ISSN 2288-4866 (Print)
ISSN 2288-4882 (Online)
http://www.jiisonline.org
J Intell Inform Syst 2017 March: 23(1): 143~159 http://dx.doi.org/10.13088/jiis.2017.23.1.143

중소기업 기술 유출에 대한 조기경보시스템 개발에 대한 연구

서봉군
국민대학교 BIT 전문대학원
(*bgseo@kookmin.ac.kr*)

박도형
국민대학교 경영대학 경영정보학부
(*dohyungpark@kookmin.ac.kr*)

급속한 IT의 발전으로 인해 개인정보뿐만 아니라 기업이 보유하고 있는 핵심 기술 및 정보에 대한 유출 위협이 중요한 이슈로 인식되고 있다. 기업에게 있어서 보유하고 있는 핵심 기술은 기업의 생존 및 지속적으로 경쟁우위를 차지하기 위해 매우 중요한 부분이다. 최근 기술 침해 사례가 많이 일어나고 있는데, 기술 유출은 기업에게 있어서 주가하락 등의 막대한 재무적인 손실을 가져올 뿐만 아니라, 기업의 신뢰에 손상을 입게 되고, 기업의 발전을 지연시키게 되는 악영향을 미치게 된다. 특히, 대기업에 비해 핵심기술이 기업 내 중요한 많은 부분을 차지하는 중소기업에 있어서 기술 유출에 대한 대비는 기업의 존립에 있어서 필수적인 요소로 볼 수 있다. 이처럼 정보 보안 관리의 필요성과 중요성이 대두되면서 기업 입장에서 조기에 기술 침해 위협에 대해 확인하고 대비할 필요가 있다. 본 연구에서는 기술 유출에 영향을 미치는 요인들을 탐색하는 실증 분석을 수행하고, 인공지능 알고리즘을 통해 기술유출 조기경보시스템을 개발하고자 한다. 구체적으로 본 연구에서는 중소기업이 보유한 기술 유출에 영향을 미치는 요인들을 로지스틱 회귀분석을 통해 확인해보고, 통계분석을 통해 검증된 요인들을 기반으로 인공지능 여러 기법들 중 하나인 Support Vector Machine을 활용하여 기술침해 가능성을 조기에 알려주는 모형을 개발하였다. 본 연구에서 제안하는 기술 유출 가능성에 대한 조기 경보 모형을 통해 기업 및 정부 관점에서 기술 유출을 미리 예방할 수 있는 기회를 제공할 수 있을 것으로 기대된다.

주제어 : 기술 유출, 중소기업, 조기경보시스템, 서포트 벡터 머신

논문접수일 : 2017년 3월 13일 논문수정일 : 2017년 3월 20일 게재확정일 : 2017년 3월 20일
원고유형 : 일반논문 교신저자 : 박도형

1. 서론

최근 ICT(Information and Communication Technologies)의 급속한 발전으로 개인정보 유출, 전자금융사기 등의 개인정보침해뿐만 아니라 기업이 보유하고 있는 기술이나 기술에 대한 핵심 정보에 대한 유출이 현 사회의 중요한 이슈로 인식되고 있는 상황이다. 기업이 독자적으로 보유하고 있는 핵심 기술은 기업 자체의 생존 및 지속적인 경쟁우위 창출을 위해 매우 중요하다. 하지만 여전히 기술 침해 관련 사고들이 많이 발생하고 있으며, 기술 유출의 피해를 입은 기업은 주가 하락, 신뢰 손상 등의 손실을 가져오고 있다. 결과적으로 이러한 기업은 막대한 재무적인 손실을 가져올 뿐만 아니라 기업의 발전을 현저하게 지연시키게 되는 악영향을 미치게 된다.

특히, 대기업에 비해 핵심기술의 기업 내 비중이 많은 부분을 차지하는 중소기업에 있어서 기술 유출에 대한 대비는 기업의 존립에 있어서 필수적인 요소로 볼 수 있다. 중소기업연구원

(Kosbi, 2014)에 따르면, 중소기업의 경우 대기업에 비해 기술유출 비중이 높으며, 기술 유출로 인한 피해금액 또한 갈수록 증가하고 있어 심각한 피해를 입고 있다. 중소기업의 경우 해외로의 기술 유출이 73%에 달하며, 기술 유출로 인한 피해 경험이 있는 기업의 1건당 피해 금액이 평균 16.9억 원에 이르고 있다. 이처럼 정보보안관리(Information Security Management: ISM)의 필요성과 중요성이 대두되고, 국내에서도 보안에 대해 법적인 고찰, 제도 및 정책 제시, 내부자 위험분석 관리, 기업정보보호 관리체계 등과 같은 연구가 활발히 진행되고 있는 상황이다(Kim & Kim, 2007; Chang & Song, 2009; Choi et al., 2012). 이 외에도 중소기업의 산업보안 역량에 대한 요인에 대한 평가, 중소기업의 기술보호 요인 분석과 같은 기업의 어떠한 요인들이 기업의 기술유출에 영향을 미치는 지에 대한 연구도 수행되었다(Noh & Lee, 2010; Hong et al., 2015). 이러한 연구들은 주로 보안정책수립, 보안관리, 조직적인 측면에서의 요인들을 변수로 선정하여 분석을 수행하였지만, 아직까진 중소기업의 R&D와 관련된 기술자체 특성에 대한 요인과 기술 개발 조직 특성에 대한 요인을 선정하여 함께 분석한 연구는 수행되고 있지 않은 상황이다.

본 연구에서는 기술 유출에 대한 영향요인을 기술의 가치와 관련된 요소와 기술 통제와 관련된 요소로 나누어 분석 틀을 설계하였다. 실증분석을 수행하기 위해서 중소기업청에서 수행한 통계 조사 데이터를 활용하였으며, 로지스틱 회귀분석을 통해 어떠한 요인들이 기업의 기술유출에 영향을 미치는 확인해 보았다. 마지막으로 통계분석을 통해 검증된 요인들을 기반으로 인공지능 기법들 중 하나인 SVM(Support Vector Machine)을 활용하여 기술침해 가능성을 조기에 알려주는 모형을 제안하고자 한다.

2. 이론적 배경

2.1 중소기업의 기술 유출

중소기업의 기술 유출은 인적 자원의 이동이나 체화기술의 이전, 기술 거래 간 유출 등 다양한 기술 유출 유형을 가지고 있으며, 중소기업연구원, 중소기업청, 한국인터넷진흥원 등의 다양한 기관에서는 중소기업의 기술 유출을 감소시키기 위해서 보안 역량평가 및 기술 보호 수준 등의 조사를 실시하고 있다. 이와 같은 배경 하에서 기술 유출은 정보화 사회에서 매우 중요한 이슈로 시사되고 있으며, 실제로 그 중요성이 인식되는 만큼 다양한 연구가 활발하게 진행되고 있다.

많은 선행 연구들은 정책대안의 제시가 약 90%로 대다수를 차지하고 있으며, 연구 방법은 문헌 분석이 76%를 차지하고, 실증 및 통계분석은 16%로 상대적으로 매우 낮은 비율을 차지하고 있다. 즉 중소기업의 기술 유출에 대한 실제 보안인식 및 관리 실태에 대한 연구를 통해 현행 제도의 한계와 개선점을 도출하고 차후 정책 수립기반을 제시하거나, 제도적 차원에서 산업기술 유출방지를 위해 관리 모델을 제시하고 중소기업의 특성에 맞는 유출 방지 보안의 필요성을 국외 사례를 통해 제시한다는 것이다(Chae & Ko, 2012). 일부는 단순히 제안과 필요성 등에 머무르지 않고 실증 분석을 통하여 의미 있는 결과를 제시하기도 한다. 가령 기업 재무적 차원에서의 기업 기술 유출에 대하여, Lee & Kim(2015)는 기업의 매출액과 보안투자액 간에 정(+)의 상

관관계를 규명하고, 기술 유출 방지를 위한 보안 교육과 실제 기업 보안역량 간에도 정(+)의 상관관계가 있음을 보이면서, 실제 보안 투자가 기업의 보안 역량과 연관되어 있으며 나아가 기업 매출액에도 영향을 미칠 수 있음을 시사하고 있다.

실증 및 통계분석을 통하여 기술 유출을 예측하기 위한 선행연구도 수행되고 있는데, Choi & Lee(2013)와 Hong et al.(2015)의 연구에서는 기술 유출을 관리적 보안 요인들을 통해 예측모형을 구축하기도 하였으나, 조사 자료의 회상 편향 문제, 중소기업의 산업 군이나 보유기술, 구조적 요인 등을 반영하지 못하거나, 분석 간 비교 대조 표본 수 차이 등의 한계점이 있음을 볼 수 있다.

2.2 기술 유출에 대한 영향요인 관련 선행연구

기업의 기술 유출에 영향을 미치는 요인들에 관련한 많은 선행 연구들이 수행되었다(Chang & Song, 2009 Noh & Lee, 2010 Hong et al., 2015). 이를 기반으로 본 연구에서는 기술 유출에 있어서 크게 기술의 가치(Value)와 관련된 요소와 기술 통제(Control)와 관련된 두 요소로 구분하였고, 이를 기반으로 분석을 위한 구조를 설계하였다. 첫 번째 요소인 기술의 가치(Value)가 증가하면, 기술 자체의 매력도가 높아져 기술 유출 가능성(p)이 증가할 수 있으며, 이는 기술의 자체적인 특성과 관련되어 있다고 전제하였다. 두 번째 요소인 기술의 통제(Control)가 증가하면, 기업 내부에의 규정 혹은 관리적인 보안이 강화되는 측면에서 기술 유출에 가능성(Possibility)이 낮아질 수 있고, 이는 인적, 기업의 내부적인 속성과 관련되어 있다고 전제하였다. 이를 나타내면 다음과 같다.

$$Possibility\ of\ Technology\ Leakage = f(Value, Control)$$

2.2.1 Value 관점의 기술 자체 특성

대부분의 기술 유출의 촉발 원인은 유출 기술이 보유하는 가치가 기술을 보유하고 있는 기업이 아닌, 기술을 보유하지 못한 타 기업의 경제적인 욕구를 만족시킬 수 있기 때문이다. 즉, 기술을 보유하지 못한 혹은 더 나은 기술을 보유하기 원하는 기업들은 자체적으로 경쟁력 있는 기술을 개발하기 위해서 상당부분의 긴 시간과 많은 비용이 발생하기 때문에, 타 기업의 기술 절취를 통해 선진 기업에 대해 빠른 추격을 시도한다. 기업이 보유한 기술이 시장성, 기술성, 사업성이 높을 경우에 기술의 가치가 커지기 때문에 잠재적인 유출행위자가 기술을 유출하려는 원천적인 요인이 될 수 있다(Chae & Ko, 2012).

가치가 높은 기술을 보유한 기업은 세계적으로 인정받을 수 있는 특허나 원천기술 혹은 차세대 기술 능력을 보유한 고난이도의 기술을 보유하고 있는 것을 의미한다. 이 외에도 OEM 생산능력, 자본 집약적인 기술을 가진 기업을 중간기술을 보유한 기업으로 볼 수 있으며, 단일공정의 생산기술, 자체적으로 제품 개선이나 설계능력이 부족한 기업들을 범용기술을 가진 기업으로 분류할 수 있다. 이처럼 기술의 난이도와 기술의 신규성이 기술의 가치를 결정지을 수 있으며, 보유하고 있는 기술이 고기술 혹은 신기술일 경우 기업의 보안이 더욱 중요시해 진다(Mohr, 1996).

또한 핵심 기술을 보유하지 않은 기업에서는 타 기업의 기술을 모방하는 '기술 모방 전략'을 추진하기도 하는데, 이는 기술 이전이나 구매하는 행위보다 상대적으로 경제적 지출이 적으며, 빠른 기술 획득을 할 수 있다는 점에서 기술 유

출을 하려는 의도가 커진다(Jung, 2009; Lee & Choe, 2002). 일반적으로 기업에서 보유하고 있는 제품기술을 외부 경쟁업체에서 모방 개발하는데 소요되는 기간으로 기술 자체의 난이도나 신규성에 따라 짧게는 3개월 이내 길게는 2년 이상 걸린다. 즉, 기술의 난이도나 신규성이 낮으면 기술을 모방하는데 걸리는 시간이 짧을 것이다. 반대로 기술의 난이도나 신규성이 높으면 기술을 모방하는데 걸리는 시간이 더 길어질 것이다. 결과적으로 기술의 가치가 크면 모방개발 기간이 길어질 것이고 이는 기술의 유출 가능성이 높아질 수 있을 것이라고 예측해 볼 수 있다. 마찬가지로 기업이 보유하고 있는 기술의 수명주기(Life Cycle)는 사업 성과와 상관관계가 존재하고, 수명주기가 길수록 사업성은 높아진다(Kim, 2007). 즉 수명주기가 긴 기술은 기술력이 크며, 가치가 높다고 판단할 수 있으며, 이는 기술의 가치가 증가하는 것이기 때문에 기술이 유출 될 가능성이 높아질 수 있을 것이다. 한편, 대기업과 중소기업 간 거래에서는 중소기업이 지배되거나 종속되는 수직적 불평등 관계가 형성된다. 이러한 관계 하에서 거래 관계상 우위를 점하는 대기업에 의해 중소기업의 기술 유출이 발생하는 경우가 있다. 중소기업 입장에서는 대기업의 요구를 거절하기 쉽지 않을 뿐만 아니라 오히려 분쟁이 소송으로 이어질 경우에 중소기업에게는 큰 부담으로 작용될 수 있다. 더 나아가 거래 단절 등의 보복 우려 혹은 대기업의 금전적 대가성 스카우트를 통해서 중소기업의 핵심 기술 유출을 시도하려는 사례도 존재한다(Jung, 2009; Jung, 2015). 즉, 중소기업이 보유하고 있는 기술의 가치가 커질수록 대기업에서 기술에 대한 정보를 요구할 가능성이 커질 것이며, 결과적으로 보유하고 있는 기술에 대한 유출 가능성이 증가할 것임을 예측해 볼 수 있다.

위와 같은 선행연구를 통해 본 연구에서는 Value 관점의 기술 자체 특성 요인으로서 기술의 난이도, 기술의 신규성, 기술의 수명주기, 기술의 모방기간, 대기업에서의 기술 이전 제안 유무에 대한 변수들을 분석 대상으로 선정하였다.

2.2.2 Control 관점의 기술 개발 조직 특성

기술 개발 조직 특성은 기업의 보유 역량, 조직의 규모나 구조, 조직 내의 제도 등의 기업 내부적인 속성에 관련되며, 이는 기술 자체의 가치(Value)의 정도나 기술의 특성보다는 기술을 어떻게 통제(Control)하고 관리하는 측면으로 볼 수 있다. 조직 특성의 대표적인 요인 중 하나로 기업의 규모를 들 수 있으며, 일반적으로 기업의 규모는 총 종사자 수로 유추할 수 있다. 이에 Noh & Lee(2010)의 연구에서는 산업 보안 역량 제고에 영향을 미치는 요인 중 하나로 기업 규모를 변수로 선정하여, 기업 규모가 산업보안 역량 수준과 정(+)의 상관관계를 가지고 있음을 보여주고 있다. 기업의 규모가 클수록 기술 유출에 대한 보안 대책과 같은 관리적인 측면이 강조될 가능성이 높을 것이며, 이에 대한 투자비용도 많을 것이다. 실제로 대기업에 비해 중소기업에서 기술 유출의 빈도가 높게 나타나고 있으며, 피해액도 상대적으로 큰 것으로 나타났다. 또한 중소기업 중에서도 종업원 50인 이상인 중기업에 비해 50인 미만인 소기업에서 기술 유출을 당한 비중이 높게 나타나고 있다.

성과보상제와 같은 조직 내부의 제도가 기술 유출을 통제할 수 있는 요인일 수 있는데, Hwang & Lee(2016)의 연구에서는 기술유출을 조직애착도와 같은 기술 유출범죄 동기와 관련

하여 접근하면서, 조직에 대한 애착도가 낮을수록 기술유출의 가능성이 높아지는 것으로 나타났다. 조직 애착도는 자신이 속한 조직에 대한 자신의 정체성의 정도와 조직에 머무르려는 의지를 의미하는데, Kim & Kim(2011)의 연구에서는 성과보상제의 도입으로 인해 특히 직원들의 생산성 향상에 정(+)의 관계가 있음을 보여주었으며, 이 외에도 직원의 직무 수행 노력, 인사관리의 효과성, 1인당 부가가치 등의 요인들이 성과보상제와 정(+)의 영향력을 미치고 있음을 규명하고 있는 실증분석 연구들이 수행되어왔다(Jang, 2002; Yu & Park, 2007). 반대로, 성과보상제로 인해 금전적 보상 격차에 대한 자존감과 내정동기의 약화, 부서 간 협력 저해 및 조직 분위기 경직, 성과에 대한 측정의 불신, 스트레스증가, 불안감 증대 등 오히려 부정적인 영향력을 미친다는 선행연구도 찾아볼 수 있다(Deci & Ryan, 1980; Heneman, 1992; Yang, 2004). 이와 같은 연구들을 통해서 기업이 보유하고 있는 기술의 중요도가 대기업에 비해 상대적으로 높은 중소기업의 특성 상 조직 내 제도 중 성과보상제의 유무는 직원의 조직 애착도와 유의한 관계를 가질 것이며, 나아가 기업의 기술유출 가능성에도 영향을 줄 수 있을 것으로 판단되다.

한편, 자원이 부족하고, 자체 개발 능력이 낮은 단점을 가지고 있는 중소기업에게는 공동개발, 외부 협력 등과 같은 개방형 혁신(Open Innovation)은 기업의 기술개발에 있어 효율성을 높일 수 있으며, 자금력 및 인력에 대한 부분을 보완할 수 있는 장점이 있다. 하지만 기술에 대한 정보를 공유해야 하기 때문에 핵심 자료들이 외부로 유출 될 가능성이 있으며, 실제 기술개발 과정에서 기업의 핵심 기술을 유출하고 자체 생산에 들어가는 사례들도 존재한다(Hong, 2005; Jung, 2015). 따라서 기술개발을 추진 방식에 따라서 기술 유출에 영향을 미칠 수 있기 때문에, 중소기업에서는 자체적(독자적)으로 개발을 수행할 지, 외부와 공동(위탁) 개발을 통해 기술 개발을 할지에 대해 장단점을 고려하여 기술개발을 추진할 필요가 있다.

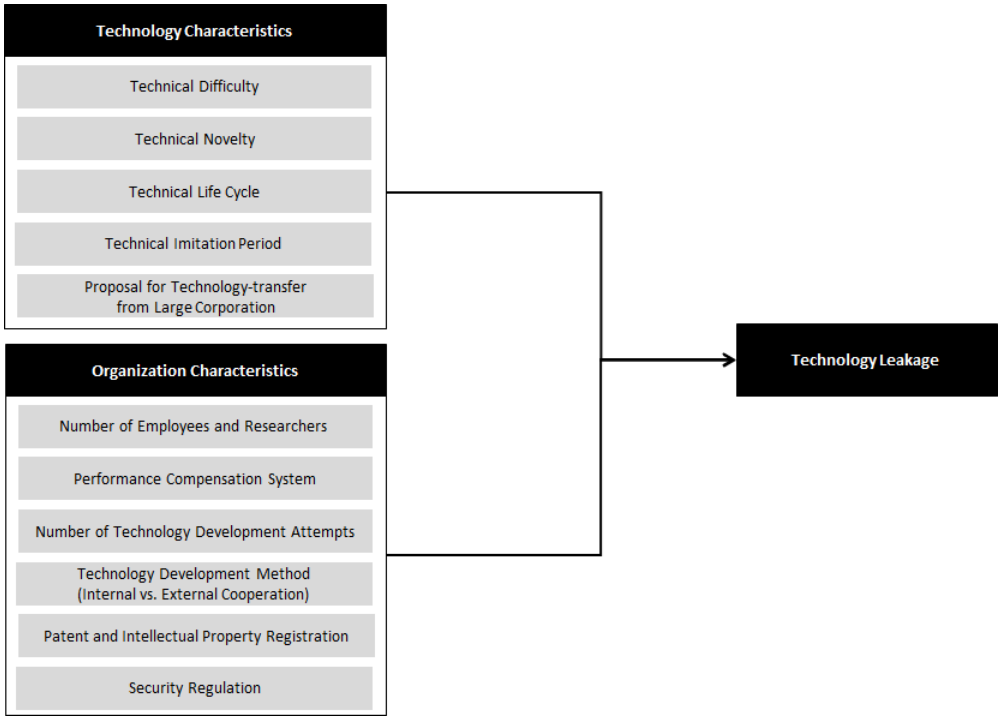
또한 기업이 기술을 개발하기 위한 시도 건수도 기술 유출에 영향을 미치는 요인일 수 있다. 중소기업의 한정된 자원 하에서 중소기업 자체에서 시도하는 기술 개발 건수가 계속해서 증가하다 보면, 오히려 핵심기술 관리에 있어서 리소스(집중도)가 분배된다. 이는 기업에서 기술에 대해 집중할 수 있는 역량을 떨어뜨리며, 기술을 통제력이 낮아지게 되어 기술 유출 가능성이 커질 수 있을 것이다.

기술 유출을 예방하고, 보안을 강화하기 위해 기업은 보유한 기술에 대해 특허 제도를 활용하고 있다. 특히 대기업에 비해 중소기업 기술의 특허출원 및 지식재산권 등록은 큰 의미를 갖으며, 기술력이 있는 중소기업이 일반 중소기업보다 기술 유출에 대한 보호 활동이 높게 나타난다. Noh & Lee(2010)의 연구에서 기술 유출을 통제할 수 있는 수단인 특허출원 실적이 산업보안 역량수준과 정(+)의 관계가 나타나고 있음을 보여주었다. 반대로 Jung(2009)의 연구에서는 기업이 보유한 기술을 특허 및 지식재산권으로 등록하는 것은 기술의 공개를 전제로 하는 행위이며, 공개에 따른 기술 유출에 대해 감안해야 한다고 주장한다. 따라서 핵심 주력 기술을 보유한 중소기업에서는 기술을 등록할 것인지, 영업비밀로 유지할 것인지, 저작권으로 보호할 것인지에 대한 전략적 방안을 고려할 필요가 있다.

기업의 기술유출 사고는 직원의 무지와 부주의한 행동에 의해 일어날 수도 있으며, 핵심 직

원의 의도적인 기술유출 행위로 인해 직·간접적으로 행해질 수 있다. 보안규정 및 정책 수립은 이러한 유출 행위자들을 직접적으로 통제를 할 수 있는 수단이기도 하며, 구성원들의 보안 의식 제고와 기업 전반적인 보안 환경에 영향을 주는 요인으로 볼 수 있다(Chae & Ko, 2012). 특히 중소기업은 대기업에 비해 보안 관리나 감독체계가 허술하기 때문에 유출 가능성이 크며, 기술유출이 발생하여도 대처를 하지 못하는 경우도 많다. Jung(2009)의 기술 유출 방지에 대한 연구에서는 기술유출 원인을 보안 규정, 보안 시스템, 보안 전담 조직 등의 보안 관리 체계가 미비하기 때문이며, 특히 중소기업이 대기업에 비해 기술유출의 약점을 보유하고 있다고 주장하였다. 대기업에 비해 기업 내 기술 비중이 높은 중소기업은 보유하고 있는 핵심기술이 유출되면 기업의 존립에 큰 영향을 미칠 수 있다. 때문에 중소기업의 경우 기술 유출 사전 예방을 위한 보안 규정이나 정책 수립이 매우 중요하다고 볼 수 있다. 이를 통해 기업의 직원들이 보안 정책에 대한 관심이 높아지고, 보안 규정에 관한 교육 제도가 갖춰지면 직원이 보안 의식을 향상시킬 수 있고, 결과적으로 기술 유출을 예방에 영향을 미칠 수 있고, 보안 위반 정도가 낮아 질 수 있을 것이다(Kim & Ahn, 2013).

위와 같은 선행연구를 통해 본 연구에서는 Control 관점의 기술 개발 조직 특성 요인이 기업의 기술 유출에 의한 피해 유무에 영향을 미칠 변수로 종사자 및 연구원 비율, 성과보상제 시행 유무, 기술개발시도 건수, 기술 개발 방식(자체



〈Figure 1〉 Research Model

개발/외부 협력 개발), 기술에 대한 특허 및 지식재산권 등록 현황, 보안규정 유무 변수를 선정하였다(<Figure 1> 참조).

3. 연구 설계

3.1 자료 수집 및 표본의 특징

본 연구에서 사용된 분석 자료는 중소기업청과 중소기업중앙회에서 공동으로 수행한 2011년, 2013년, 2014년도 '중소기업기술통계조사'이다. 상기 조사는 중소기업의 R&D 실태를 파악하고, 중소기업에 대한 기술개발 활동, 기술개발 조직, 기술보호 등과 같은 중소기업 지원에 대한 기획 및 추진을 위한 자료이며, 중소기업기술혁신촉진법 제 8조(중소기업 기술통계의 작성)에 근거하여 실시되고 있다. 조사 대상은 한국표준산업분류 (KSIC)상 제조업 및 제조업 외 기술개발수행 중소기업 42,110개사(종사자수 5인 이상 300인 미만)인 모집단 중에서 매년 약 2,200개사(제조업 1,779개사, 제조업 이외 업종 421개사)를 표본 추출하여 면접조사, E-mail, 전화조사 등의 방법으로 조사를 진행되었다.

본 연구의 분석 데이터는 KSIC기반 2자리 분류를 기반으로 30개 업종이 포함되어 있으며, 3개년 도에 걸쳐 기술 유출에 의한 피해를 입은 기업들의 수는 415개이다. 표본의 특성을 살펴보면 2011년에 기술유출 피해를 입은 기업수가 216개로 가장 많으며, 2013년(123), 2014(76) 순으로 시간이 지남에 따라 기술 유출에 대한 빈도수가 점점 줄어들고 있다. 향후 유망사업으로 주목받고 있는 6개의 첨단 산업기술 6T(IT, BT, NT, ET, ST, CT)를 기반으로 구분했을 경우에는 해당없음을 제외한 IT(Information Technology)업종이 가장 높은 비율로 기술유출에 의한 피해를 입었으며, 뒤를 이어 ET(Environment Technology), BT(Biology Technology)업종 순으로 높은 것을 볼 수 있다(<Table 1>, <Table 2> 참조).

〈Table 1〉 Technical statistics on KSIC-based technology infringement

Code	2011	2013	2014	Total
10	7	2	2	11
11	2	0	1	3
13	8	3	4	15
14	0	3	1	4
15	4	3	4	11
16	3	5	1	9
17	7	1	0	8
18	4	1	0	5
19	0	1	1	2
20	20	4	5	29
21	4	3	1	8
22	12	6	1	19
23	5	1	2	8
24	2	1	1	4
25	19	10	4	33
26	15	8	3	26
27	21	10	6	37
28	11	12	5	28
29	23	16	8	47
30	10	2	3	15
31	2	1	3	6
32	8	2	1	11
33	12	6	4	22
38	1	0	0	1
58	5	6	4	15
62	1	2	2	5
63	0	2	3	5
70	5	3	3	11
72	5	7	1	13
73	0	2	2	4
Total	216	123	76	415

〈Table 2〉 Number of infringement case based on 6T

	IT	BT	ST	NT	ET	CT	None	Total
2011	42	12	1	0	10	2	149	216
2013	23	4	4	0	11	4	77	123
2014	14	4	0	2	8	1	47	76
Total	79	20	5	2	29	7	273	415

이를 기반으로 본 연구에서는 KSIC 기반의 동종 산업 내에서 연도별로 무작위 추출을 통해 기술 유출에 의한 피해를 입은 기업(n=415)과 피해를 입지 않은 기업(n=415)을 대상으로 1:1대응 표본을 만들어 분석을 수행하였다.

3.2 변수의 측정 및 분석 방법

본 연구에서는 3개년 데이터에서 기술유출 여부를 종속변수로 하였으며 기술 침해를 당한 기업의 경우 1로, 침해를 당하지 않은 기업의 경우 0으로 값을 부여하였다. 독립변수에는 기술 자체 특성 요인과 기술 개발 조직 특성 요인을 사용하였으며, 기술 자체 특성에는 기술의 난이도(Q1), 기술의 신규성(Q2), 기술의 수명주기(Q3), 기술의 모방기간(Q4), 대기업으로부터 기술 이전 요구 유무(Q5) 변수가 포함되어 있다. 기술 개발 조직 특성에는 종사자 수(Q6), 연구원 비율(Q7), 성과보상제 시행 유무(Q8), 기술개발시도 건수(Q9), 기술의 개발 방식 (Q10), 특허 및 지식재산권 등록 현황(Q11), 보안 규정 유무(Q12)을 포함하여 총 12개 문항을 독립변수로 사용하였다. 이러한 문항을 통해 국내 중소기업이 보유하고 있는 기술 유출에 변수들이 미치는 영향력을 측정해 보기 위해 로지스틱 회귀분석을 수행하였다. 로지스틱 회귀 분석의 경우 이항 확률을 가진 종속변수를 통계적으로 사용하기 위해 용이하며, 주가지수, 부도예측, 구매예측 등의 경영학 측면에서 다양하게 활용되고 있다(Barniv et al., 1997; Zhang et al., 1999). 본 연구에서는 로지스틱 회귀분석 모형에 대해 변수 전체를 탐색하기 위해서 모든 변수를 모델에 포함시키는 '입력' 방식을 사용하여 분석을 수행하였다.

4. 연구 결과

4.1 연구 모형 분석

기술 자체 특성과 기술 개발 조직 특성 요인의 총12개의 독립변수들과 종속변수인 기술유출의 관계를 규명하기 위해 로지스틱 회귀분석을 수행한 결과<Table 3>, 기술 자체 특성 요인에서는 기술의 난이도(Q1), 기술의 신규성(Q2), 대기업에서의 기술이전 제안 유무(Q5) 3개의 변수들이 유의하게 도출되었으며, 기술의 수명주기(Q3), 기술의 모방기간(Q4) 변수는 유의하지 않은 것으로 나타났다. 즉 기술 자체의 난이도가 높고, 새로운 기술일수록 기업에서는 기술에 대해 R&D 투자비용과 긴 기간이 소모 되었다는 것이고 이는 기술의 매력도가 증가했음을 의미한다. 따라서 기술의 매력도가 증가하게 되어, 외부에

〈Table 3〉 Results of Research Model

Independent variable	Nonstandard Beta	Standard Beta	Wals	p-value	Exp(B)
Technical Difficulty (Q1)	.349	.116	8.993	.003	1.418
Technical Novelty (Q2)	.234	.085	7.654	.006	1.263
Technical Life Cycle (Q3)	-.023	.046	.243	.622	.977
Technical Imitation Period (Q4)	.012	.058	.039	.844	1.012
Proposal for Transfer of Technology from Large Corporation (Q5)	1.563	.312	25.076	.000	4.771
Number of Employees (Q6)	-.002	.001	1.719	.190	.998
Number of Researchers (Q7)	-.012	.006	3.474	.062	.988
Performance Compensation System (Q8)	.440	.183	5.797	.016	1.553
Number of Technology Development Attempts (Q9)	.256	.079	10.400	.001	1.291
Technology Development Method (Q10)	.101	.155	.425	.514	1.106
Patent and Intellectual Property Registration (Q11)	.004	.002	5.619	.018	1.004
Security Regulation (Q12)	.256	.164	2.427	.119	1.292
Constant	-1.777	.331	28.830	.000	.169

서 기술을 유출하려는 유인이 커지게 되어 유출의 위험 역시 커질 것임을 추측해볼 수 있다. 기술 개발 조직 특성 요인에서는 연구원 비율(Q7), 성과보상제 유무(Q8), 기술개발 시도건수(Q9), 특허 및 지식재산권 등록현황(Q11) 4개의 변수들이 유의하게 도출되었고, 종사자 수 (Q6), 기술의 개발 방식(Q10), 보안 규정 유무(Q12)변수들은 유의하지 않은 것으로 나타났다. 특히, 기술유출로 인한 피해에 대해 유의하게 도출된 변수들 중 기술의 난이도 및 신규성, 대기업에서의 기술이전 제안 유무, 성과보상제 유무, 기술개발 시도건수, 특허 및 지식재산권 등록 현황 변수들은 모두 양의 상관관계를 나타나고 있지만, 연구원 비율 변수 유의수준($p<.10$)수준으로 음의 상관관계를 나타내고 있다. 즉 기업에 종사하는 연구원의 수가 작을수록 기술유출의 가능성이 커지는 것을 의미하며, 이는 기업의 규모가 작아 인적 자원에 대한 보안관리가 미흡하였거나, 중소기업이 보유하고 있는 핵심 기술에 대한 중요정보를 알고 있는 연구원이 소수이기 때문에 오히려 유출에 대한 유인이 더 컸을 것으로 추측해 볼 수 있다. 유의하게 도출된 변수들 중 대기업에서의 기술이전 제안 유무가 가장 강한 영향력을 보이고 있으며, 성과보상제도 유무, 기술의 난이도, 기술개발 시도건수, 기술의 신규성 순으로 영향력이 나타나고 있다.

4.2 SVM을 통한 지능형 기술 유출 조기경보시스템

마지막으로 본 연구에서는 앞서 제시한 모든 요인들을 사용하여, 인공지능기법 중 하나인 SVM(Support Vector Machine)을 통해 기술 유출 예측 모형을 설계하였다. 예측 모형을 설계하기 위한 기법으로는 로지스틱 회귀분석, ANN(Artificial Neural Network), CBR(Case-based Reasoning)등과 같은 기법들이 있지만, SVM은 타 기법에 비해 예측성과가 가장 높고, 적은 학습자료 만으로

〈Table 5〉 Experiment result on Polynomial/Radial Basis Function Kernel

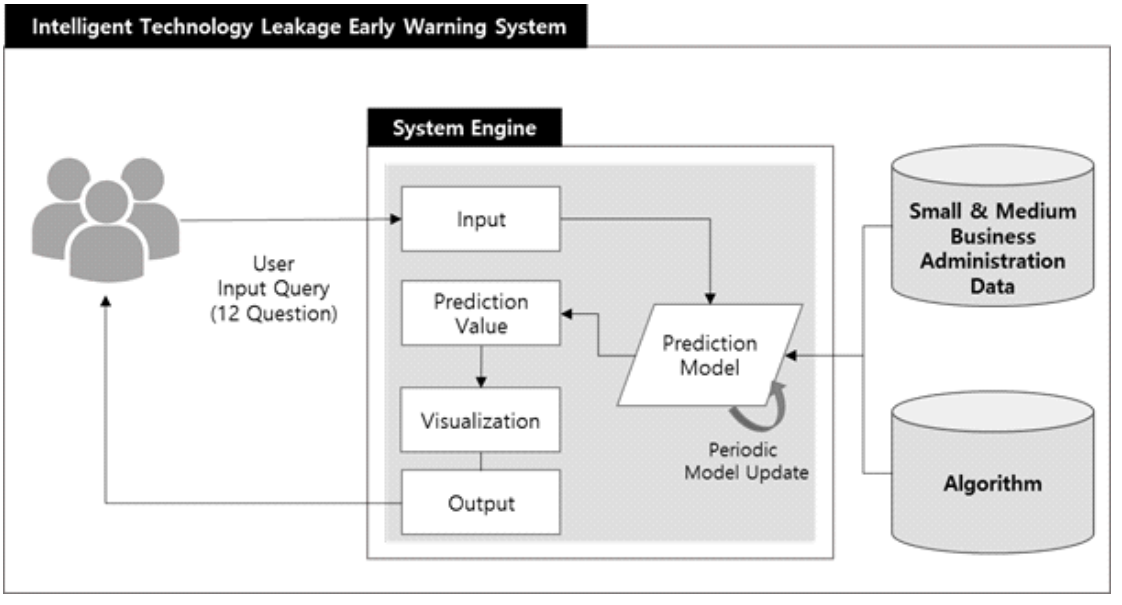
Type	C	d	Training	Validation	Type	C	δ^2	Training	Validation
Polynomial Kernel	1	1	62.80%	63.86%	RBF Kernel	1	1	92.17%	59.04%
		2	60.99%	62.05%			25	65.51%	62.05%
		3	64.46%	60.84%			50	62.95%	63.25%
		4	71.23%	58.43%			75	60.54%	64.46%
		5	75.15%	57.23%			100	59.34%	65.06%
	10	1	60.84%	59.64%		10	1	95.48%	57.23%
		2	63.40%	59.64%			25	68.07%	63.25%
		3	70.48%	60.24%			50	64.01%	66.27%
		4	76.96%	57.83%			75	64.01%	67.47%
		5	83.43%	56.63%			100	63.55%	65.66%
	33	1	60.84%	59.04%		33	1	96.69%	57.83%
		2	63.86%	62.05%			25	71.23%	61.45%
		3	72.44%	62.05%			50	66.57%	66.27%
		4	79.82%	59.04%			75	64.01%	63.86%
		5	85.09%	61.45%			100	63.25%	65.06%
	55	1	60.84%	59.04%		55	1	97.14%	59.04%
		2	65.36%	60.84%			25	72.59%	61.45%
		3	74.10%	59.64%			50	67.17%	64.46%
		4	81.48%	55.42%			75	65.21%	65.06%
		5	86.30%	59.64%			100	64.16%	65.06%
	78	1	60.84%	59.04%		78	1	97.59%	59.04%
		2	67.17%	61.45%			25	73.34%	61.45%
		3	74.70%	58.43%			50	68.37%	63.25%
		4	82.23%	56.63%			75	65.81%	66.27%
		5	87.05%	59.64%			100	64.76%	65.06%
	100	1	60.84%	59.04%		100	1	97.59%	58.43%
		2	67.02%	62.05%			25	74.25%	61.45%
		3	75.60%	57.83%			50	69.58%	61.45%
		4	82.98%	56.63%			75	66.57%	66.87%
		5	87.35%	59.04%			100	64.61%	65.06%

도 신속하게 수행이 가능하며, 비교적 간단한 방법으로 좋은 성능을 낼 수 있는 장점이 있다(Ahn, et al., 2005). 본 연구에서는 SVM의 커널 함수로서 다항식 커널과 RBF 커널을 사용하여 커널함수의 상한 C와 커널 파라미터(d, δ^2)에 다양한 값들을 대입해 실험을 수행하였는데, Tay & Cao(2002)에 따라 C의 값을 1, 10, 33, 55, 78, 100으로 설정하였고, δ^2의 값을 1, 25, 50, 75, 100으로 설정하여, 각각의 값을 다르게 대입해 보았다. SVM을 실험하기 위해서 LIBSVM을 사용하였다. SVM 실험 결과, RBF 커널 적용 시 C=10, δ^2=75일 때, 67.47%로 가장 우수한 예측률을 보이고 있음을 알 수 있다(<Table 5> 참조).

본 연구에서 사용된 12개의 문항들과 SVM을 통한 예측 알고리즘을 기반으로 지능형 기술 유출 조기경보 시스템을 설계하였다(<Figure 2> 참조). 사용자가 12개 문항에 대해 값을 입력하면, 중소기업청에서 제공하는 기술유출 데이터와 SVM기반의 알고리즘을 통해 설계된 예측모형에서 분석을 수행하게 된다. 모형에서는 수행된 분석의 결과물로 예측 값을 추출하게 되고, 이는 시스템 엔진에서 시각화과정을 거쳐 결과 값을 최종적으로 사용자에게 보여주게 된다.

5. 결론

본 연구에서는 중소기업청과 중소기업중앙회에서 수행한 중소기업기술통계 조사 문항을 바탕으로 중소기업의 기술 유출에 영향을 미치는 요인들을 알아보기 위해 기술유출 중소기업 415개, 기술유출 미경험 중소기업 415개에 대해 통계분석을 수행하였다. 분석을 위해 기술 자체 특성, 기술 개발 조직 특성 총 두 가지 요인으로 구분하였고, 요인들에 속하는 각각의 변수들이 중소기업의 기술유출에 어떠한 영향을 미치는지



〈Figure 2〉 Intelligent Technology Leakage Early Warning System

회귀분석을 통해 가설을 검증하였다. 마지막으로 전체 요인들에 대해 데이터마이닝 기법을 사용하여 중소기업의 기술침해가능성을 조기에 알려주는 모형을 개발해보았다.

본 연구는 각각 세 가지 이론적 공헌과 실무적 공헌을 가지고 있다. 이론적인 공헌에는 첫 번째, 기존 중소기업 기술유출과 관련된 연구들에서는 기술유출과 관련된 요인들을 주로 보안 정책, 조직에 중점을 두고 분석을 하였지만, 본 연구에서는 중소기업이 보유하고 있는 기술 자체의 특성과 조직의 특성 두 가지 모두를 고려하여 통합적으로 분석해본 점이 공헌이라 할 수 있겠다. 둘째, 3개년에 걸쳐 기술 유출 피해를 보고한 다수의 중소기업을 대상으로 분석했다는 점이 의의가 있다. 기존의 연구는 단 개년의 소수의 데이터만으로 분석을 행하고 있는데, 본 연구에서는 다개년 다수의 다양한 업종 사례를 중심으로 연구를 진행했다는 점이 의미 있다. 마지막으로 본 연구는 인공지능 모형 개발 관점에서 의미를 가질 수 있는데, 기존 인공지능 연구가 다루지 않은 기술 침해 부분을 기술 침해 유무의 대응 표본을 중심으로 조기 경보 모형을 개발했다는 점이 기존의 인공지능 연구 분야를 넓히는 데 기여했다고 볼 수 있다.

실무적인 공헌으로는 첫 번째, 실제 중소기업 기술 유출 피해의 유무에 따라서 실증적으로 요인들을 도출하였기 때문에, 정책 담당자에게 어떤 기업들이 기술 보호 관점에서 관리되어야 하는지 방향성을 제시하였다는 점이다. 둘째, 중소기업 관점에서도 자신의 현재 상태 및 개발하고 있는 기술 특성에 입각해서, 기술 유출 관련되어 얼마나 많은 자원을 할당하여 보호해야 하는지의 전략적 의사결정에 도움을 줄 수 있다. 마지막으로 본 연구가 제안하는 기술 유출 조기 경보 시스템의 활용 관점에서 공헌을 가진다. 기술 유출은 예방이 무엇보다 중요한데, 기술 유출의 가능성에 대한 조기 경보는 기업 및 정부 관점에서 기술 유출을 미리 예방할 수 있는 기회를 제공한다는 측면에서 의미 있을 것으로 사료된다.

이러한 공헌에도 불구하고 본 연구에서는 중소기업 데이터를 기반으로 분석을 수행하였기 때문에 기술유출에 대해 대기업은 분석대상에서 배제되었다는 점, 산업별 표본이 부족하여 산업군별 분석을 수행하지 못하였다는 점, 설문 조사가 대상자의 기억에 의존한 응답이기 때문에 회상 편향(recall bias)의 한계점이 있을 수 있다. 데이터를 기반으로 하는 정량적인 분석과 실제 고충을 파악해 볼 수 있는 정성적인 분석이 함께 설계되고 수행된다면, 더 완성도 있는 연구가 될 수 있을 것이라고 기대한다.

참고문헌(References)

Ahn, H. C., I. G. Han, and K. J. Kim, "Purchase prediction model using the support vector machine," *Journal of Intelligence and Information Systems*, Vol.11, No.3(2005), 69~81.

Barniv, R., A. Agarwal, and R. Leach, "Predicting the outcome following bankruptcy filing: a three-state classification using neural networks," *Intelligent Systems in Accounting, Finance and Management*, Vol.6, No.3 (1997), 177~194.

Chae, J. W. and Y. H. Ko, "Exploring case Study on Security Factors and Strategy to Prevent Leakage of Corporate Information for CEO," *The Journal of Professional Management*,

Vol.15, No.1(2012), 87~113.

Chang, E. M., "Effects of Individual Performance Based Compensation on Employee's Work Effort: In the context of Commitment HR Bundles," *Korean Journal of Management*, Vol.11, No.1, 133~158.

Chang, H. B. and J. H. Song, "The Exploratory Study on the Evaluation of Security System for Industrial Technology Leakage Prevention," *Korean Journal of Industry Security*, Vol.1, No.1(2009), 50~61.

Choi, E. R., B. G. Lee, Y. I. Park, and K. M. Park, "A Study on the Leaking Channels of Industrial Technology," *Police Science Institute*, Vol.26, No.1(2012), 225~260.

Choi, P. A. and M. H. Lee, "A Study on Industrial Security Factors Influencing Industrial Technology Outflow Prevention Using Logistic Regression," *The Korean Society of Private Security*, Vol.12, No.3(2013), 182~206.

Deci, E. L., & R. M. Ryan, "The empirical exploration of intrinsic motivational processes," *Advances in experimental social psychology*, Vol.13(1980), 39~80.

Heneman, R. L., *Merit pay: Linking pay increases to performance ratings*. Addison Wesley Longman, 1992

Hong, J. P., "The Effect of Technological Collaboration on the Innovation Performance of Small and Medium-sized Firms," *The Journal of Small Business*, Vol.27, No.3(2005), 3~32.

Hong, J. S., W. H. Park, Y. H. Kim, and K. H. Kook, "Small Business Technological Assets Protection Factors Analysis Using Logistic Regression Analysis," *The Journal of Society for e-Business Studies*, Vol.20, No.3(2015), 1~10.

Hwang, H. D. and C. M. Lee, "A Study on the Relationship between Industrial Espionage, Self-Control, and Organizational Commitment," *Korean Security Science Review*, No.47(2016), 119~137.

Jung, J. S., "The Study of Protective Solution and People in Technology Outflow about SMEs," *International commerce and information review*, Vol.17, No.3(2015), 133~152.

Kim, D. B. and J. H. Kim, "Antecedents of the Performance Based Pay: A Comparison of Japanese and Korean Firms," *Quarterly Journal of Labor Policy*, Vol.11, No.1(2011), 25~54.

Kim, H. J. and J. H. Ahn, "An Empirical Study of Employee's Deviant Behavior for Improving Efficiency of Information Security Governance," *The Journal of Society for e-Business Studies*, Vol.18, No.1(2013), 147~165.

Kim, M. B. and K. J. Kim, "The law regarding the outflow prevention & a protection of industrial technology and Issues," *Intellectual Property Society*, Vol.23, No.2(2007), 1~36.

Kim, U. J, *Modern technology management, economics*, Ajin, Seoul, 2007

Korea Small Business Institute, "Status and Tasks of SME Technology Protection Support Policy", *KOSBI SME Foucs*, Vol.14, No.17(2014).

Lee, C. S. and Y. H. Kim, "An Analysis of Relationship between Industry Security Education and Capability," *The Journal of Society for e-Business Studies*, Vol.20, No.2(2015), 27~36.

Lee, M. S. and R. G. Choe, "Imitation Strategy, Environment, and Business Performance in followers," *Korean Management Review*, Vol.31, No.2(2002), 405~429.

Mohr, J. J., "The management and control of information in high-technology firms," *The Journal of High Technology Management Research*, Vol.7, No.2(1996), 245~268.

Noh, M. S. and S. Y. Lee, "Explaining Industrial Security of SMEs in Korea," *Korean Public Administration Review*, Vol.44, No.3(2010), 239~259.

Tay, F. E. and L. J. Cao, "Modified support vector machines in financial time series forecasting," *Neurocomputing*, Vol.48, No.3(2002), 847~861.

Yang, K. Y., "The Limitations and New Agendas for the New Managerial Reform Initiatives in Korean Local Governments," *The Korean Journal of Local Government Studies*, Vol.8, No.2(2004), 245~265.

Yu, G. C., "Determinants and Organizational Effectiveness of Performance-based Human Resource Management," *Korean Journal of Management*, Vol.15, No.3(2007), 187~224.

Zhang, G., M. Y. Hu, B. E. Patuwo, and D. C. Indro, "Artificial neural networks in bankruptcy prediction: General framework and cross-validation analysis," *European journal of operational research*, Vol.116, No.1(1999), 16~32.

Abstract

Development on Early Warning System about Technology Leakage of Small and Medium Enterprises

Bong-Goon Seo* · Do-Hyung Park**

Due to the rapid development of IT in recent years, not only personal information but also the key technologies and information leakage that companies have are becoming important issues. For the enterprise, the core technology that the company possesses is a very important part for the survival of the enterprise and for the continuous competitive advantage. Recently, there have been many cases of technical infringement. Technology leaks not only cause tremendous financial losses such as falling stock prices for companies, but they also have a negative impact on corporate reputation and delays in corporate development. In the case of SMEs, where core technology is an important part of the enterprise, compared to large corporations, the preparation for technological leakage can be seen as an indispensable factor in the existence of the enterprise. As the necessity and importance of Information Security Management (ISM) is emerging, it is necessary to check and prepare for the threat of technology infringement early in the enterprise.

Nevertheless, previous studies have shown that the majority of policy alternatives are represented by about 90%. As a research method, literature analysis accounted for 76% and empirical and statistical analysis accounted for a relatively low rate of 16%. For this reason, it is necessary to study the management model and prediction model to prevent leakage of technology to meet the characteristics of SMEs. In this study, before analyzing the empirical analysis, we divided the technical characteristics from the technology value perspective and the organizational factor from the technology control point based on many previous researches related to the factors affecting the technology leakage. A total of 12 related variables were selected for the two factors, and the analysis was performed with these variables.

In this study, we use three - year data of "Small and Medium Enterprise Technical Statistics Survey" conducted by the Small and Medium Business Administration. Analysis data includes 30 industries based

* Graduate School of Business IT, Kookmin University
** Corresponding Author: Do-Hyung Park
School of Management Information System, Kookmin University
Jeongneung-Ro 77, Seongbuk-Gu, Seoul, 02707, Korea
Tel: +82-2-910-4018, Fax: +82-2-910-4017, E-mail: dohyungpark@koomin.ac.kr

on KSIC-based 2-digit classification, and the number of companies affected by technology leakage is 415 over 3 years. Through this data, we conducted a randomized sampling in the same industry based on the KSIC in the same year, and compared with the companies (n = 415) and the unaffected firms (n = 415) 1:1 Corresponding samples were prepared and analyzed.

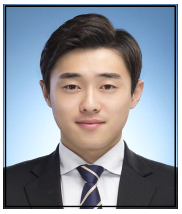
In this research, we will conduct an empirical analysis to search for factors influencing technology leakage, and propose an early warning system through data mining. Specifically, in this study, based on the questionnaire survey of SMEs conducted by the Small and Medium Business Administration (SME), we classified the factors that affect the technology leakage of SMEs into two factors(Technology Characteristics, Organization Characteristics). And we propose a model that informs the possibility of technical infringement by using Support Vector Machine(SVM) which is one of the various techniques of data mining based on the proven factors through statistical analysis.

Unlike previous studies, this study focused on the cases of various industries in many years, and it can be pointed out that the artificial intelligence model was developed through this study. In addition, since the factors are derived empirically according to the actual leakage of SME technology leakage, it will be possible to suggest to policy makers which companies should be managed from the viewpoint of technology protection. Finally, it is expected that the early warning model on the possibility of technology leakage proposed in this study will provide an opportunity to prevent technology Leakage from the viewpoint of enterprise and government in advance.

Key Words : Technology Leakage, Datamining, Early Warning System, SVM

Received : March 13, 2017 Revised : March 20, 2017 Accepted : March 20, 2017
Publication Type : Regular Paper Corresponding Author : Do-Hyung Park

저 자 소 개



서 봉 군
국민대학교 경영정보학부에서 학사 학위를 취득하였으며, 현재 동 대학원에서 Customer Experience, Business Analytics 트랙으로 석사과정에 재학 중이다. 주요 관심 분야는 Customer Experience, Customer Analytics, Experience Design 등이다.

박 도 형
KAIST 경영대학원에서 MIS 전공으로 석사/박사학위를 취득하였다. 현재 국민대학교 경영대학 경영정보학부 조교수로 재직 중이며, 한국과학기술정보연구원(KISTI)에서 유망 아이템 발굴, 기술가치 평가 및 로드맵 수립, 빅데이터 분석 등을 수행하였고, LG전자에서 통계, 시선/뇌파 분석, 데이터 마이닝 등 활용한 연구 및 소비자 평가 모형을 개발을 담당했었고, 스마트폰, 스마트 TV, 스마트Car 등에 대한 Technology, Business, Market Insight 기반 컨셉 도출 프로젝트를 다수 수행하였다. 현재 주여 관심 분야는 SNS나 온라인 구전 등의 사용자 행동 이론(User Behavior), 사용자 경험 디자인 프로세스 및 혁신 제품 발굴(User eXperience), 빅데이터 기반 사용자 분석(User Analytics) 등이다.