건수는 407건이며 해외유출 95건, 국내유출 312건으로 4분의 3 이상이 국내유출이었고 검거인원은 719명에 이르고 있다[9]. 연도별 추세를 보면 2009년 검거 건수 46건에서 해마다 증가하여 2012년, 2013년에는 100여 건의 기술유출 검거 실적을 기록하였다. 2010년의 경우 산업기술유출로 검거된 40건의 피해액은 9조 2000억 원으로 유추되고, 국내 유출 31건, 해외유출 9건이 발생하였다. 해외유출은 중국 7건, 인도 2건 등 모두 아시아지역 중에서도 일부 국가로 한정되어 유출되었다[8].

〈Table 1〉 The number of Technology Leakage and Tracking

YEAR		2009	2010	2011	2012	2013
NIS	ALL	43	41	46	30	49
	small businesses	41	30	37	24	31
technology leakage	Average	1.8	1.6	1.6	1.6	1.5
	empirical rate	14.7	13.2	12.5	12.1	10.2
	amount	10.2	14.9	15.8	15.7	16.9
Arrest result	ALL	46	40	84	140	97
	internal	30	31	60	113	78
	foreign	16	9	24	27	19

2.2 선행 연구

중소기업의 기술보호는 정보보호 분야에서 연구가 시작되었다. 이정우는 중소기업 정보보호관리 모델을 연구하였으며[11], 김정덕은 중소기업 보호체계를 제시하였다[5]. 김종기는 기업 규모에 따라 자산, 위협, 취약성, 사용자 등 여러 가지 보호에 대한 직원의 인식 차이를 연구 하였고[6], 문현정은 중소기업의 보안교육을 분석하였다[12]. 박춘식은 일본 정보보호 가이드라인을 분석하여 중소기업에서 적용 할 수 있는 기술보호의 관리・정책・기술 대책을 제시하였다[18].

2010년부터 다양한 방식의 중소기업의 기술보호 연구들이 진행 되었다. 노민선은 중소기업의 기술유출이 심각하며, 중소기업의 보안 역량을 연구하여 기술유출 기업의 보안상담 지원을

통한 기술보호 강화, 정부지원 R&D 사업 참여 기업에 대한 보안 강화, 중소기업 기술보호 지원을 위한 정부 예산 증대 등을 중소기업 기술보호를 위한 정부 정책으로 제시하였다[16]. 남재성은 중소기업의 기술 유출 분석을 통해 중소기업의 기술유출 피해의 심각성을 확인하고, 중소기업의 기술보호를 위해서는 중소기업의 보안설비 구축의 정부 지원 확대, 국가 차원의 기술유출 피해보상 보험 검토, 기술유출 수사 강화, 기소 전 몰수 보전제도 이용, 중소기업 임치제도 증대 등을 제시하였다[14].

박정구는 중소기업의 기술유출실태와 중소기업 기술보호에 관한 현행 법제도를 통해 시행되고 있는 중소기업 기술보호 지원 정책과 특징을 살펴보고 체계적인 중소기업 기술보호를 위해 다수의 집행기관 간 효율적 지원시스템 구축 필요하고, 중소기업 경쟁력 강화정책으로서의 중소기업 기술보호지원제도가 확립이 필요하며 수요자인 중소기업 중심의 지원제도의 체계 및 내용 정비를 제시하였다[19].

2.3 로지스틱 회귀분석

로지스틱 회귀분석은 종속변수가 범주 혹은 명목척도 일 때 사용하는 분석방법이다. 로지스틱 회귀분석은 모형은 종속변수가 0 또는 1이라는 변수로 나타나며, 설명변수는 양적인 변수를 분석하며, 종속변수가 나타날 수 있는 확률값을 분석한다. 그러므로 로직스틱 회귀분석은 사건발생 가능성을 나타낸다. 로지스틱 회귀분석의 추정된 모형적합성은 우도값으로 검정되며, 이 값이 낮을수록 적합하다고 나타나므로 로지스틱 회귀분석의 데이터의 분석모형 적합 여부를 확인할 수 있는 적합도 평가척도라고 할 수 있다. 적합도 방식의 통계량은 χ^2으로 주어지며, 유의확률의 값이 0.05보다 작아야 통계모형이 올바르다는 귀무가설을 채택할 수 있다[7].

3. 연구 방법

3.1 연구 대상 및 연구자료

본 연구는 중소기업청에서 2013년도에 실시한 중소기업 기술보호 역량 및 수준조사의 대상인 1,561개 기업 중 43개 대기업을 제외한 1,518개 중소기업의 자료를 분석하였다. 이 중에서 기술유출 경험이 있는 155개 중소기업과 기술유출 미경험 중소기업 1,363개에 대해 구분하여 기술유출 요인에 대해 분석하였다.

중소기업 기술보호 역량 및 수준조사의 조사내용은 기술보호 역량 및 수준, 기술유출 실태, 기술유출 피해보험제도 도입에 대한 의견 관련 질문, 정책지원 관련 활용실태 및 수요, 회사 일반현황 총 5개 영역으로 구성되어 있고, 기술 보호 역량 및 수준 부문은 보안규정의 제정 및 공포, 보유자산에 보안등급을 관리하는지 여부를 확인하는 보안 정책 수립부문과, 보안규정의 제정 및 공포, 보유자산에 보안등급을 관리하는지 여부를 확인하는 보안관리 부문, 임직원 대상으로 정기적 직원 보안교육 실시와 보안서약서 징구 여부를 확인하는 인력관리 부문, 통제구역 설정여부와 중요자료 보관 대책 수립여부를 확인 등 보안사고/재해 관리로 세분화 되어 조사가 이루어졌다. 2013년 기술보호 역량 및 수준 모형은 23개 항목으로 구성하고 100점 만점으로 보안정책 수립 20점,

보안관리 45점, 인력관리 30점, 보안사고/재해관리 5점 총 100점으로 구성하였다. 각 영역별 점수를 합한 결과를 바탕으로 기업의 기술보호 수준을 우수, 양호, 보통, 취약, 위험 등 5단계 수준으로 구분하였다.

3.2 변수 구성

최근 3년간의 기술유출 경험유무를 종속변수로 하였으며, 보안정책수립, 보안관리, 인력관리, 보안사고/재해관리를 독립변수로 사용하였다.

보안정책수립 변수에서는 보안규정 보유여부(Q1), 기술유출 시 대응절차(Q2), 보안정책 위반 직원 징계 절차(Q3), 보유자산에 대한 관리(Q5), 보안관리자 지정 운영(Q6)이 포함되며 보안관리 변수에는 유무인 경비시스템 운영(Q7), 외부인 접견실 운영(Q8), 출입자 통제 시스템 운영(Q9), 중요 자산관리시스템 운영(Q10), 통제구역 운영(Q11), 보안감사 실시여부(Q12), 정보화기기 반입 및 반출통제(Q13), 외부침입방지를 위한 내부 네트워크 관리(Q14), 정보시스템 로그관리(Q15), 디지털 자산관리 시스템 운영(Q16), 보안업데이트(Q17) 여부가 포함되었다. 인력관리 변수에는 임직원 보안교육(Q18), 임직원 부재시 보안활동 수행(Q19), 보안서약서 징구(Q20), 퇴사자의 동향파악(Q21)을 사용하였고 보안사

〈Table 2〉 Variable

dependent variable		3 years experience in technology leakage	
Independent variable	Security Policy	Q1	security regulations
		Q2	response procedures in case of technology leakage
		Q3	disciplinary procedures for violators of the security policy
		Q5	assets management
		Q6	Designation and Management of the security manager
	Security Management	Q7	Operating Manned & unmanned security system
		Q8	Operating the reception room for visitors
		Q9	Operating the control system for visitors
		Q10	importance assets management system
		Q11	Operating the restricted area
		Q12	implementation of the security audit
		Q13	control of exportation and importation for ICT equipment
		Q14	internal network administration for External intrusion prevention
		Q15	information system log management
		Q16	Operating the digital assets management system
		Q17	security update
	manpower management	Q18	security education for employees
		Q19	security activities in the absence of the employees
		Q20	security pledge
		Q21	prehension the trends of retirements
	Security incident control	Q22	establishment the crisis management system
		Q23	iprotection provisions for important data

고/재해관리 변수에는 주요시설의 위기관리시스템 수립 시행 여부(Q22), 중요자료의 보호대책(Q23)이 포함되었다. 총 22문항을 변수로 사용하였다.

설문문항 중 다양한 답변이 가능한 문항 4의 보안투자부분은 변수에서 제외하였다. 변수설명은 <Table 2>와 같다.

3.3 연구 방법 및 모형

본 연구에서는 기술보호 역량 및 수준의 4개 영역의 23문항 중 다양한 답변이 가능한 보안설비 투자부분(Q3)을 제외한 22문항과 기술유출 경험에 대해서 기술분석 및 단변량 분석을 시행하였고 기술유출과 관련이 있는 요인을 분석하기 위하여 로지스틱 회귀분석을 실시하였다.

단변량 분석을 통해 P-value가 0.05 이하인 모든 문항을 stepwise 로지스틱 회귀분석을 실시하였으며, 모형 선택의 기준으로 AIC(Akaike Information Criterion), BIC(Bayes Information Criterion), 우도비(likelihood), c-통계량 등을 적용하였다.

4. 연구 결과

4.1 단변량 분석

문항 1에서 문항 23까지 각각의 문항에 대하여 기술유출 유무와 관계가 있는지에 대해 단변량 분석을 시행하여 기술유출과 각 변수간에 통계적 연관성을 확인한 결과, 문항 21의 퇴사자 동향 파악을 제외한 모든 문항의 P-value가 0.05 미만으로 기술유출과 유의한 관계가 있음을 확인 할 수 있었다. 기술보호 정책 및 관리가 이루어지고 있을 때, 기술보호가 효과적으로 작용하는 것으로 분석되었다.

4.2 로지스틱 회귀분석

기술유출 경험이 있는 155개 중소기업과 기술

〈Table 3〉 Univariate Analysis of Technology Leakage

No	chi-squared	P-value	No	chi-squared	P-value
Q1	23.459933	0.0000080	Q13	19.982931	0.0000458
Q2	29.897691	0.0000003	Q14	29.613485	0.0000004
Q3	34.003800	0.0000000	Q15	32.189135	0.0000055
Q5	39.031371	0.0000000	Q16	33.746655	0.0000008
Q6	21.905341	0.0000683	Q17	26.537956	0.0000003
Q7	14.194081	0.0026525	Q18	21.599752	0.0000790
Q8	16.193667	0.0000572	Q19	45.773467	0.0000000
Q9	42.734334	0.0000000	Q20	21.574607	0.0014456
Q10	7.943532	0.0048260	Q21	0.789965	0.6736918
Q11	38.352503	0.0000000	Q22	12.773453	0.0003516
Q12	42.442083	0.0000000	Q23	29.242808	0.0000020

$P < 0.05$.

유출 미경험 중소기업 1,363개에 대해 구분하여 기술유출 요인에 대해 분석하였다. 단변량 분석을 통해 P-value 0.05 이상인 문항 21의 퇴사자 동향 파악을 제외한 모든 문항을 AIC (Akaike Information Criterion)를 이용하여 로지스틱 회귀분석 한 결과 기술유출 대응절차(Q2), 접견실 운영(Q8), 출입자 통제시스템 운영(Q9), 중요자산 관리시스템 운영(Q10), 정기적인 보안감사(Q12), 내부 네트워크 관리(Q14), 보안 업데이트(Q17), 직원 보안교육(Q18), 임직원 부재 시 보안활동(Q19), 중요자료의 보호대책(Q23)이 요인으로 분석되었으며, 이 선택된 10개의 항목 중 P-value가 0.05보다 작은 항목인 출입자 통제시스템 운영(Q9), 정기적인 보안감사(Q12), 임직원 부재 시 보안활동(Q19), 중요자료의 보안대책 마련(Q23) 등 4가지 요인이 기술 보호 핵심요인으로 분석 되었다. 4가지 요인 중 보안감사(Q12)는 회귀계수의 추정치가 0.46683으로 변수 값이 1이 증가하면 유출이 일어날 확률에 대한 로짓인 log(p/(1-p)) 값이 0.46683만큼 증가하는 결과를 보였다. 그러므로 보안감사(Q12)를 실시하지 않을수록 기술유출이 일어날 확률이 더 높아지는 것으로 나타나 기술유출 위험도를 낮추기 위하여 정기적 보안감사 실시에 필요함을 시사하고 있다. 김혜정과 안중호의 연구에서도 자신이 속한 기업이 보호 규정에 대한 관심이 높다고 생각할수록 보안위반 수준은 낮아진다고 기술하였다[4]. 출입자 통제시스템(Q9) 및 임직원 부재 시 보안활동(Q19)은 출입자 통제 시스템 및 보안 활동이 적을수록 기술유출이 일어날 가능성이 더 커지는 것으로 확인 되었으며, 중요자료의 보호대책(Q23)은 정기적으로 백업관리를 할수록 기술유출 위험이 적어지는 것으로 분석되었다.

〈Table 4〉 Logistic Regression Analysis

	Estimate	Std.Error	z value	Pr(>|z|)
(Intercept)	-1.9492	0.72013	-2.707	6.80E-03
Q2	0.31295	0.16293	1.921	5.48E-02
Q8	0.29043	0.18838	1.542	1.23E-01
Q9	-0.23996	0.11261	-2.131	0.033106
Q10	-0.34285	0.23033	-1.488	0.136623
Q12	0.46683	0.1915	2.438	0.014777
Q14	-0.29207	0.16553	-1.764	0.077664
Q17	0.33615	0.2068	1.625	0.104057
Q18	-0.23242	0.12581	-1.847	0.064692
Q19	-0.15447	0.07035	-2.196	0.028101
Q23	0.20416	0.089	2.294	0.021791

$P < 0.05$.

5. 결 론

본 연구에서는 중소기업 기술보호 핵심요인을 분석하기 위하여 중소기업 기술보호 역량 수준 상의 설문조사 문항을 바탕으로 기술유출 중소기업 155개 중소기업과 기술유출 미경험 중소기업 1,363개 총 1,518개 중소기업에 대해 기술보호 요인을 로지스틱 회귀분석을 통해 분석하였다. 출입자 통제시스템 운영, 정기적인 보안감사, 임직원 부재 시 보안활동, 중요자료의 보호대책 4가지 요인이 기술보호 요인으로 분석되었다. 출입자 통제 및 중요자료 보호 시스템 구축비용의 정부지원 강화, 보안감사 및 임직원 부재 시 보안활동 관련 체크리스트와 보안관리 매뉴얼을 제작하여 배포하는 등의 지원들이 정부차원에서 집중적으로 이루어진다면 기술보호 효과를 극대화 할 수 있을 것이다. 중소기업에서도 이 4가지 요인에 대해

집중적으로 투자하고 관리한다면 효율적인 기술보호 체계를 구축하고 운영할 수 있을 것으로 기대된다.

이제까지 중소기업의 기술보호 연구들은 단순 정량적으로 기술보호 요인을 도출하는 연구가 대부분이었으나, 본 연구는 기술유출 경험유무에 따라 실증적으로 핵심요인을 도출하였으며 또한 실무자 및 연구자들에게 중소기업 기술보호 방향성을 제시 하였다는데 의의가 있다. 이러한 연구결과에도 불구하고 본 연구에서는 다음과 같은 한계를 가지고 있다. 본 연구의 조사 자료는 대상자의 기억에 의존한 응답이므로 회상 편향(recall basis)의 문제가 있을 수 있다. 또한 분석 측면에서의 한계로 중소기업 산업군, 보유 기술, 지역, 매출액 등 다양한 분류 방법 및 통계방법을 통해 분석이 이루어진다면 보다 더 향상된 기술보호 대책들이 도출될 수 있을 것으로 기대된다.

References

[1] 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.

[2] Hong, S. C., “Recent SMEs main phase indicator changes cause and implications,” Focus for Korea Small Business Institute, 2014. 8. 13.

[3] Jung, C. H., Lee, J. T. and Chung, D. K., “A Study on the Security Management System Model for the Information Security of the Aviation infrastructure,” The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 87-96, 2011.

[4] Kim, H. J. and Ahn, J. H., “An Empirical Study of Employee’s Deviant Behavi or for Improving Efficiency of Information Security Governance,” Society for e-Business Studies, Vol. 18, No. 1, pp. 147-164, 2013.

[5] Kim, J. D., Chang, H. B., and Ryoo, S. Y., “A Study of Information Security Management System for Small and Medium Enterprises,” Journal of The Korean Association of Small Business Studies, Vol. 28, No. 2, pp. 267-294, 2006.

[6] Kim, J. K. and Jeon, J. H., “Comparison of Users’ Perception of Information Security Elements on Computer Virus Between Large and Small-and-Medium Companies,” International Journal of Reliable Information and Assurance, Vol. 16, No. 2, pp. 79-92, 2006.

[7] Kim, M. J., Sung, J. H., and Kwon, K. H., “Analysis of The Relation Between The Material Weakness of Internal Accounting Control System and Firm’s Characteristics Variables, Validation Comparison of Testing Models,” Korean international accounting review, Vol. 29, pp. 1-23, 2010.

[8] Korean National Police Agency, “The White Paper for Korean National Police Agency 2011,” 2011.

[9] Korean National Police Agency, “The White Paper for Korean National Police Agency 2013,” 2013.

[10] Lee, C. S. and Kim, Y. H., “An Analysis of Relationship between Industry Security Education and Capability: Case Centric on Insider Leakage,” The Journal of Society for e-Business Studies, Vol. 20, No. 2, pp. 27-36, 2015.

[11] Lee, J. W., “Developing Information Security Management Model for SMEs: An Empirical Study,” Asia Pacific Journal of Information Systems, Vol. 15, No. 1, pp. 115-133, 2005.

[12] Moon, H. J., “Training Status and Problems for Information Security empowerment of Small-and-Medium Companies in Korea,” International Journal of Reliable Information and Assurance, Vol. 19, No. 1, pp. 29-39, 2009.

[13] Mun, B. K., “The competitiveness in world export markets the number one item,” Trade Focus for Institute for International Trade, Vol. 14, No. 2, 2015.

[14] Nam, J. S., “Actual Condition of Damage of Industrial Secrets Leakage Crime and its Measures at Small or Medium Sized Business Focusing on Legal · Systematic Methods,” Korean Association of Public Safety and Criminal Justice, Vol. 46, No. 1, pp. 44-75, 2012.

[15] National Industrial Security Center, “Technology Leakage Statistics,” 2014.

[16] No, M. S., “Factors Assessment of industrial security capabilities of Small-and-Medium Companies,” Korean Public Administration Review, Vol. 44, No. 3, pp. 239-259, 2010.

[17] OECD, “2013 OECD Science, Technolog and Industry Scoreboard 2013,” 2013. 10. 23.

[18] Park, C. S., “Information Security Measures Guidelines Trends of Small-and-Medium Companies in Japan,” International Journal of Reliable Information and Assurance, Vol. 20, No. 1, pp. 19-30, 2010.

[19] Park, J. K., “Problems and Legal Solutions related to the Technology Protection Support System for Small and Medium Enterprise(SME) in Korea,” Institute for Law of Science and Technology, Vol. 20, pp. 185-224, 2014.

[20] Small and Medium Business Administration, “2013 Technology Protection Capabilitiy & Sueftyrvey on the level of Small & Medium Business,” 2014.

저 자 소 개

홍준석	(E-mail: jun0817@kaits.or.kr)
2012년	성균관대학교 정보통신대학원 정보보호전공 (공학석사)
2013년~현재	서울과학기술대학교 IT정책대학원 산업정보시스템 (박사과정)
현재	한국산업보안기술협회 중소기업기술지킴센터 관제운영팀장
관심분야	보안관제정책, 침해사고대응, 중소기업 보안

박원형	(E-mail: whpark@kdu.ac.kr)
2002년	서울과학기술대학교 산업정보시스템공학과 (공학사)
2005년	서울과학기술대학교 정보산업공학과 (공학석사)
2009년	경기대학교 정보보호학과 (이학박사)
2011년	서울과학기술대학교 산업정보시스템공학과 겸임교수
현재	극동대학교 사이버안보학과 조교수/학과장
관심분야	보안관제기술, 윈도우포렌식, 산업보안

김양훈	(E-mail: yhkim@kdu.ac.kr)
2005년	대진대학교 컴퓨터공학과 (공학사)
2007년	대진대학교 컴퓨터공학과 (공학석사)
2011년	대진대학교 컴퓨터공학과 소프트웨어전공 (공학박사)
현재	극동대학교 사이버안보학과 조교수
관심분야	보안관리, 보안거버넌스, 보안문화

국광호	(E-mail: khkook@seoultech.ac.kr)
1979년	서울대학교 산업공학 (학사)
1981년	서울대학교 대학원 산업공학 (석사)
1989년	미조지아 공과대학교 대학원 산업공학 (박사)
1989년~1993년	한국전자통신연구원 선임연구원
1993년~현재	서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 교수
관심분야	정보보호, 정보통신, 산업보안