Society of Korea Industrial and Systems Engineering Vol. 37, No. 2 : 77-84, June 2014 ISSN : 2005-0461(print)
http://dx.doi.org/10.11627/jkise.2014.37.2.77 ISSN : 2287-7975(online)

A Study on Improvement Plans for Technology Protection of SMEs in Korea

Jang Hoon Lee*† · Wan Seon Shin** · Hyun Ju Park***

*Management Strategy Team, Samsung Thales
**Department of Systems Management Engineering, Sungkyunkwan University
***Department of Management of Technology, Sungkyunkwan University

중소기업 기술보호 개선방안에 대한 연구

이장훈*† · 신완선** · 박현주***

*삼성탈레스 경영전략팀
**성균관대학교 시스템경영공학과
***성균관대학교 기술경영학과

The purpose of this research is to identify and develop technology protection plans for small and medium-sized enterprises (SMEs) by analyzing past technology leakage patterns which were experienced by SMEs. We identified factors which affect the technology leakage, and analyzed patterns of the influences using a data mining algorithms. A decision tree analysis showed several significant factors which lead to technology leakage, so we conclude that preemptive actions must be put in place for prevention. We expect that this research will contribute to determining the priority of activities necessary to prevent technology leakage accidents in Korean SMEs. We expect that this research will help SMEs to determine the priority of preemptive actions necessary to prevent technology leakage accidents within their respective companies.

Keywords : Technology Protection, Technology Leakage, Industrial Security

1. 서 론

최근 국내 기업의 핵심기술 유출은 해마다 증가하고 있고 국가적인 차원에서 피해액 손실도 매년 크게 증가하고 있다. 최근 5년간 우리나라 주요 사업의 기술유출에 따른 피해액은 220조 원에 달했고 2010년 총 예산과 비슷한 액수이다[3]. 국정원 발표에 의하면 산업기밀보호센터가 창설되어 본격적으로 활동을 시작한 지난 2004년부터 2010년까지 우리 산업기술의 불법적인 해외유출 적발사건이 총 244건에 달할 뿐만 아니라 해마다 증가추세를 보이는 것으로 나타나 우리기술 유출에 대한 심각성을 느끼게 하고 있다[11].

첨단기술 유출을 방지하는 것은 쉬운 일이 아니며 첨단기술은 본질적으로 무체물이고 비배제성(non-excludability)을 특징으로 하기 때문에 첨단기술이 제 3자에게 공개된 경우에는 이를 물리적으로 회수할 방법이 없다. 첨단기술은 유출되기 전에 보호하는 것이 가장 중요하다. 그러한 보호방법은 첨단기술 소유자의 보호노력에서 시작된다고 할 것이다. 그리고 차선책으로는 타당하고 효과적인 법적 보호방법을 강구하는 것이 필요하다[12]. 지난 2010년 기준 전체 기업 수 대비 중소기업이 차지하는 비중은 전체의 99%에 이르고 있으며, 중소기업이 차지하는 총

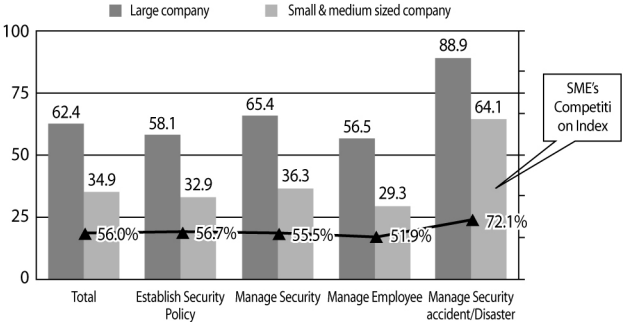
Received 16 April 2014; Finally Revised 29 May 2014;
Accepted 24 June 2014
† Corresponding Author : stephen153@naver.com

수출 비중(직수출 및 대기업을 통한 간접수출 포함)은 전체의 38.8%를 나타내고 있다[4]. 지난 2010년 국내 모든 기업의 산업기밀 유출범죄 피해는 발생건수 1건당 평균 약 16억 7천만 원 정도의 피해금액을 보이고 있는 것으로 나타나고 있다. 이 가운데, 대기업은 유출 1건당 약 39억 2천만 원의 피해금액을 경험하고 있으며, 중소기업은 10억 6천만 원 정도의 피해금액을 경험하고 있다[9]. 이처럼 국가경제에 있어 중소기업이 차지하는 비중만 보더라도 그 중요성은 매우 크다 할 수 있다.

2012년 중소기업청과 중소기업기술정보진흥원에서 중소기업 기술보호 역량 및 수준을 조사한 결과, 전체 조사대상 기업 1,566개 중 최근 3년간 기술유출 경험이 있는 중소기업이 12.1%로 나타났다. 또한 중소기업의 기술유출 실태를 빈도별로 볼 때 '1회' 유출이 73.6%로 가장 많았고, '2회' 이상은 26.3%로 나타나 기술유출을 반복적으로 경험하는 중소기업이 여전히 존재하고 있었다. 중소기업의 피해금액은 건당 15.7억 원으로 대기업(25.1억 원)의 2/3 수준인 것으로 조사되어 기술유출 피해 발생 시 중소기업에 미치는 영향력이 대기업에 비해 상대적으로 매우 높음을 시사하고 있으며, 중소기업의 역량 부족으로 기술유출 우려가 큰 상황 속에서 이러한 문제점은 더욱 심화되고 있다.

국가정보원 산업기밀보호센터에서 2005년부터 2012년까지 8년간 국내에서 발생한 산업스파이 사건 현황을 조사한 결과, 최근 5년간의 기술유출건수 202건 중 71%가 중소기업에서 발생하였다[14]. 2012년 기술보호 역량지수는 36.1점, '취약' 수준으로 평가되었으며, 기업규모별로 대기업은 62.4점으로 양호한 수준을 나타냈고, 중소기업의 기술보호 역량(34.9점)은 전반적으로 대기업의 절반을 조금 넘는 수준인 것으로 조사되었다[10]. 기술보호 역량 평가결과 중소기업의 42.4%는 '위험' 수준으로 진단되었고, '취약' 수준은 29.4%를 차지한 것으로 나타나, 인력과 자금력이 열악한 중소기업 기술보호 역량의 현주소를 보여주고 있다. <Figure 1>에서 "중소기업 경쟁지수[1])"를 살펴보면, 중소기업의 기술보호 역량은 전반적으로 대기업의 절반을 조금 넘는 수준인 것으로 나타났으며, '보안사고/재해관리' 측면에 대한 관리 역량은 대기업과의 간극이 다소 좁혀진 것으로 나타났다(중소기업 경쟁지수 72.1%).

이와 같이 중소기업의 기술유출은 매우 심각한 상황이며, 대기업에 비해 기술보호 역량이 부족하여 여전히 많은 위험에 노출되어 있고 기업성장의 걸림돌이 되고 있다. 그러나 자금과 인력이 부족한 중소기업에서 대기업 수준의 보안관리 환경을 갖추기란 현실적으로 어려움이 있는 것 또한 현실이다. 중소기업기술정보진흥원 조사결과에 따르면 중소기업이 느끼는 기술보호의 가장 큰



<Figure 1> SME's Competition Index

애로사항은 '예산부족(1순위 44.5%)으로 가장 높게 나타났다. 따라서 자금과 인력, 그리고 기술유출 방지를 위한 환경이 부족한 중소기업에서는 가장 빈번히 발생하는 기술유출 대상과 기술유출 수단에 역량을 집중하여 우선적으로 기술유출 방지를 위한 개선활동을 할 필요가 있다.

본 논문에서는 기술유출을 경험한 기업들의 패턴을 분석하고자 한다. 데이터마이닝 알고리즘을 이용하여 기술유출에 영향을 미치는 요인이 무엇인지, 어떤 요인이 가장 큰 영향을 미치는지 등에 대한 패턴을 분석한다. 본 논문에서 제시한 분석결과와 개선방안을 활용하면, 자금과 역량이 부족한 중소기업에서 기술정보 유출사고 예방을 위해 사전에 어떤 활동을 우선적으로 강화해야 하는지 등 기술보호 개선방안을 수립하는데 도움이 될 것이다.

본 논문의 구성은 다음과 같다. 제 2장에서는 기술유출과 기술보호 관련 선행연구에 대해 살펴보고, 제 3장에서는 본 논문이 제안하는 데이터마이닝 의사결정나무 분석 방법에 대해 설명한다. 제 4장에서는 분석결과를 근거로 중소기업 기술유출 방지를 위한 개선방안에 대해 제시하고, 제 5장에서는 결론을 맺을 것이다.

2. 선행연구 검토

2.1 기술유출 방지를 위한 관리적 대응방안 연구

허승표 외 4명은 "군집화를 이용한 기업 핵심기술 분류에 관한 연구"에서 내부 인력에 대한 사전 정보를 데이터마이닝 방법을 통해 핵심기술 유출 징후 분류 방법을 제안하고 기밀 유출자 행위 분석을 토대로 유출 가능성이 있는 그룹을 도출하였다[3]. 정태황 외 1명은 "산업기술보호 관리실태 및 발전방안에 관한 연구"에서 국가핵심기술 보유 기관을 대상으로 관리적 보안업무 실태를 조사/분석하여 대응방안을 제시하였다[6]. 채정우 외 1명은 "전문경영인의 기업정보 보호를 위한 산업기술 유출요인과 대응전략에 대한 탐색적 사례연구"에서 2010년도 산업

1) 중소기업 경쟁지수 = 중소기업역량지수/대기업 역량지수.

기밀 유출 사례 5건을 분석하여 산업기술 유출에 영향을 미치는 5가지 보안관리 요인(기술매력도, 보안정책, 물리 공간 통제, 가상 공간 통제, 유출행위자)을 도출하고 산업기술유출방지 관리 프레임을 제시하였다[1]. 장항배는 "중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계"에서 델파이 방법을 적용하여 중소기업 산업기술 유출방지 관리체계를 수립하였다. 3개의 관리체계 영역(지원역량, 지원환경, 기반구조), 5개의 관리체계 항목(교육 및 훈련, 관리적 보안, 인적보안, 물리적 보안, 기술적 보안)과 22개의 관리체계 세부항목을 설계하였다[2].

2.2 기술유출 방지를 위한 제도 · 정책적 대응방안 연구

나종갑은 "국제 M&A 및 인력이동과 첨단산업 기술유출 방지제도 연구"에서 국제규범상의 문제와 국제 M&A를 통한 기술유출방지에 관한 하나의 모델법이라 할 수 있는 미국의 EXON-FLORIO ACT를 고찰하고 우리나라의 산업기술의 유출방지 및 보호에 관한 법률의 내용과 문제점, 그리고 기술인력에 의한 유출방지 관련제도의 문제점에 대해 제시하였다[12]. 임창묵은 "기술유출방지를 위한 정책수단에 관한 연구"에서 현재 시행중인 산업보안정책을 정책수단 측면에서 분석하고 개선방안 제시, 정부는 규제측면에서 기술유출 규제내용을 명확히 하여 법 적용의 실효성을 제고시켜야 하며 유인 측면에서는 기술유출방지를 위한 예산 및 기술지원을 통해 기업 측의 자발적인 협조를 유도하여 기술보호 효과를 높이도록 해야 하고, 정보제공 측면에서는 기업 측이 지속적인 교육을 통해 관련규정에 대한 인식을 제고시키고 기업윤리 의식을 향상시킴으로써 잠재적인 범행의지를 감소시켜야 한다고 주장하였다[11]. 남재성은 "중소기업의 산업기밀 유출범죄 피해실태와 대책-법·제도적 방안을 중심으로"에서 중소기업의 산업기밀 유출실태를 살펴 본 후 그 피해를 감소시킬 수 있는 4가지 법·제도적 방안을 제시하였다[13]. 노민선 외 1명은 "중소기업의 산업보안 역량에 대한 영향요인 평가"에서 중소기업의 산업보안 역량수준에 영향을 미치는 요인을 살펴보고, 실증분석 결과를 중심으로 중소기업의 보안역량 제고를 위해 정부 차원에서 우선적으로 추진해야 할 6가지 방안을 제시하였다[15].

2.3 기술유출 방지를 위한 보안시스템 구축방안 연구

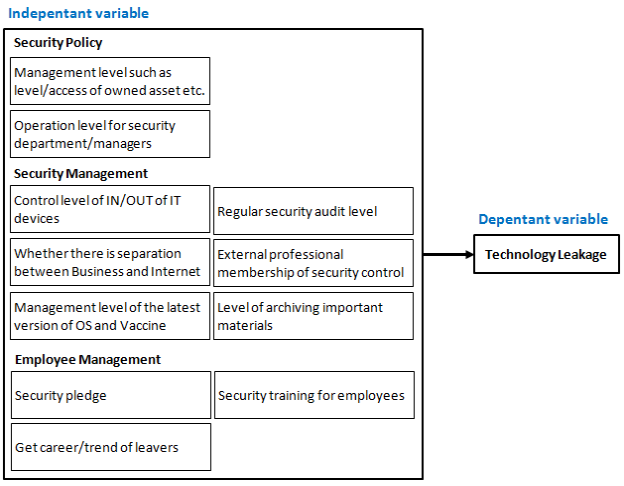
정진홍 외 1명은 "기술유출 방지를 위한 과학적 보안시스템의 구축방안에 관한 연구"에서 기술유출 방지를 위한 다양한 보안시스템 구축 방법 등 기술적 보안측면(보안시스템, 네트워크 보안조치, PC보안, 주변기기 보안관리로 구분)에서 어떤 조치들이 취해져야 하는지 제시하였다[5]. 윤인수는 "내부자에 의한 정보유출 방지를 위한 보안시스템 구축에 관한 연구"에서 기존의 정보유출 방지 시스템이 해킹과 같은 외부의 침입만을 차단하는데 치중되어 있음을 지적하며 내부자에 의한 정보유출을 차단하기 위한 시스템을 설계하였다[18]. 김민수는 "중소기업을 위한 정보유출 방지 시스템 설계 연구"에서 중소기업의 정보유출 예방 시스템의 DB 해킹을 탐지하고 방지하는 등 기술적 위험을 관리할 수 있고, 중소기업 여건에 적용 가능한 GUI 환경의 정보유출예방시스템을 설계하였다[7]. 신관선, "우리나라 산업기술 보안시스템 발전방향에 관한 연구"에서 기존 문헌 연구를 통해 우리나라와 선진국의 산업기술 보안시스템의 특성과 기술유출 실태를 살펴보고, 산업기술 보안시스템 발전 방향을 국가와 기업 차원에서 제시하였다[16].

3. 연구방법

3.1 연구모형 및 변수정의

3.1.1 연구모형

연구모형은 중소기업청과 중소기업기술정보진흥원에서 기술유출방지 지원방안 및 장기적인 정책 수립을 목적으로 실시한 <2012년 중소기업 기술보호 역량 및 수준조사>에서 구분한 설문항목 카테고리(보안정책, 보안관리, 인력관리)를 준용하여 <Figure 2>와 같이 정리하였다.



<Figure 2> Research Model

3.1.2 변수 정의

종속변수 : 기술정보 유출 여부

독립변수 : 보유자산 등급/접근 등 관리 수준, 보안 관리 부서/관리자 운영수준, 정보화기기 반입/반출

통제 수준, 업무용-인터넷용 통신망 분리여부, OS/백신 최신버전 관리 수준, 정기적인 보안감사 실시 수준, 외부 전문 보안관제서비스 가입 여부, 보안서약서 징구 실시 여부, 퇴사자 진로/동향 파악, 직원 보안교육, 중요자료 보관 시행 수준

본 연구에서는 앞서 제시한 개념적 연구모형을 실증적으로 검증하기 위해 중소기업청과 중소기업기술정보진흥원에서 기술유출방지 지원방안 및 장기적인 정책 수립을 목적으로 실시한 <2012년 중소기업 기술보호 역량 및 수준조사> 결과를 2차 데이터로 활용하였다. 중소기업 기술보호 역량 및 수준조사에서는 기술유출 실태, 대기업 대비 중소기업의 기술보호 역량 평가 등을 측정할 수 있는 항목이 포함되어 있다. 2012년 실시된 중소기업 기술보호 역량 및 수준조사에서는 부설연구소를 보유한 중소기업 11,912개사 중 업종, 기술유출방지사업 수혜기업을 고려하여 선정한 1,501개 기업과 비교대조군으로 대기업 65개를 대상으로 하여 인터넷과 전화, 그리고 팩스/이메일을 통해 설문조사를 실시하였으며, 유효한 설문은 1,566개로 나타났다.

본 연구는 중소기업의 기술보호 개선방안에 대한 연구를 목적으로 하므로 전체 유효설문 1,566개 설문 중 중소기업 1,501개 설문결과만을 분석에 활용하였다. 실제 분석을 수행하기 위해 <Figure 2>에서 제시한 연구모형과 관련이 있고 보안정책, 보안관리, 인력관리 각 항목별 내용이 중복되는 설문은 배제하고, 각 항목별 수준을 대표할 수 있는 11건의 설문을 선별하여 해당 설문 결과만을 분석에 활용하였다.

3.2 분석방법론

3.2.1 데이터마이닝 의사결정기법을 이용한 분석

중소기업 기술보호 역량 및 수준조사 결과 데이터를 활용하여 분석범주를 선택한다. 사전 설정한 분석범주별 분석할 설문항목을 정의하고, 각 항목별 독립변수와 종속변수를 설정한다. 분석의 목적이 설문문항 간의 패턴을 도출하기 위함으로 본 논문에서는 의사결정나무 분석기법을 적용한다. 분석도구로 SPSS 18 분류분석을 이용하였다.

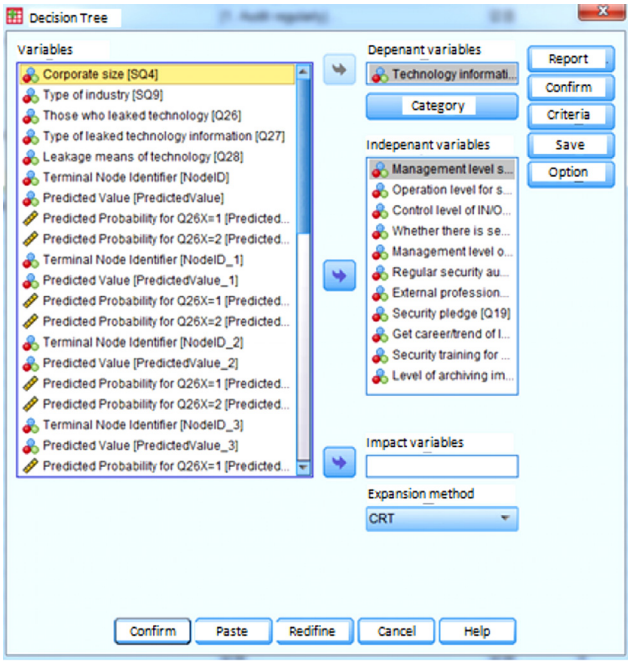
<Table 1> Variable Definition

Variable	Criteria
Management level such as level/ access of owned asset etc.	1. Instruction for asset classification criteria is clear and is implemented according to the current instruction. 2. Instruction is established, but is not being implemented. 3. No instruction, no systematic administration
Operation level for security department/managers	1. Designate only security manager 2. Designate only full-time security manager 3. Designate only interlocking security manager 4. No security department/managers 5. Designate only full-time/interlocking security managers
Control level of IN/OUT of IT devices	1. Control IN/OUT of all IT devices into the company grounds, 2. Control IN/OUT of part of IT devices into the company grounds, 3. No control IN/OUT of IT devices
Whether there is separation between Business and Internet network	1. Seperation between internal and external network 2. No Seperation between internal and external network
Management level of the latest version of OS and Vaccine	1. Managed 2. Not managed
Regular security audit level	1. Audit regularly 2. Audit if needed(non-regularly) 3. No audit
External professional membership of security control service	1. Joined 2. Not joined
Security pledge	1. Conducted 2. Not conducted
Get career/trend of leavers	1. Get trend of all leavers 2. Get trend of major leavers 3. Not get trend of leavers
Security training for employees	1. Regular security training for all employees at least once a year 2. Regular security training for part of employees at least once a year 3. Non-regular security training if needed
Level of archiving important materials	1. Regular back-up by itself 2. Non-regular back-up by itself 3. Back-up through external professional services 4 .Not managed
Technology information leakage	1. leaked 2. Not leaked

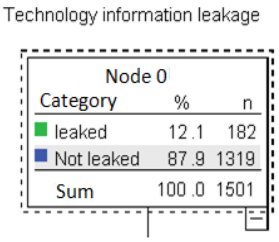
3.2.2 SPSS 18을 활용한 의사결정트리 분석

변수 설정을 위해 <Figure 3>과 같이 “기술정보 유출여부”를 종속변수로 지정하고 “보유자산 등급/접근 등 관리수준” 등 나머지 변수들은 독립변수로 지정하였다. 그리고 확장방법을 CRT로 선택하여 의사결정트리 분석을 수행하였다.

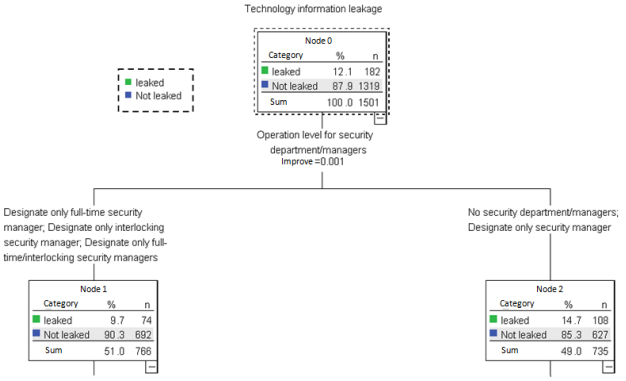
설문은 1,566개로 나타났다. 루트노드가 생성된 결과를 보면 <Figure 4>와 같이 전체 조사대상자 1,501명 중에서 기술정보 유출을 경험한 업체가 182개인 12.1%를 차지하며, 나머지 1,377개인 87.9%는 기술정보 유출을 경험하지 않은 것으로 분석되었다. 다음 <Figure 5>는 “기술정보 유출여부”라는 종속변수에 가장 영향이 큰 독립변수를 찾아낸 첫 번째 분리 결과이다. <Figure 5>에서 볼 수 있듯이 “보안부서/관리자 운영수준 향상”에 대한 p값(유의확률)이 0.001로 매우 작다는 것을 확인할 수 있다. 의사결정트리에서 “보안 관리부서/관리자 운영수준”이 기술정보 유출에 첫 번째로 영향을 많이 주는 변수로 선택되었다. 이 의사결정트리를 CRT 알고리즘으로 규칙을 정하여 성장시키면 전체 트리가 <Figure 6>과 같이 나타난다. 최종 결과트리에서 “보안 관리부서/관리자 운영수준”이 기술정보 유출에 가장 중요한 영향을 미친다는 사실을 알 수 있고, 그 중에서 보안관리부서/관리자 모두 없거나 보안관리자가 지정되었더라도 외부 보안관제 서비스를 가입하지 않고 반출입 통제를 하지 않는 경우에 기술유출이 발생하였다. 하지만 전임 또는 겸직 보안관리자만 지정하거나 겸직 보안관리자만 지정한 경우라도 관련 지침이 없고 체계적으로 관리하지 않거나 지침이 있으나 이행하지 않는 경우와 정기적인 보안감사를 필요시에만 실시하거나 전혀 실시하지 않는 경우에는 기술유출이 발생하였다. 따라서 보안 관리부서와 담당자가 있더라도 관련 지침이 없거나 체계적으로 관리하지 않거나 실천하지 않고, 보안감사를 정기적으로 실시하지 않는 경우에는 기술유출 발생에 안심할 수 없다는 것을 발견할 수 있다.



<Figure 3> Variable Definition in SPSS



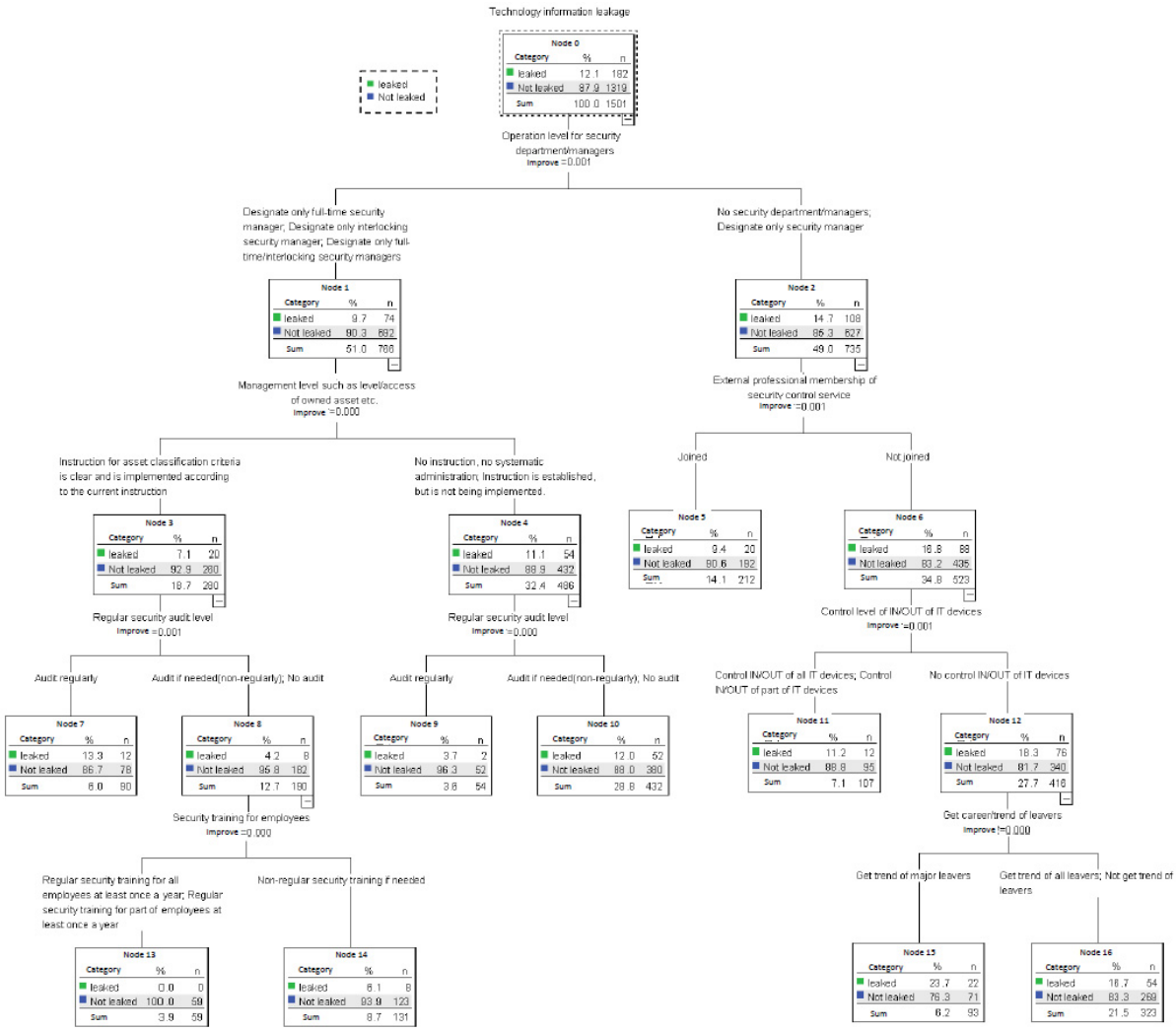
<Figure 4> Result of Decision Tree Analysis 1 in SPSS



<Figure 5> Result of Decision Tree Analysis 2 in SPSS

4. 연구결과

최종 의사결정트리 분석결과 “보안관리부서/관리자 운영수준”이 기술유출에 가장 큰 영향을 미치는 것을 발견할 수 있다. 그 다음 “외부 전문 보안관제서비스 가입여부” 순으로 기술유출에 중요한 영향을 미친다는 사실을 알 수 있었다. 보유자산 분류기준 지침이 명확하고 현재의 지침에 따라 이행하며 전임 또는 겸임 보안관리자를 지정하여 운영하고, 정기적인 보안감사를 실시하는 경우 기술유출 가능성이 낮아지는 것으로 분석되었다. 이와 반대로 보안 관리부서/관리자 모두 없고, 외부 전문 보안관제서비스에 가입하지 않고, 정보화기기 반출입을 통제하지 않으며, 모든 퇴사자의 동향을 파악하거나 전혀 파악하지 않는 경우 기술유출 가능성이 높아지는 것으로 분석되었다.



<Figure 6> Result of Decision Tree Analysis 3 in SPSS

이 같은 분석결과에 대한 원인을 다음과 같이 추측해 볼 수 있다. 첫째, 임직원 및 경영진의 보안의식 부족을 원인으로 들 수 있다. 중소기업 기술보호 역량 및 수준 조사 보고서(2012)에 따르면 기술유출 사고가 발생하는 이유로 '임직원들의 보안의식 부족'(1순위 38.8%, 종합순위 55.6%)이 가장 높게 응답되었다. 또한 중소기업이 기술보호를 위한 보안관리에 가장 큰 애로사항으로 '예산부족'(1순위 44.5%, 종합순위 62.6%), 다음으로 '보안전담 인력부족'(1순위 15.9%, 종합순위 56.2%)과 '기술보호 인프라 부족'(1순위 10.3%, 종합순위 52.4%) 등의 순으로 높게 나타났다[10]. 이는 경영진들이 임직원들의 보안의식 강화나 관련 투자에 여전히 우선순위를 두고 있지 않음을 방증하는 것이다. 둘째, '보안관리/감독체계 미흡'을 들 수 있다. 기술유출 사고가 발생하는 이유로 '보안관리/감독체계 미흡'(1순위 29.7%, 종합순위 62.4%) 이 두 번째로 높게 응답되었다[10]. 특히 '보안관리 부서나 관리자가 모두 없는 경우'가 대기업(10.8%)에 비해 중소기업(41.9%)이 4배 가량 많은 것으로 나타나 중소기업의 보안관리 지침, 반출입 통제, 보안감사 등 보안관리/감독체계와 이의 실천이 매우 미흡한 상황임을 알 수 있다. 셋째, 정보유출 수단의 다변화 때문이다. 최근 정보유출 방법을 보면(조사결과) 단순 복사 및 절취(27.5%), E-Mail(22.5%)에 이어 휴대용 저장장치(20.3%)를 이용한 정보 유출 빈도가 높은 것을 확인할 수 있다[10]. 최근 스마트기기 등 휴대용 정보화 기기의 확산으로 인해 그 빈도는 더 증가할 것으로 예상된다. 또한 외부 전문 보안관제 서비스, 외부 침입에 의한 정보 유출의 경우 적발이 쉽지 않고, 이미 정보가 유출된 이후에 확인되는 경우가 많다. 이처럼 정보유출 수단이 매우 다양해지고 누구나 쉽게 접근이 가능하기 때문에 단순히 내부 교육을 통한 의식제고나 감사활동을 통한 사후 관리만으로는 한계가 있다.

5. 결 론

기술유출에 영향을 미치는 독립변수를 통해 아래와 같이 중소기업 기술보호를 위한 개선방안으로 세 가지를 제시하고자 한다.

첫째, 기술보호 전문가를 양성하고 보안 리더십을 갖게 하는 것이다. 산업기밀 실태조사 보고서(2010)에 따르면 국내 산업보안 전문가가 부족하다는 응답(47.0%)이 충분하다는 응답(8.1%)보다 월등히 높았고, 응답기업의 56.6%가 보안 전문가 양성과 자격증 제도에 찬성하였으며 47.9%가 보안 자격증 소지자의 채용에 긍정적으로 응답하였다.[9] 따라서 기술보호 전문가를 양성하여 담당자로 임명할 뿐만 아니라 기술보호를 위한 예산 수립, 모니터링, 감사활동 및 감사결과 제재를 가할 수 있는 수준의 적절한 권한을 부여하여 실질적인 관리활동이 가능하도록 해야 한다. 단순히 보여주기식의 담당자 임명은 임직원들로 하여금 오히려 책임감을 경감시켜 역효과가 날 수 있음을 주의해야 한다. 둘째, 기술보호를 위한 법적 제도적 개선을 하는 것이다. 기술유출 방지를 위해 중소기업이 필요로 하는 정책으로 '기술보호를 위한 법적 제도적 조치 강화'(57.7%)를 가장 많은 기업이 선택한 것으로 나타났다[10]. 보안관리/감독체계 수립을 위한 관리지침을 제도화 하고 보안관리 지침, 반출입 통제, 보안감사 등 보안관리/감독체계 운영수준에 따라 인센티브나 Penalty를 부과하는 체제를 수립하는 것이다. 셋째, 물리적인 보안환경 개선을 위한 예산을 확대하고 지원방식을 개선하는 것이다. 중소기업에 지원한 기술개발 예산 규모는 2011년 6,288억 원, 2012년 7,150억 원, 2013년 7,837억 원 수준으로 매년 증가추세에 있다[8]. 그러나 기술보호를 위한 지원은 2013년 55억 원으로 기술개발 예산의 0.7% 수준에 불과하다. 연구개발 지원금액 대비 기술유출방지를 위한 예산 규모는 미약한 것을 알 수 있다. 문서 보안관리를 위한 DRM, 모바일을 통한 기술유출 방지를 위한 MDM, 외부 침입 방지를 위한 방화벽과 IDS(침입탐지시스템), 사용자의 작업공간을 별도로 분리하는 클라우드 환경 등에 집중해야 한다. 또한 이같은 솔루션을 기업들이 알아서 도입하고 투자비를 지원하는 형태는 바람직하지 못하다. 현재 각 시스템별 벤더가 각기 달라 일부 시스템을 구축했다 하더라도 결국 전체 환경 통합시 막대한 비용을 부담해야 하는 것이 현실이다. 따라서 정부차원의 패지지화된 솔루션을 개발하여 배포하는 등 예산 지원방식을 다변화할 필요가 있다.

6. 논의 및 시사점

기존 2012년 실시된 중소기업 기술보호 역량 및 수준조사에서는 중소기업 및 대기업을 대상으로 기술유출 실태를 파악하고, 기술보호 역량 수준을 진단하기 위해 조사가 실시되었으며, 현재 중소기업의 경우 대기업에 비해 전 영역에서 보안역량이 취약함에도 불구하고 보안성 강화를 위해 투자가 어려운 중소기업에 대한 정부의 지원활동이 보다 강화될 필요가 있음을 확인했다. 본 연구에서는 기술유출을 경험한 중소기업들을 의사결정기법을 통해 살펴본 결과 여러 요인들 중 "보안관리부서/관리자 운영수준"이 기술유출에 가장 큰 영향을 미치는 것을 발견할 수 있었다. 이것은 대기업에 비해 기술보호 역량, 자금과 인력이 모두 부족한 중소기업에서 현실적으로 어떤 부분에 우선적으로 역량을 집중해야 하는지 제시했다는 점에서 의미가 있다.

본 연구는 다음과 같은 한계를 지니고 있으므로 연구결과를 해석하는데 주의를 기울일 필요가 있다. 첫째, 납품 중심의 수급 기업인 경우 대기업에 종속되어 있는 수직적인 분업체계가 고착되어 있는 현실을 감안할 때[17], 실제 국내 중소기업에서의 기술유출 건수 및 피해의 심각성은 본 논문에서 언급한 내부 관계자에 의한 유출보다는 거래 관계에 있는 대기업에 의한 기술 유출의 비중이 더 클 수 있다. 그러나 본 논문에서 활용한 <2012년 중소기업 기술보호 역량 및 수준조사> 설문에서는 내부의 기술유출 방지에 초점이 맞추어져 있다. 따라서 향후 연구에서는 기술 유출 사실을 직/간접적으로 인지한 상태에서 외부 관계자에 의한 기술유출 실태 및 개선방안에 관한 연구가 필요하다. 둘째, 데이터마이닝 기법 중 의사결정트리 기법만을 활용하여 데이터를 분석하였다. 향후 연구에서는 수집된 데이터 특성에 맞는 추가적인 통계분석을 실시하여 분석결과의 신뢰도를 검증한다면 보다 의미 있는 해석이 가능할 것이다. 셋째, 현재 기업의 기술보호를 위한 관리적 대응방안, 제도 정책적 개선방안, 시스템 구축방안에 대한 연구는 활발히 진행되고 있지만 아직까지 기술보호 평가모델에 관한 연구는 부족한 실정이다. 따라서 향후 연구에서는 기술보호 관리체계 및 기술보호 평가모델을 수립한다면 기업에서 자체 진단을 통해 어떤 부분에 역량을 집중해야 하며 필요한 조치는 무엇인지 식별하는데 유용하게 사용될 수 있을 것이다.

References

[1] Chae, J.W. and Ko, Y.H., Exploring Case Study on Security Factors and Strategy to Prevent Leakage of Corporate Information for CEO : Focused on Korea Manufacturing Company Major Cases in 2010. *Korean journal of CEO and Management Studies*, 2012, Vol. 15, No. 1, p 87-113.

[2] Chang, H.B., The Design of Information Security Management System for SMEs Industry Technique Leakage Prevention. *Journal of Korea Multimedia Society*, 2010, Vol. 13, No. 1, p 111-121.

[3] Huh, S.P., Lee, D.S., and Kim, K.N., A Study on The Leak of Core Business Technologies Using Preventative Security Methods Such as Clustering. *Korean Journal of convergence security*, 2010, Vol. 10, No. 3, p 23-28.

[4] Institute For International Trade, *Trade Focus-Strategies of SMEs and exports decline*, 2010, Vol. 9, No. 61, p 9-11.

[5] Jeong, J.H. and Roh, J.H., The Research of Implementing Scientific Security System to Prevent Technology Leakages : Focusing on the Role and Function of Technical Security. *Korean Journal of Scientific Criminal Investigation*, 2011, Vol. 5, No. 3, p 288-301.

[6] Jeong, T.H. and Chang, H.B., A Study on the Real Condition and the Improvement Directions for the Protection of Industrial Technology. *Korean security science review*, 2010, No. 24, p 147-113.

[7] Kim, M.S., Design of Information Leakage Protection System for Small and Medium-sized Enterprise, Chonnam University master's dissertation, 2014.

[8] Korea Institute of S&T Evaluation and Planning, Government Research and Development Budget Analysis in the FY 2013.

[9] Korea Technology and Information Promotion Agency for SMEs; TIPA, *A Report on the Current Status of Management of Industrial Confidential Information*, 2010.

[10] Korea Technology and Information Promotion Agency for SMEs; TIPA, *Technology Protection Capability and Survey on the Level of Small and Medium Business*, 2013.

[11] Lim, C.M., Research of Policy Instruments to Prevent Technology Leakages. *Korean Journal of Scientific Criminal Investigation*, 2012, Vol. 6, No. 1, p 1-9.

[12] Na, J.G., A Study on a Legal System for the Protection of Exportation of High-technology in Cross-border M&A : with emphasis on an Analysis of M&A cases. *Korean Journal of Business Administration and Law*, 2009, Vol. 19, No. 2, p 75-116.

[13] 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 Review*, 2012, Vol. 46, p 45-75.

[14] National Industrial Security Center; NISC, http://service4.nis.go.kr.

[15] Noh, M.S. and Lee, S.Y., Explaining Industrial Security of SMEs in Korea : An Ordered Logit Analysis. *Korean Public Administration Review*, 2010, Vol. 44, No. 3, p 239-259.

[16] Shin, K.S., A Study on the Development Direction of Industrial Technology Security Systems in Korea, Kyungnam University doctoral dissertation, 2011.

[17] Woo, J.P. and Kwang, H.P., An Empirical Study on the Influence of Collaborative Performance of Large Corporations and SMEs Value Chain Competence in SMEs, *Society of Korea Industrial and Systems Engineering*, 2012, Vol. 35, No. 3, p 16-23.

[18] Yoon, I.S., (A) Study on Construction of Security System for Prevent of Information Extraction by an Insider, Kangwon University master's dissertation, 2007.