중소기업에 대한 ISMS 인증효과와 영향요인에 관한 연구

김인관*, 박재민**, 전중양***

An Study on the Effects of ISMS Certification and the Performance of Small and Medium Enterprises

In Kwan Kim*, Jaemin Park, Joong Yang Jeon*****

요 약 본 논문은 산업기술 보호와 관련된 국제표준의 역할에 주목하여 중소기업에 대한 ISMS의 효과와 성과에 미치는 영향요인을 분석한 것이다. 특히 인증의 효과 및 성과에 관한 설문조사를 통해 경영성과 및 운영성과를 측정하고, 요인분석을 통해 도출된 성과변수에 대하여 분산분석과 회귀분석을 통하여 ISMS 인증효과에 영향을 미치는 주요 요인을 도출하였다. 요인분석과 집단이분산성을 고려한 회귀분석 결과, 업종과 기업 규모에 따른 영향은 확인되지 않았으나 보안조직 여부, 정보보안투자 그리고 경영진과 종업원의 보안의식 수준이 ISMS 인증효과에 유의한 영향을 미치는 것으로 나타났다. 이를 통해 산업기술유출을 방지하기 위해서는 인증과 병행해 보안 역량과 투자가 병행되어야 하고, 업종 혹은 산업의 구분이 크지 않은 만큼 산업기술 보호를 위한 인프라 혹은 시스템으로서 인증의 중요성을 확인할 수 있었다고 하겠다.

주제어 : 산업기술, 기술보안, ISMS, 인증효과, 보안의식

Abstract This paper focuses on the role of international standards related to industrial technology and to analyze determinants to affect ISMS and its performance. Particularly its financial and operational performance were measured by survey aiming at an influence of certification and its performances. The variables explaining the performance were drawn out from factor analysis and then critical variables to affect performance were discovered by ANOVA and regression analysis. As a result of the analysis considering heteroscedastic and factor analysis, type of business and firm size were not significantly related to the performance but the existence of information security unit, investment in information security and the status of security consciousness in executives and employees were positively related. As a result, this study shows that security certification should be implemented with suitable capabilities and the investments to protect from leaking industrial technology and proved the importance of the security certification as an infrastructures and system.

Key Words : Industrial Technology, Technology Security, ISMS, Certification Effect, Security Consciousness

1. 문제의 제기

우리나라의 연구개발 투자비율은 2010년 국내총생산 대비 3.74%로 경제협력개발기구(OECD) 가입국 가운데 이스라엘(4.25%), 핀란드(3.84%)에 이어 세 번째로 높은 수준이다[27]. 우리나라는 짧은 산업화 기간 동안 선진국의 기술을 도입하여 빠른 시간 내에 기술을 습득하였고, 이 과정에서 축적된 학습능력을 바탕으로 ICT를 활용한 여러 분야에서 세계적으로 우수한 기술력을 보유하게 되었다[28]. 또 1980년대 이후 정부 차원에서 연구개발에 대한 투자를 지속적으로 증가시켜 왔고, 2000년대 들어서도 정부의 지속적인 R&D 투자 노력으로 2010년에 이

※ 본 논문의 초고는 '2011 한국기술혁신학회 춘계학술대회(11.6.17)'에서 발표된 바 있다.
*지식경제부 에너지안전팀장
**건국대학교 경영대학 기술경영학과 교수(교신저자)
***건국대학교 경영대학 기술경영학과 박사과정
논문접수: 2012년 12월 2일, 1차 수정을 거쳐, 심사완료: 2013년 1월 15일

르러 연구개발 투자액 40조원을 돌파한 바 있다[4]. 특히 우리나라는 과거 추격형 모델에서 이제는 일부 기술 분야에서 오히려 추격의 대상이 되었고, 전반적으로 탈추격형에 기반한 선도형 기술혁신모형으로 전환하고자 노력하고 있다[9].

한편으로 보면 1950년대에 이미 Solow[29][30]가 예상한 바와 같이 선진국 경제성장의 50~70%가 총요소생산성의 증대에 의해 이루어지고 있고, 우리나라의 경우에도 노동과 자본에 의한 성장의 한계를 기술발전에 의해 극복할 수밖에 없는 상황이다[23]. 이 같이 과거의 개발도상국들이 속속 기술경쟁에 뛰어들면서 세계시장에서의 경쟁은 확대·심화되고 있다. 또 기술혁신이 가속화되면서 신기술 및 신제품의 생존주기도 단축되고 있다. 이 같은 경향은 경쟁자 보다 앞서 신제품을 주요 시장에 출시해야 할 필요성을 높이는데, 결과적으로 이것은 냉전체제 붕괴 이후 불붙기 시작한 산업정보의 수집을 더욱 격화시키게 되었다. 이에 따라 미국을 비롯한 주요 선진국은 자국으로부터의 기술유출 사례가 점차 증가함에 따라 경제스파이법 등을 제정·시행하는 등 자국의 기술을 보호하기 위한 강력한 조치를 취하게 되었다[8].

우리나라의 경우 1990년대에 이미 상당한 첨단 기술력을 보유하고 있었지만 한편으로 해외기술의 수집과 활용에 의존했던 탓에 기술보호에 대해서는 소극적으로 대응해 왔고, 중소기업의 기밀·기술유출방지를 위한 체계적인 시스템 역시 미흡한 실정이었다[6].

그러나 1998년 1월 삼성전자의 반도체 기술유출사건을 계기로 산업기술보호의 필요성이 제기되면서 그해 12월 「부정경쟁방지 및 영업비밀보호에 관한 법률」이 제정되었다. 이어 2007년에는 핵심기술의 적극적인 보호를 위해 「산업기술보호의 유출방지 및 보호에 관한 법률」이 제정된 바 있다. 하지만 인적·물적 자원이 풍부한 일부 대기업을 제외한 대부분의 중소기업은 경영진의 보안의지와 기술보호에 대한 지식과 경험이 부족하고, 기술유출방지를 전담할 조직이 없어 법률 제정만으로 기술자산에 대한 효과적인 보호를 기대하기 어려운 실정이다[6]. 따라서 산업기술의 유출 방지를 위해서는 지재권 등 제도적인 보호수단과 더불어 기술에 관한 국가적인 통합보안관리시스템의 구축이 필요해진다. 다시 말해, 지금과 같이 기업과 기업, 산업과 산업이 서로 네트워크로 연결되어 있는 경우 1~2개 주요 기업의 정보보호 만으로는 기업과 산업의 보안을 유지할 수 없다는 것이다. 이로 인해 비록 지재권의 보호를 위한 정부 주도의 제도 개선이 지속적으로 추진되고 있다고 하더라도 이것만으로는 전체적이고 포괄적인 기술보호가 될 수 없다. 즉 산업기술의 보호는 이들 어느 하나만으로 가능하지 않고, 제도적 측면과 시스템 측면이 동시에 이행되어야 가능하다는 것이다.

본 연구는 이 같은 문제의식을 바탕으로 산업기술 보호와 관련하여 법률적인 접근보다는 통합기술보안체제의 기능을 하는 국제표준에 대해 그 효과적 활용방안에 대해 접근하고자 하였다. 특히 산업기술 보호와 관련된 대표적 국제표준인 ISO/IEC 27001[1]을 토대로 수립된 ISMS(Information Security Management System)를 중소기업에 적용할 경우 그 효과성과 활용 정도에 영향을 미치는 요인을 분석함으로써 효과적인 기술보안체계 구축 및 운영을 위한 함의를 도출하고자 하였다. 명확한 실증분석을 위해 본 연구는 상기 국제표준의 인증을 받은 중소기업만을 대상으로 하였고, 국제표준 적용에 따른 중소기업의 성과는 한국인정원이 2010년도에 실시한 실태조사를 바탕으로 하였다.

2. 선행연구

2.1 관련 개념 및 정의

「산업기술혁신촉진법」에 따르면 "산업기술"이란 「산업발전법」 제2조에 따른 산업, 「광업법」 제3조 제2호에 따른 광업, 「에너지법」 제2조 제1호에 따른 에너지와 관련한 산업, 「신에너지 및 재생에너지 개발·이용·보급 촉진법」 제2조 제1호에 따른 신·재생에너지와 관련한 산업 및 「정보통신산업 진흥법」 제2조 제2호에 따른 정보통신산업의 발전에 관련된 기술로 정의하고 있다. 「산업기술유출방지 및 보호에 관한 법률」은 "산업기술"을 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 소관 분야의 산업경쟁력 제고 등을 위하여 법령이 규정한 바에 따라 지정 또는 고시·공고하는 기술로 ① 국내에서 개발된 독창적인 기술로서 선진국 수

1) ISO27001은 영국의 상무성 주관으로 정보보안관리실무규범(A Code of Practice for Information Security Management)이라는 주제로 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 하였으며, ISMS는 ISO2001을 바탕으로 국내 실정에 맞도록 구성된 인증체계로 사용되고 있다[10].

준과 동등 또는 우수하고 산업화가 가능한 기술, ② 기존 제품의 원가절감이나 성능 또는 품질을 현저하게 개선시킬 수 있는 기술, ③ 기술적·경제적 파급효과가 커서 국가기술력 향상과 대외경쟁력 강화에 이바지할 수 있는 기술, ④ 이들의 산업기술을 응용 또는 활용하는 기술로 정의되며, 법으로 정한 산업기술은 일반적인 산업기술이 아닌 법으로 보호해야 하는 대상을 명백히 규정한 것이다.

이와 관련해 기술유출은 해당국가의 특허전략이나 지적재산권 보호 전략과 밀접한 관계를 갖는데, 해당 국가에서 기술유출을 어떻게 규정하고, 국가 정책적으로 보호해야할 기술을 어떻게 하는가에 따라 정의될 수 있다. 중소기업청의 "기술유출 대응 매뉴얼"에 따르면, 기술유출은 기업의 입장에서 중요자산으로 보호하고 있는 기술상의 정보와 노하우에 대한 유출 및 침해행위를 말하고 6가지로 분류하고 있다(<표 1> 참조).

〈표 1〉 기술유출의 분류 및 내용

구분	내 용
1	절취·기망·협박, 그 밖의 부정한 방법으로 기술정보를 취득하는 행위 또는 그 취득한 기술정보를 사용하거나 공개하는 행위
2	규정 또는 계약에 따라 기술정보에 대한 비밀유지의무가 있는 자가 기 기술정보 등을 절취·기망·협박 그 외의 부정한 방법으로 유출하는 행위 또는 그 유출한 기술정보를 사용하거나 공개하거나 제3자가 사용하게 하는 행위
3	위의 1, 2의 규정에 해당하는 행위가 개입된 사실을 알고 그 기술정보를 취득·사용 및 공개하거나 기술정보를 취득한 후에 위 1, 2의 규정에 해당하는 행위가 개입된 사실을 알고 사용하거나 공개하는 행위
4	위의 1, 2의 규정에 해당하는 사실을 중대한 과실로 알지 못하고 기술정보를 취득·사용 및 공개하거나 기술정보 등을 취득한 후 1, 2의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 기술정보를 사용하거나 공개하는 행위
5	지식경제부 장관의 승인을 얻지 아니하거나 부정한 방법으로 국가핵심기술의 수출을 추진하는 행위
6	국가핵심 기술의 수출중지, 수출금지, 원상회복 등의 조치에 대한 지식경제부 장관의 명령을 이행하지 아니한 경우

자료 : 중소기업청[17]

좀 더 엄밀하게는 산업기술의 유출 대상은 특허로 보호를 받는 기술이 아닌 영업비밀이나 기술개발과정의 기술이라고 볼 수 있다. 즉, 특허를 받은 기술은 정보공개를 바탕으로 독점권을 부여 받고 있지만 영업비밀은 경제적 가치가 있는 정보에 대한 비공개와 비밀관리를 전제로 법적인 보호를 받기 때문에 정보자산에 대한 유출방지의 대상이 되는 것이다.[2)]

〈표 2〉 특허제도와 영업비밀보호제도 비교

구분	특허제도	영업비밀
보호 대상	기술적 발명	경제적 가치를 지닌 경영상·기술상 모든 정보
보호 요건	신규성·진보성·산업적 이용가능성	비공지성·비밀관리성 경제적 유용성
보호 기간	출원일후 20년간	비밀로 관리되는 기간
공개 여부	공개	비공개
이전 여부	실시권(통상, 전용) 부여	이전 불가

자료 : 노민선·이삼열[7]

또한 산업보안과 정보보안은 실무적으로는 혼용해서 사용하지만[3)] 엄밀한 의미에서는 상당히 다른 개념이라는 점에서 보다 엄밀한 분석을 위해서는 구분되어야 할 필요성이 있다. 예를 들어, 국가정보대학원[1]은 산업보안을 "첨단기술 뿐만 아니라 산업활동에 유용한 기술상·경영상의 정보나 인원, 문서, 시설, 통신 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호·관리하기 위한 대응방안이나 활동"을 의미하는 것으로 정의하고 있다. 또 최선태·유형창[19]은 산업자산에 대한 보안, 즉 산업 활동을 하는 모든 구성원, 시설물과 같은 유형자산과 정보를 포함한 무형자산 그리고 서비스와 프로세스에 대한 보호와 안전성을 유지하는 모든 활동, 또는 산업자산의 안정성을 제고하는 제반 활동을 산업보안이라고 정의하였고, 노민선·이삼열[7]은 산업체에서 직접보유하거나 산업활동과 관련된 물리적 자산, 인적자산, 기

2) 중소기업청의 "기술유출 대응 매뉴얼"에서 기술유출은 국가, 기업, 기술개발자 등 각 이해관계자의 시각에 따라 기술거래, 기술협력 혹은 직업선택의 자유 등과 그 개념이 혼동되고 있다고 하였다.

3) 비록 산업보안과 정보보안은 그 의미와 정의에서 차이가 있지만, 그 대상에 있어서는 서로 상이하거나 사전적으로 구분되는 것은 아니라는 점에서 실무적으로는 혼용될 수 있겠다.

술상・경영상의 정보를 중요도에 따라 각종 위해요소로부터 보호하는 모든 활동이라고 정의한 바 있다.

반면 정보보안은 관찰이나 측정을 통해 수집된 자료를 실제 문제에 도움이 될 수 있도록 분석하여 정리된 지식을 안전하게 지키는 활동이라고 정의된다[26]. 또 NIST는 정보시스템 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability)을 유지하기 위하여 정보시스템에 취해진 보호조치라고 정의하였고, 미연방정보보안관리법은 “정보의 무결성, 비밀성, 가용성을 유지하기 위해 권한 없는 접속・이용・공개・방해・변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것”이라고 정의하고 있다. 교육과학기술부는 “정보통신 수단으로 수집・가공・저장・검색・송수신되는 정보의 유출・위변조・훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적・물리적・기술적 수단을 강구하는 일체의 행위”라고 말한다. 단 한국법제연구원[21]은 정보보안에서 개인정보 보호와 영업비밀 보호와 같은 정보의 내용에 대한 보호는 제외하고 있다.

2.2 관련 선행연구

국내에서 산업기술 보호와 국제표준에 관한 연구는 대단히 드문 편이다. 특히 국제표준의 적용 효과 및 활용성과에 미치는 영향을 분석하고, 그 결과를 바탕으로 기술보안체계 구축을 위한 함의를 찾는 연구는 전무하다고 해도 과언이 아니다. 하지만 기술유출의 문제점과 대안을 모색하는 연구는 최근 들어 몇 차례 발표된 바 있다. 이들 선행연구들은 대개 세 가지 주제로 구분해 볼 수 있는데, 첫 번째는 기술유출의 원인 혹은 보안시스템의 문제점을 파악하고 그 해결책을 모색하는 것이고, 두 번째는 기술유출의 경제적 영향을 가늠하는데, 세 번째는 기업의 정보보호에 관한 태도가 어떻게 결정되는지에 관한 것이다.

이들 중 첫 번째 주제에 해당하는 대표적인 연구가 정병일[15]과 장항배[12] 등이라면, 마지막에 해당하는 연구로 노민선·이삼열[7] 그리고 기술유출의 경제적 영향에 관한 것으로 전재완[14]을 들 수 있다. 이들 중 전자에 해당하는 정병일[15]은 기술유출을 환경과 제도적 관점에서 접근했는데, 이 연구는 기술유출이란 대체로 기술을 이전하는 과정에서 발생하고, 기술이전대상과 기술이전의 방식, 시기적・지역적 제한에 따라 기술유출의 불법여부가 판단된다고 보고 있다. 또 기술유출은 사후구제수단보다는 사전예방이 최선책이라고 할 수 있고 이를 위한 제도적인 장치의 구비가 바람직하다고 한다. 더불어 기술의 개발과 산업보안을 분리하여 취급할 것이 아니라 기술개발의 필수요소로서 산업보안을 포함시켜 운영하고 개발자의 이익을 보장하여 지속적인 기술개발이 이루어지도록 하는 제도장치 마련이 시급한 것으로 보았는데, 비교적 기술유출에 관한 제반 문제점을 폭넓게 다루었다는 점에서 의의가 있다. 이에 앞서 장항배[12]는 국내 주요기업에서 사용하고 있는 문서보안 시스템을 대상으로 전문가 집단을 통한 델파이 방법론을 활용하여 보안수준을 평가한 바 있다. 그 결과는 모든 평가영역에서 평균 이상의 보안성을 나타내지 못하였으며, 특히 정보 중요성 관점의 평가항목들을 충족하지 못한 것으로 평가하였다. 또 기존의 외부침입방어 관점의 보안성 평가와 달리 산업기술 유출방지 관점(내부적으로 안전한 정보유통, 정보반출시 책임성 있는 정보추적)의 새로운 보안시스템 평가모형과 측정방법을 제시하고 이에 대한 적합성을 논의하였다. 뒤이은 장항배・송지훈[13]은 1990년대 이후 컴퓨터의 비약적인 발전으로 모든 작업이 컴퓨터에 의존하고 있고, 이로 인해 외부침입자가 아닌 내부자에 의한 기술유출 사고가 빈번하게 발생하고 있다고 본다. 이와 관련해 산업기술유출방지 시스템이 개발되었으나 외부침입 방어목적의 보안시스템을 평가하기 위한 기존의 정보보호 3요소(기밀성, 무결성, 가용성) 관점의 평가로는 한계성에 직면하게 되었다고 보았다. 이 같은 분석으로부터 산업기술 정보에 대한 접근권한을 보유한 내부직원들에 대한 새로운 보안시스템평가모형과 측정방법이 필요하다고 하였다. 이 같은 논의와 관련해 김성원[3]은 국가 R&D 수행과정 및 기술성과물의 보호관리에 관한 중요성이 매우 중요해졌으며, 국가 R&D와 관련된 각종 보안관리규정 체계가 연구수행기관의 입장에서 명확하게 이해되어 운영될 수 있도록 구체화되고, 현실성과 관리효과성이 있는 기술보안관리 시스템의 정비가 필요하다고 보았다. 개방형 혁신 환경 속에서 핵심기술을 어떻게 보호하고 외부로 신성장 동력기술을 어떻게 제대로 확보할 것인가를 법제도적 관점에서 검토했던, 최치호[20]는 기술보호를 위한 기술보호를 위한 구체적 방안을 연구협의 단계, 연구수행 단계, 기술확보 단계 등으로 구분해 제시하고, 이 문제점을 해소하기 위한 입법조치를 제안하였다는 점에서 의미 있는 연구로 판단된다.

전술한 두 번째 주제의 연구로서 전재완[14]은 기업이

개발한 기술은 그 기업만의 피해로 끝나는 경우가 매우 적다고 전제하였는데, 이는 한 기업의 기술유출이 시장에서 다른 경쟁기업이나 국가 경제적 차원에서 매우 심각한 영향을 미치기 때문이라고 보았다. 또 기술에 대한 피해를 추정하기 위해서는 관련 산업들에 미치는 영향력을 고려할 수 있는 산업연관분석과 같이 전 산업 및 국가적 규모의 피해를 측정할 수 있는 기법의 적용이 필요하다고 보았다.

이들 연구와는 다소 다른 관점에서 노민선·이삼열[7]은 중소기업의 산업보안에 미치는 영향요인을 분석하였는데, 실증분석 결과는 기업규모와 특허출원 실적이 중소기업의 산업보안 역량 수준에 통계적으로 유의미한 것으로 나타났으나 업종, 기술유출경험, 기술수출실적, 국가연구개발사업 참여 여부 등은 통계적으로 유의미한 관계를 보이지 않는 것으로 분석하고 있다. 또 이 분석 결과를 바탕으로 정부차원에서 중소기업 지원범위의 구체화, 기술유출 경험이 있는 중소기업에 대한 컨설팅 강화, 혁신형 중소기업 인증시 보안관리 항목을 평가지표에 반영, 기술을 해외로 이전하거나 해외로 진출하고자 하는 중소기업에 대한 보안정책 강화, 국가연구개발사업 참여기업에 대한 보안교육 강화, CEO의 인식제고를 위한 지원확대 등을 제안한 바 있다.

3. 분석자료 및 분석모형

3.1 분석자료

본 연구의 분석이 기초하는 자료는 「ISMS : Information Security Management System(정보보안경영시스템) 국제표준 도입 및 인증의 효과성에 대한 실태조사」라는 제목으로 ISO/IEC 27001[4] 인증기관으로부터 동 국제표준에 의해 인증을 획득한 기업과 정보보안과 관련된 학계, 산업계, 인증심사원 및 컨설턴트를 대상으로 실시된 조사의 결과이다.

설문내용은 인증기업 및 전문가에 대해 별도로 작성되었으며, 설문대상별 편차를 확인하기 위하여 일부 동일한 내용이 각각의 설문에 포함되어 있다. 이중 인증기업에 대한 설문항목은 7개 분야 174항목으로 구성되어 있는데, ISMS 인증의 효과 및 성과에 대해서는 먼저 경영성과 측면과 운영적 측면으로 구분하고 이들 각각에 대해 8개와 19개의 설문문항으로 조사하고 있다. 이들은 5점의 리커트척도(Likeret Scales)를 사용하였고, 응답자는 “귀사의 상황과 일치된다고 생각되는 내용을 [V] 해주시기 바랍니다”는 물음에 대해 각 항목별로 ① 전혀 효과가 없다, ② 효과적이지 않다, ③ 보통이다, ④ 효과적이다, 또는 ⑤ 매우 효과적이다로 답하도록 하였다. <표 3>은 ISMS 인증의 효과 및 성과에 관한 설문항목을 소개하고 있다.

〈표 3〉 ISMS 인증의 효과 및 성과 관련 설문문항

구분	설문문항
경영성과 측면	법규준수에 효과적
	고객 및 이해관계자의 신뢰 증가
	매출액 증가
	보안투자의 효율성 증가
	시장 점유율 및 시장경쟁력 강화
	전반적으로 보안투자 비용 감소
	정보 유출 등 보안사고 감소
운영성과 측면	보안사고 예방에 효과적
	보안업무의 체계적 관리에 효과적
	직원들의 보안에 대한 인식 제고 및 기업 내 보안 문화 형성
	보안업무의 규정화로 보안 준수 방법 명확화
	일회적이 아닌 지속적인 보안관리에 효과적
	고객과의 의사소통 채널 및 피드백 관리구조 개선
	프로세스 접근방식의 운영으로 계획 및 목표 달성이 원활
	시스템적 운영방식이 활성화되어 운영에 대한 효과성 및 효율성 향상
	정량화된 성과 측정을 통해 시스템 개선을 위한 정보수집 및 분석 능력 향상
	데이터에 근거한 의사결정을 통해 기업 운영 및 성과에 대한 결과가 예측 가능
	인적자원관리(인원보안)에 효과적
	보안업무에 대한 책임과 권한이 명확해짐
	보안업무를 위해 부서간 연계 협력체계가 수립됨
	물적자원관리(물리적 보안)에 효과적
	IT 등의 관리(기술적 보안)에 효과적
	협력업체(외주업체) 관리에 효과적
	보안업무에 대한 일관된 방침 및 목표 관리 능력 향상
	경영진의 보안에 대한 관심과 인식의 증가

4) 산업기술보호와 관련된 대표적인 표준이라고 할 수 있는 ISO/IEC 27001은 1995년 영국에서 수립되었다. 기업에서 수년간 보안업무를 수행한 전문가들이 모여 정보보호에 꼭 필요하고, 그 효과성이 있다고 판단되는 대응책(안전대책)들을 모아 "Code of practice for information security management"를 작성해 영국표준(BS 7799: British Standard 7799)으로 정한 것에서부터 시작되었다. 현재 ISO/IEC family 표준문서는 모두 15개로 구성되어 있고, 이들 표준 문서 중 일부는 이미 국제표준으로 확정되었으나 일부는 아직도 개발 중에 있으며 향후에도 점점 늘어날 것으로 예상되고 있다[5]. 이에 대한 자세한 내용은 ISO/IEC(2009)에서 찾을 수 있다.

이 조사는 ISO/IEC 27001 인증을 획득한 119개 국내 기업 및 기관(이하 “기업”, “조직” 또는 “인증기업”) 전체를 설문대상으로 하였으며 55개 기업이 응답하였고, 회수율은 46.2%를 나타냈다(<표 4> 참조). 이 중 제조업은 22개(40%)였으며, 비제조업은 33개(60%)로 구성되었다. 또한 전체적으로 ISO/IEC 27001 인증기업은 중견기업 이상의 규모가 많은 것으로 나타났으며, 응답기업의 경우도 500인 이상의 사업장이 52.7%로 과반수를 넘는 것으로 나타났다. 500인 이상 다음으로는 100인 미만(21.8%), 100~300인(16.4%), 300~500인(5.5%)의 순이었다.

〈표 4〉 응답기업의 일반현황

	구분	기업 수	비율 (%)		구분	기업 수	비율 (%)
업종	전체	55사	100.0	기업규모	전체	55	100.0
	제조업	22사	40.0		100인 미만	12	21.8
					100~500인	12	21.9
	비 제조업	33사	60.0		500인 이상	29	52.7
					무응답	2	3.6

본 연구에서 채택한 독립변수인 보안전담조직 보유여부는 보유와 미보유로, 경영진과 종업원의 보안의식 수준은 각각 높음, 보통, 낮음으로, 정보보안에 대한 투자수준 역시 높음, 보통, 낮음으로 응답하도록 하였다.

3.2 가설설정

정보보호를 위한 대부분의 선행연구는 우리나라의 산업기술보호를 위한 제도가 정착된 기간이 짧아 주로 산업기술보호, 정보보호를 위한 법적, 제도적 문제점이나 지원 등을 주로 다루었다. 반면 전술한 바와 같이 정보보호 제도나 그 영향요인을 분석한 선행연구는 거의 없다. 본 연구는 정보보호를 위해 국제적 표준으로 활용되고 있는 ISO/IEC27000과 관련해 ISMS 인증기업을 대상으로 이들 기업의 ISMS 인증효과에 대한 영향요인이 무엇이었는지 파악하는데 목적이 있다. 특히 ISMS의 활용 효율성과 그 성과의 영향요인을 도출하기 위해 다음과 같은 가설을 설정하였다.

가설 1: 제조업과 비제조업에 따라 ISMS 인증의 효과는 차이가 있을 것이다.

「부정경쟁방지 및 영업비밀 보호에 관한 법률」은 “영업비밀이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다”고 정의한 바 있다. 이처럼 보호해야 하는 기밀이란 기업의 기술상 및 경영상의 정보 등도 포함해야 하고, 국내에서 ISMS 인증을 받은 기업수도 비제조업이 많은 현실에서 볼 때 ISMS 도입이 제조업과 비제조업 중 어디에 더 큰 효과를 가져 올 것인가를 보는 것은 정책적 함의가 크다고 보았다.[5)]

가설 2: 기업규모가 큰 기업이 ISMS 인증의 효과가 클 것이다.

전술한 바와 같이 국내 ISMS 인증기업은 제조업 보다 비제조업이 많다. 하지만, 기업 규모에 있어서는 500인 이상의 대기업 뿐 아니라 100인 미만의 중소기업도 상당하다. 노민선・이삼열[7]에 따르면 기업 규모가 커짐에 따라 산업보안 역량 수준도 높은 것으로 나타났다. 이 같은 설문조사의 결과, 즉 ISMS 인증에 의한 효과가 기업의 규모에 따라 차이가 있는 지 실증적인 분석을 통해 확인하고자 한다.

가설 3: 보안조직이 있는 기업에서 ISMS 인증의 효과가 있거나 더 클 것이다.

국내 중소기업은 대부분 인력, 예산 등의 제약으로 보안 관련 업무는 총무팀 등 관리부서에서 부수적인 업무로 수행하고 있다. 하지만 고숙련인력의 유동성이 증가하고, 업무활동의 상당부분을 IT기기에 의존하는 등 대내외적으로 내부기밀 유출의 가능성이 높아짐에 따라 직원의 보안의식 제고를 전담하는 보안조직이 대기업 뿐 아니라 중소기업에서도 속속 설치되고 있다. 이 같은 보안조직이 ISMS 인증의 효과에 어느 정도나 기여하는 지를 확인해 보고자 하였다.

가설 4: 경영진의 보안의식 수준이 높은 경우 ISMS 인증의 효과가 있다.

5) 지식경제부가 조사한 2007년 기준 우리나라 주요 업종의 기업규모별 현황을 보면 제조업은 10.4%, 서비스업종은 86.4%, 지식서비스산업은 14.7%이다[18].

우리는 그 동안 기술개발에 있어 추격형 모형에 머물러 있었다고 볼 수 있다[9]. 그리고 나름의 노하우나 보호해야 할 가치 있는 암묵적 지식은 많지 않았다. 이로 인해 우리 정부와 기업은 산업기술의 유출에 대해서 관심이 적었으며, 모든 것은 지적재산권으로 보호될 수 있다는 인식이 많았다[6]. 따라서 경영진의 관심도가 기술보호에 있어 중요한 요인이며, ISMS 인증의 효과에도 영향을 미친다고 하겠다. 즉 경영진의 보안의식이 높으면 해당기업의 영업비밀이나 중요기술의 유출이 상대적으로 제한될 수 있다고 볼 수 있다. 이 같은 지적을 바탕으로 통상적으로 인식하고 있는 경영진의 보안의식 수준이 ISMS 인증에 얼마나 효과가 있는지를 알아보고자 한다.

가설 5: 종업원의 보안의식 수준이 높은 경우 ISMS 인증의 효과가 있다.

영업비밀이나 산업기술, 정보 등의 유출은 대부분 사람을 통해서 이루어진다. 한국산업기술진흥협회[22]가 조사한 “산업기밀관리 실태조사 보고서”에 따르면 기업들은 기술유출의 발생 원인으로 허술한 보안관리 및 감독체제, 임직원의 보안의식 부족 등을 지적하고 있다. 또한 기술유출관계자로 퇴직 임직원의 비중이 가장 높고(73%), 경쟁업체, 협력업체 종업원의 순으로 나타나 종업원의 보안의식이 중요하다고 볼 수 있다.

가설 6: 정보보안에 대한 투자 수준에 따라 ISMS 인증의 효과가 증가한다.

전술한 한국산업기술진흥협회[22]에 따르면 기술유출 방지에 투자하고 있다는 기업은 53% 수준(대기업 58.8%, 벤처기업 54.6%, 중소기업 52.1%)이나 금액으로는 33백만원 수준(대기업 185백만원, 벤처기업 20백만원, 중소기업 16백만원)으로 매우 미미한 수준이다. 또 조사대상 중소기업의 절반이상은 정보보호 인증체계가 구축될 경우 인증을 받을 의사가 있는 것으로 조사되었다. 또 인증에 필요한 비용은 일부 또는 전부 부담할 의사가 있는 것으로 나타났다. 따라서 정보보안에 대한 투자가 증대된다면 ISMS 인증의 효과가 나타날 것으로 가설을 설정하였다.

4. 실증분석 결과

4.1 ISMS 인증효과의 요인분석

실증분석을 위해 우선 타당성을 분석하였다. 타당성 분석은 일반적으로 측정도구가 측정하고자 하는 변수에 대해 개념이나 속성을 얼마나 정확하게 측정하고 있는가를 알아보기 위함이다. 이를 위해 일차적으로 인증효과 및 성과에 대하여 요인분석(factor analysis)을 실시하였다. 요인분석 방법으로는 주성분(principle components) 분석법을 사용하였는데, 고유치(eigenvalue)가 1 이상이 되는 요인그룹을 선택하였고, 요인 축 간의 독립성을 유지하면서 회전하기 때문에 요인 축 간의 상관관계가 거의 없는 직각회전(varimax)법을 요인회전방식으로 사용하였다.

이 같은 주성분분석법은 상관관계가 높은 변수들을 조합해서 그 변수들의 정보를 가능한 많이 함축하고 있는 새로운 인위적인 변수를 만들어냄으로써 많은 자료를 단순화하고 요약·정리하기 때문에 “자료 축약기법”으로 불리는데, 본 논문에서는 이 과정을 통해 ISMS 인증의 효과 및 성과를 구성하는 경영성과 측면과 운영성과 측면을 대표하는 요인을 도출하였다.

〈표 5〉 ISMS 인증의 효과 및 성과 중 경영성과 측면의 요인분석 결과

경영성과 측면	(1)	(2)
법규준수에 효과적	0.033	0.860
고객 및 이해관계자의 신뢰 증가	0.201	0.799
매출액 증가	0.688	0.345
보안투자의 효율성 증가	0.740	0.037
시장 점유율 및 시장경쟁력 강화	0.689	0.271
전반적으로 보안투자 비용 감소	0.580	0.436
정보 유출 등 보안사고 감소	0.671	-0.097
고유값(Eigenvalue)	2.920	1.174
설명변량(% of Variance)	0.417	0.168
누적설명변량(Cum-Variance)	0.417	0.585
크론바흐 알파계수(Cronbach's Alpha)	0.662	0.746

우선 ISMS 인증의 효과 중 경영성과 측면[6]에 대한 탐색적 요인분석의 결과 요인적재치(factor loading)가 0.5 이상인 항목을 기준으로 2개의 요인이 도출되었다

6) 경영성과에 대한 요인추출에 있어 총 8개 설문문항 중 1개(전반적으로 경영성과에 효과적)는 전반적인 평가를 묻는 것으로 주성분분석에서 제외하였다.

(<표 5> 참조). 또 이들 2개의 요인은 전체 총분산 가운데 58.5%를 설명하는 것으로 나타났다.

이 요인분석 결과를 바탕으로 볼 때 ISMS 인증의 효과를 구성하는 첫 번째 요인은 '법규준수에 효과적', '고객 및 이해관계자의 신뢰 증가' 등에 기여하는 『기업 외부환경 성과』로 그룹화될 수 있으며, 두 번째 요인은 '보안투자의 효율성 증가', '보안투자 비용 감소', '보안사고 감소' 등 『기업 내부환경 성과』로 그룹화 될 수 있다고 보았다. 그리고 이 같은 요인분석 결과에 대해 각 척도의 신뢰성을 평가하기 위해 크론바흐 알파계수(Cronbach's alpha reliability coefficient)를 구하였다. 신뢰성 검증 결과, 모든 항목들의 신뢰도가 0.6을 초과하여 측정도구의 신뢰성은 적정하다고 판단되었다[31].

다음으로 ISMS 인증의 효과 중 운영성과 측면에 대한 총 설문문항 18개에 대해서 요인분석을 실시하였고, 결과적으로 5개의 요인이 추출되었다. ISMS의 운영성과 측면의 문항에 대한 첫 번째 요인은 '보안사고 예방과 보안업무의 체계적 관리에 효과적'이며 '일관된 목표관리 능력'과 '직원들의 보안에 대한 인식 제고' 등을 포괄하는 『실행적 보안관리』에 대한 효과로 그룹화될 수 있으며, 두 번째 요인은 '시스템적 운영방식의 활성화'나 '정보 수집' 및 '성과 예측 가능' 등이 그룹화될 수 있는 『시스템적 보안관리』로 구분되었다. 세 번째는 『보안업무체계』, 네 번째는 『자원관리보안체계』, 마지막으로 다섯 번째는 '보안업무에 대한 일관된 방침 및 목표 관리 능력 향상' 및 '경영진의 보안에 대한 관심과 인식의 증가' 등 『경영진 보안관리 역량』 등으로 구분될 수 있다고 보았다. 이들 요인 중 『경영진 보안관리 역량』의 경우 크론바흐 알파계수가 0.6에 미달되어 전체 항목과 일관성이 낮은 것으로 판단되었다. 이에 따라 해당하는 두 항목을 제외한 후 다시 실시한 결과가 <표 6>에 제시되어 있다.

그 결과 모든 변수들의 크론바흐 알파계수가 0.6 이상으로 신뢰성이 확보되었고, 전체 총분산 중 67.8%를 설명해 우수한 설명력을 가진 것으로 판단되었다.

결과적으로 요인분석을 통해 ISMS 인증의 효과 및 성과를 구성하는 두 유형, 즉 경영성과 측면과 운영성과 측면에서 각각 2개 요인(기업 외부환경 성과, 기업 내부환경 성과)과 4개 요인(실행적 보안관리, 시스템적 보안관리, 보안업무체계, 자원관리보안체계)을 추출하게 되었다.

<표 6> ISMS 인증의 효과 중 운영적 측면의 요인분석 결과

운영적 측면	(1)	(2)	(3)	(4)
보안사고 예방에 효과적	0.287	0.609	0.197	0.281
보안업무의 체계적 관리에 효과적	0.129	0.585	0.186	0.481
직원들의 보안에 대한 인식 제고 및 기업 내 보안 문화 형성	0.347	0.499	0.413	0.072
보안업무의 규정화로 보안 준수 방법 명확화	0.225	0.603	0.509	-0.080
일회적이 아닌 지속적인 보안관리에 효과적	0.149	0.890	0.061	0.170
고객과의 의사소통 채널 및 피드백 관리구조 개선	0.679	-0.106	0.345	0.295
프로세스 접근방식의 운영으로 계획 및 목표 달성이 원활	0.680	0.236	0.399	0.039
시스템적 운영방식이 활성화되어 운영에 대한 효과성 및 효율성 향상	0.626	0.506	0.295	0.162
정량화된 성과 측정을 통해 시스템 개선을 위한 정보 수집 및 분석 능력 향상	0.720	0.427	0.079	0.009
데이터에 근거한 의사결정을 통해 기업 운영 및 성과에 대한 결과가 예측 가능	0.778	0.292	-0.216	0.224
인적자원관리(인원보안)에 효과적	0.681	-0.025	0.401	0.144
보안업무에 대한 책임과 권한이 명확해짐	0.223	0.085	0.783	0.166
보안업무를 위해 부서간 연계 협력체계가 수립됨	0.035	0.265	0.755	0.057
물적자원관리(물리적 보안)에 효과적	0.134	-0.037	0.155	0.813
IT 등의 관리(기술적 보안)에 효과적	0.111	0.279	0.009	0.842
협력업체(외주업체) 관리에 효과적	0.294	0.264	0.029	0.571
고유값 (Eigenvalue)	6.600	1.658	1.382	1.219
설명변량 (% of Variance)	0.412	0.104	0.086	0.076
누적설명변량 (Cum-Variance)	0.412	0.516	0.602	0.678
크론바흐 알파계수 (Cronbach's Alpha)	0.827	0.866	0.679	0.730

4.2 실증분석 및 가설의 검증: t-검정 및 F-검정

아래에서는 ISMS 인증효과에 관한 영향요인을 분석하기 위해서 55개 응답기업의 특성(업종, 기업규모, 보안전담조직 보유 여부)과 경영진 및 종업원의 보안의식 수준 그리고 정보보안에 대한 투자수준 등 주요 핵심 문항을 중심으로 성과요소별 점수에 대한 t-검정과 F-검정을 실시하여 그 결과 전술한 가설이 통계적으로 유의한지를

분석하였다.

우선 제조업 혹은 비제조업에 따라 ISMS 인증효과에 차이가 있다는 [가설 1]과 관련해 업종 구분에 따른 ISMS 인증효과의 차이에 대하여 t-검정을 실시하였다. 분석 결과, 경영성과 측면이나 운영적 측면에서 모두 통계적으로 유의하지 않은 것으로 분석되었다.[7] 따라서 ISMS 인증의 효과는 업종에 따라서 차이가 있지 않은 것으로 판단된다.

기업 규모에 따라 ISMS 인증효과에 차이가 있다는 [가설 2]의 경우 기업의 규모가 100인 미만, 100~500인, 500인 이상으로 구성된 만큼 기업규모 구분에 따른 ISMS 인증 성과의 차이에 대하여 요소별로 ANOVA를 활용한 F-검정을 실시하였다. 그 결과, 업종과 마찬가지로 경영성과 측면이나 운영적 측면 모두 통계적으로 유의하지 않은 것으로 분석되었고, 결과적으로 기업 규모는 그 자체만으로 ISMS 인증의 성과에 크게 영향을 미치지 못하는 것으로 보았다.

〈표 7〉 보안전담조직 유무에 따른 ISMS 인증효과 및 성과 차이 검정 결과

구 분		Levene의 등분산 검정		평균의 동일성에 대한 t-검정		
		F	유의확률	t	자유도	유의확률
실행적 보안관리	등분산이 가정됨	0.346	0.559	-2.331	52	0.024
	등분산이 가정되지 않음			-2.243	12.88	0.043
시스템적 보안관리	등분산이 가정됨	8.505	0.005	-1.950	52	0.057
	등분산이 가정되지 않음			-3.137	34.58	0.035

[가설 3]은 보안조직이 있는 기업이 ISMS 인증효과가 있다는 것이다. 기업 내 보안전담조직 유무에 따라 ISMS 인증효과 및 성과의 차이가 있는지를 t-검정으로 검토하기에 앞서 Levene의 등분산 검정을 실시하였는데, 시스템적 보안관리($p<.01$)와 보안업무체계($p<.1$)는 등분산 가정에 위배됨을 확인할 수 있었다. 이 같은 조건에서 실시한 t-검정에서 보안전담조직 여부가 비교적 높은 유의성($p<.05$)으로 시스템적 보안관리에 영향을 주는 것을 확인할 수 있었다. 더불어 보안전담조직은 실행적 보안관리에도 영향을 주었는데, 다시 말해 보안전담조직이 존재할 경우 보안업무에 대한 일관된 방침 및 목표 관리가 가능해지고, 일회적이 아닌 지속적인 보안관리가 가능하다는 점을 보여준다고 하겠다. 즉, 분석 결과, 실행적 보안관리와 시스템적 보안관리 요인에 대해서는 보안전담조직 유무에 따라 통계적으로 유의미한 차이가 있는 것으로 분석되었다.

〈표 8〉 경영진의 보안의식 수준에 따른 ISMS 인증효과 및 성과 차이 검정 결과

구분		제곱합	자유도	평균제곱	F	유의확률
기업내부환경성과	집단-간	1.125	2	0.562	2.60	0.084
	집단-내	11.050	52	0.217		
	합계	12.175	54			
시스템적 보안관리	집단-간	1.350	2	0.675	3.36	0.043
	집단-내	10.243	52	0.235		
	합계	11.593	54			
보안업무체계	집단-간	2.191	2	1.095	3.80	0.029
	집단-내	14.684	52	0.288		
	합계	16.875	54			

다음으로 [가설 4]에 대하여 ANOVA 분석을 실시하였다. 이것은 경영진의 보안의식 수준이 높은 경우 ISMS 인증의 효과가 있다는 것인데, 분석 결과 경영성과 측면에서는 기업 외부환경 성과에 대해서 그리고 운영적 측면에서는 시스템 보안관리와 보안업무체계 요인에 대해서는 경영진의 보안의식 수준에 따라 통계적으로 유의미한 차이가 있는 것으로 분석되었다. 다시 말해, 경영진의 보안의식이 높을수록 보안투자의 효율성이 증가하고, 정보 유출 등 보안사고의 감소에도 기여하는 것으로 나타났다. 더불어 경영진의 보안의식은 보안업무에 대한 체계성과 일관성을 높이고 정량화된 성과 측정과 데이터에 근거한 의사결정과 같은 보안관리의 시스템화에 기여함과 동시에 보안업무에 대한 책임과 권한 그리고 부서간 연계 협력체제의 구축과 같은 보안업무체계가 마련되는데 기여하는 것으로 판단된다.

이 같은 경영진의 보안의식 수준에 따른 ISMS 인증성과와 비교해 [가설 5]의 종업원의 보안의식 수준이 높

7) 유의하지 않은 t-검정과 F-검정 결과는 지면 관계상 제시하지 않았다. 하지만 요청에 따라 모두 제공될 수 있음을 밝혀둔다.

은 경우 ISMS 인증효과에는 다소 차이가 있다. F-검정을 통해 분석한 결과, 실행적 보안관리 요인에 대해서 통계적으로 대단히 유의미한 차이(p<.01)가 있는 것으로 분석되었는데, 이것은 ISMS 인증효과 중 보안사고의 예방이나 보안업무의 체계적 관리, 보안 문화 형성 등과 같이 보안관리 업무의 실행단계에서 보다 효과적으로 성과와 연계된다는 점을 나타낸다.

〈표 9〉 종업원의 보안의식 수준에 따른 ISMS 인증효과 및 성과 차이 검정 결과

구분		제곱합	자유도	평균 제곱	F	유의 확률
실행적 보안 관리	집단-간	1.810	2	0.905	5.38	0.008
	집단-내	8.576	51	0.168		
	합계	10.386	53			

이제 [가설 6]에 대해 F-검정을 실시하도록 하였다. 이것은 정보보안에 대한 투자수준에 따라 ISMS 인증의 효과에 차이가 있을 것이라는 가설이다. 본 논문이 기반하고 있는 「ISMS 국제표준 도입 및 인증의 효과성에 대한 실태조사」는 응답기업에 "귀사는 정보보안을 위한 보안비용 투자는 어떻습니까?"라고 묻고, 이를 5점 리커트 척도로 답하도록 하고 있다. 이 정보를 바탕으로 정보보안에 대한 투자 수준에 따른 ISMS 인증효과 및 성과의 차이에 대하여 F-검정을 실시한 결과, 경영성과 측면이나 운영적 측면 모두에서 통계적으로 유의한 결과를 얻을 수 있었다. 특히 앞선 보안전담 조직, 경영진 보안의식 그리고 종업원 보안의식에서의 결과와 비교해 상당한 차이가 있었다. 예를 들어, 경영성과 측면에서는 정보보안투자는 기업 외부환경 성과에서 유의한 차이를 나타냈는데, 이것은 보안투자가 높을수록 법규준수나 고객 및 이해관계자의 신뢰 증가에 기여한다는 점을 의미한다. 운영적 측면에서는 보안업무체계와 자원관리 보안체계를 강화하는데 기여했는데, 이들 두 요인의 경우 모두 성과 창출을 위해서는 일정 정도는 기업 차원의 관리 노력이나 자원의 투입이 요구된다는 점에서 논리적인 결과로 판단된다.

〈표 10〉 정보보안 투자 수준에 따른 ISMS 인증효과 및 성과 차이 검정 결과

구분		제곱합	자유도	평균 제곱	F	유의 확률
기업 외부 환경 성과	집단-간	2.367	2	1.184	3.25	0.047
	집단-내	18.601	51	0.365		
	합계	20.968	53			
보안 업무 체계	집단-간	1.770	2	0.885	2.99	0.059
	집단-내	15.105	51	0.296		
	합계	16.875	53			
자원 관리 보안체계	집단-간	1.271	2	0.636	3.98	0.025
	집단-내	8.155	51	0.160		
	합계	9.426	53			

이 같은 t-검정과 F-검정 결과, 즉 기술보호와 관련한 ISMS 인증의 효과 및 성과를 요인별로 분석한 결과, 보안전담조직이 있을 경우 실행적 보안관리 및 시스템적 보안관리에 대한 성과 및 효과가 보안전담조직이 없을 때보다 유의미한 차이가 있고, 경영진의 보안의식 수준이 높으면 높을수록 기업 내부환경 성과, 시스템적 보안관리, 보안업무체계를, 종업원의 보안의식 수준은 실행적 보안관리 효과를 증진시켰으며, 정보보안 투자 수준은 기업 외부환경 성과, 보안업무체계 그리고 자원관리 보안체계에 대한 효과가 있었음을 확인할 수 있었다.

4.3 실증분석 및 가설의 검증: 회귀분석

다음 분석단계로 요인분석을 통해 도출한 ISMS 인증의 효과 및 성과변수에 대해 가설에서 제시한 설명변수의 영향을 확인하기 위해 회귀분석을 실시하였다. 회귀분석을 실시하기 전에 설명변수 사이에 서로 상관관계가 없는지 확인하였다. 이를 위해 업종, 기업규모, 보안전담조직 여부, 경영진 및 종업원의 보안의식 수준 그리고 정보보안에 대한 투자수준을 설명변수로 하는 회귀식의 VIF(Variance Inflation Factor)를 측정하였다. 결과적으로 평균 VIF가 1.75에 지나지 않았고, 각 변수들의 VIF가 2.5를 넘는 경우는 없어 다중공선성(multicollinearity) 문제는 없었다.

그러나 서로 다른 업종과 규모의 기업에 대한 조사 결과는 이분산성(heteroskedasticity) 존재를 의심하게 한다. 이분산성의 검정을 위해 아래에는 잘 알려진 Breusch-Pagan/Cook-Weisber 검정을 실시하였다[25].

〈표 11〉 ISMS 인증효과 및 성과에 대한 영향요인 분석 결과

구분	기업 외부환경 성과		기업 내부환경 성과		실행적 보안관리		시스템적보안관리		보안업무체계		자원관리 보안체계	
	(1-1)	(1-2)	(2-1)	(2-2)	(3-1)	(3-2)	(4-1)	(4-2)	(5-1)	(5-2)	(6-1)	(6-2)
제조업 여부(제조업=1)	-0.133		-0.080		-0.007		-0.118		0.140		-0.132	
기업 규모(100인 미만 기준)												
100~500인	0.272		-0.135		0.164		0.086		-0.021		0.216	
500인 이상	-0.023		-0.078		0.098		0.003		-0.005		-0.092	
보안전담조직 여부(보유=1)		0.040		-0.067	0.251§	0.230	0.292*	0.092		0.151		0.225
정보보안 투자 수준 (소극적 기준)												
보통	0.088	0.152		0.181		0.238*		0.005	0.073	0.101	0.369**	0.502***
적극적	0.544*	0.522*		0.109		0.157		0.021	0.345§	0.383§	0.391*	0.549***
경영진 보안의식 수준 (높은 기준)												
보통		0.091	-0.090	-0.025		0.148	0.095	0.303*	-0.281	-0.212		0.241
낮음		-0.259	-0.504**	-0.546***		0.023	-0.030	-0.270	-0.315	-0.463		0.032
종업원 보안의식 수준 (높은 기준)												
보통		-0.270		-0.010	-0.338**	-0.400**		-0.225§		-0.028		-0.129
낮음		0.145		-0.065	-0.360§	-0.291§		-0.236		0.230		0.470**
R-squared	0.160	0.338	0.096	0.144	0.250	0.300	0.111	0.237	0.173	0.355	0.225	0.318
F-통계량	2.30 (0.060)	1.720 (0.128)	9.16 (0.000)	4.16 (0.001)	3.60 (0.005)	3.62 (0.003)	4.68 (0.001)	2.72 (0.019)	1.42 (0.222)	1.56 (0.171)	5.42 (0.001)	7.91 (0.000)

주 : 1. §는 10%, *는 5%, **는 1%, ***는 0.1% 신뢰수준에서 유의함을 나타냄
2. ( )안은 heteroskedasticity-robust 표준오차를 나타냄. 로버스트 표준오차에 따른 추정 결과에서는 R-squared값을 제공함

검정 결과, 성과요인 중 시스템적 보안관리(p=0.049), 보안업무체계(p=0.034), 자원관리 보안체계(p=0.065)에 대한 회귀식에서 이분산성이 존재하는 것으로 나타났다. 또 설명변수 중에서는 정보보호 투자 수준(p=0.066)에 있어 이분산성을 확인할 수 있었다.[8] 이들 변수에 존재하는 이분산성을 고려하기 위해 일반적인 최소자승법(OLS) 대신 Huber-White의 로버스터(robust) 추정을 실시하였다.[9]

또 ISMS 인증의 성과요소 각각에 대해 2개의 회귀모형을 적용하였다. 첫 번째는 제조업 여부와 기업 규모를 통제변수로 하고, 앞서 실시한 t-검정과 F-검정에서 유의한 차이를 보였던 변수를 설명변수로 하여 추정한 것이다. 따라서 <표 11>에서 볼 수 있듯이 각 성과변수별로 설명변수의 조합에는 차이가 있게 된다. 반면 두 번째 모형은 성과변수에 관계없이 앞선 t-검정과 F-검정에서 적어도 한 가지 이상의 성과변수에 유의한 영향을 나타냈던 보안전담조직, 정보보안 투자, 경영진 보안의식 그리고 종업원 보안의식을 설명변수로 하여 추정한 것이다.

추정 결과, 기업의 외부환경 성과를 종속변수로 한 (1-1)과 (1-2)에서는 정보보안 투자가 적극적인 경우에 소극적인 기업에 비해 법규준수나 고객 및 이해관계자의 신뢰가 증가하는 효과가 있는 것으로 나타났고, 이것은

8) Breusch-Pagan/Cook-Weisberg 검정은 전체 회귀식에 대한 검정과 개별 변수에 대한 독립적 검정을 실시할 수 있다[24].
9) 이분산 문제를 해소하기 위한 추정방법 중 본 논문에서와 같이 조건부분산이 알려져 있지 않은 경우에도 적용할 수 있는 방법으로 실행가능한 일반최소자승법(Feasible Generalized Least Squares)이 대안이 될 수 있다. 그러나 실제 두 추정 결과가 추정계수나 t-검정 결과에는 큰 차이점이 없으므로 본 논문에서는 로버스트 추정을 실시하기로 한다.

앞서 실시한 일원분산분석(ANOVA) 결과와 일치하는 결과이다. 또 다른 경영성과요소인 기업 내부환경 성과에 있어서는 경영진의 보안의식 수준이 두 회귀식, 즉 (2-1)과 (2-2)에서 모두 유의하게 나타나 <표 8>의 결과와도 일치했다.

다음으로 ISMS 인증의 운영적 측면을 나타내는 4개의 성과변수에 대해서도 동일한 회귀분석을 실시하였는데, 그 중 실행적 보안관리의 성과는 보안전담조직과 종업원의 보안의식 수준이 높을수록 정비례한다는 결과를 확인할 수 있었다. 단지 회귀식 (3-2)에서는 보안전담조직 대신 정보보안 투자의 수준이 영향을 미치는 것으로 나타났는데, 보안전담조직과 정보보안 투자는 서로 상관관계가 있을 수 있음을 감안하면 <표 7>과 <표 9>을 포함한 분석의 결과는 대체로 일관된다고 판단된다. 시스템적 보안관리의 경우 <표 7>과 <표 8>를 통해 보안전담조직과 경영진의 보안의식 수준이 영향을 미치는 것으로 예측되었으나 <표 11>의 (4-1)과 (4-2)의 결과는 회귀분석을 통해 전자, 즉 보안전담조직의 유의성은 확인되지만 경영진의 보안의식은 (4-2)를 통해서만 나타나 그 결과가 명확하지 않다고 판단된다. 보안업무에 대한 책임과 권한 그리고 부서간 연계 협력체계의 수립과 관련된 성과를 지칭하는 보안업무체계의 경우 앞선 <표 8>와 <표 10>을 통해 정보보안 투자 수준과 경영진의 보안의식이 영향요인으로 제시되었으나 다른 설명변수의 영향을 통제하게 되는 회귀분석을 통해서는 정보보안 투자가 적극적인 기업에서만 영향을 확인할 수 있었다. 또 물리적·기술적 보안에 관한 성과를 나타내는 자원관리 보안체계의 경우 <표 10>에서 확인된 정보보안 투자 수준이 (6-1)과 (6-2)를 통해서도 확인됨으로써 정보보안에 대한 투자 수준에 따라 ISMS 인증의 효과가 증가한다는 [가설 6]을 일부 지지하고 있다고 하겠다.

5. 분석 결과 및 결론

우리나라는 최근 들어 과거의 기술추격자에서 점차 기술혁신을 주도하는 선도자 역할로 자리바꿈 하고 있다[16]. 이와 더불어 산업기술의 유출 문제도 점차 빈번해지고, 이로 인한 경제적 피해도 급속히 증가하고 있다[11]. 그 동안 우리나라는 기술개발을 촉진하기 위한 법, 제도, 지원정책 등을 잘 정비해 왔으나 개발된 기술을 보호하고 불법적인 유출을 방지하는데 있어서는 아직까지 초보적인 단계로 평가된다[2].

이 같은 현실에서 본 논문은 국내 중소기업의 산업기술 보호 및 유출방지와 관련된 ISMS 적용의 효과성과 활용 정도를 분석하였다. 특히 ISMS 효과에 대한 영향요인을 도출하고, 이러한 영향요인을 바탕으로 중소기업의 산업기술보호에 필요한 효율적인 정책대안을 제시하고자 하였다. 이를 위해 본 논문은 ISMS 인증을 받은 중소기업을 대상으로 하여 그 활용성과와 관련된 6가지의 가설을 제시하고, 이에 대해 통계적인 가설검정을 실시하였다. 실증분석 및 가설검정 결과는 다음과 같이 요약해 볼 수 있다.

첫째, 제조업과 서비스업에 따라 ISMS 인증의 효과에 차이가 있을 것이라는 가설은 t-검정 및 회귀분석 결과 유의하지 않은 것으로 나타났다. 비록 「부정경쟁방지 및 영업비밀 보호에 관한 법률」에 따른 보호해야 하는 기밀에 기업의 기술 뿐 아니라 경영상의 정보 등도 포괄적으로 규정하고 있고, 인증을 받은 기업수도 비제조업이 많지만 업종에 따른 효과성 차이는 없다는 면에서 ISMS 인증의 효과가 굳이 서비스업에 국한되지 않는다고 볼 수 있겠다.

둘째, 기업 규모에 따른 ISMS 인증의 효과나 성과 차이도 확인하지 못하였다. 이것은 노민선・이삼열[7]에서 기업 규모가 산업보안 역량 수준과 유의미한 관계로 나타난 것과는 다소 차이가 있다. 하지만 본 논문은 ISMS 인증을 받은 기업을 대상으로 하였기에 분석대상의 차이가 있다. 특히 ISMS 인증을 받은 기업은 이미 정보보호의 필요성에 대한 인식이 높다는 측면에서 볼 때 이 같은 조건 하에서는 기업 규모가 인증효과에 커다란 영향을 미치지 못하는 것으로 해석해 볼 수 있겠다.

셋째, ISMS 인증은 보안조직이 있는 기업에서 더욱 긍정적인 효과를 가질 것이라는 가설을 검토한 결과 유의미한 상관관계가 있는 것으로 나타났다. 중소기업의 보안업무를 체계적으로 관리하는 것은 실행적 보안관리와 시스템적 보안관리에 있어 기업의 산업기술보호에 효과적이라는 것을 알 수 있었고, 이 가설은 지지되었다고 판단된다.

넷째, 경영진 및 종업원의 보안의식이 ISMS 인증에 차이를 가질 것이라는 가설에 대해서는 기업의 내부환경, 실행적 보안관리, 시스템적 보안관리 그리고 자원관리 보안체계 등 폭넓은 성과요인들에 있어 그 효과를 확인

할 수 있었다. 또 대체로 경영진의 보안의식은 경영성과 측면에서 유의하게 나타난 반면 종업원의 보안의식 수준은 운영적 측면의 성과에 보다 유의하게 영향을 미치는 것으로 나타났다. 즉, 경영진의 보안의식이 높을수록 보안투자의 효율성이나 보안사고의 감소에 효과적이고, 종업원의 보안의식 수준은 보안업무의 체계적 운영을 도모할 수 있다는 면에서 적절한 결과로 판단된다.

다섯째, 정보보안에 대한 투자 수준이 ISMS 인증효과 및 성과에 차이를 가져올 것이라는 가설에 대해서는 통계적으로 대단히 유의미한 결과를 확인할 수 있었다. 특히 이것은 경영적 측면은 물론 운영적 측면에서도 성과에 긍정적인 영향을 미쳤고, 특히 보안업무체계와 자원관리 보안체계와 같이 보안업무의 관리 능력을 향상시키는 것으로 나타났다.

이 같은 분석 결과를 바탕으로 볼 때 몇 가지 중요한 정책적인 함의를 찾을 수 있다. 먼저 비록 국제표준인 ISMS 인증을 받은 기업에서도 그 효과 및 성과는 기업의 보안 노력이나 경영진·종업원의 보안의식에 의해 영향을 받고 있다. 따라서 기술유출을 방지하기 위해서는 인증과 관련된 활동 외에도 여러 가지 내부 역량과 투자가 병행되어야 하겠다. 더불어 물리적·기술적 수단, 관련 인프라 그리고 체계적이고 시스템 차원의 관리 노력이 함께 요구된다. 둘째는 정보보안 투자가 ISMS 인증의 효과를 높이는데 중요한 요소이자 수단이지만 경영진과 종업원의 보안의식이 중요한 기능을 수행한다는 점이다. 대체로 정보보안 투자는 경영진의 보안의식과 상관성이 있다고 예상되었지만 실증분석 결과 그렇지 않았고, 경영진의 보안의식을 종업원의 보안의식이 따라가는 것도 아니라는 점에서 인증이나 물리적 투자의 성과를 담보하기 위해서는 경영진은 물론 종업원의 보안의식을 함양하기 위한 별도의 관심과 노력이 요구된다고 하겠다. 더불어 적어도 ISMS 인증을 받은 중소기업에 있어서는 제조업과 서비스업의 업종 구분이 크게 영향을 못 미치는 것으로 나타나 업종이나 산업의 구분 없이 향후 인증과 관련된 지원을 추진해야 할 것으로 보았다. 단지 본 논문이 ISMS 인증을 받은 기업만을 대상으로 하였기 때문에 인증의 효과성을 논하기에는 다소 한계를 지니고 있다고 하겠다. 이 같은 점은 기술유출과 관련된 현재의 조사가 지나치게 소극적이고 적은 규모로 행해지고 있다는 점을 시사하는 한편 향후 보다 포괄적인 실태조사와 분석이 필요하다는 점을 말해주고 있다고 하겠다.

참 고 문 헌

[1] 국가정보대학원 (2006), 산업보안실무.

[2] 김민배 · 김경준 (2007), “산업기술의 유출방지 및 보호에 관한 법률과 쟁점”, 산업재산권, pp. 1-36.

[3] 김성원 (2009), “국가R&D관련 보안관리 제도에 관한 검토”, 산업보안연구학회논문지, Vol. 1, No. 1, pp. 75-91.

[4] 김용희 (2012) “지속가능성장을 위한 중소기업 R&D 현황 및 투자 지원 방향”, 한국과학기술기획평가원, 이슈페이퍼, 2012-03.

[5] 김인관 외 (2011), “산업기술 보안의식과 정보보안 투자가 ISMS 인증에 미치는 영향분석”, 한국기술혁신학회 학술대회, pp.101-115.

[6] 남재성 (2012), “중소기업의 산업기밀 유출범죄 피해 실태와 대책: 법, 제도적 방안을 중심으로”, 한국공안행정학회보, Vol. 45, pp.45-75.

[7] 노민선 · 이삼열 (2010), “중소기업의 산업보안 역량에 대한 영향요인 평가”, 한국행정학보, Vol. 44, No. 3, pp.239-259.

[8] 산업자원부 (2007), 산업기술의 유출방지 및 보호에 관한 기본계획(안).

[9] 송위진 외 (2006), “탈추격형 기술혁신체제의 모색”, 과학기술정책연구원, 정책연구, pp. 488-503.

[10] 오남석 외 (2011), “정보보호 수준평가 방법 개선에 관한 연구”, 전자상거래학회지, Vol. 16, No. 2, pp.159-169.

[11] 이대성 외(2010), “정보유출 방지 연구기술 동향”, 정보보호학회지, pp.56-65.

[12] 장항배 (2010), “중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계”, 한국멀티미디어학회논문지, pp.111-121.

[13] 장항배 · 송지훈(2010), “산업기술 유출방지를 위한 보안시스템 평가 탐색적 연구”, 산업보안연구학회논문지, Vol. 1, No. 1, pp.50-61.

[14] 전재완 (2009), “기술 유출이 산업에 미치는 피해 추정기법에 관한 고찰”, 산업보안연구학회 논문지, 1(1), pp.20-32

[15] 정병일 (2011), “산업보호와 사이버안전의 법제연구”, 한국IT서비스학회, 학술대회논문집, pp. 324-328

[16] 정선양 (2012), 「기술과 경영」, 제2판, 경문사.

[17] 중소기업청 (2007), “중소기업 기술유출 대응매뉴얼 -기술유출방지 관련 법제 및 보안서식 자료집-”, 한

국산업기술진흥협회.
[18] 지식경제부 (2010), 「2010 지식서비스산업 백서」.
[19] 최선태 · 유형창 (2010), "한국 산업보안교육 프로그램의 정립에 관한 연구", 한국경호경비학회지 Vol. 25, pp.185-208
[20] 최치호 (2009), 개방형 혁신체제에서 기술보호 및 확보방안에 대한 법제도적 고찰, 산업보안연구학회논문지, Vol. 1, No. 1, pp.33-49
[21] 한국법제연구원 (2007). 「정보보안 관련법제의 문제점과 개선방안」, 한국법제연구원, p.127
[22] 한국산업기술진흥협회 (2010), "산업기밀관리 실태조사 보고서", 중소기업청.
[23] 한성안(2010), "진화경제학적 동반성장 모형", 경제학연구, Vol. 58, No. 3, pp.255-290.
[24] Baum (2006), An Introduction to Modern Econometrics Using Stata, Stata Press.
[25] Breusch, T. S. & A. R. Pagan (1979), A Simple Test for Heteroscedasticity and Random Coefficient Variation, Econometrica Vol. 47, No.5, pp.1287-1294
[26] Eloff M. M. & S. H. von Solms (2000), "Information Security Management: An Approach to Combine Process Certification and Product Evaluation", Computer & Security, Vol. 19.
[27] OECD(2010), Main Science and Technology Indicators, Vol. 2010/1.
[28] OECD(2012), Internet Economy Outlook.
[29] Solow, R. (1956), "A Contribution to the Theory of Economic Growth", Quarterly Journal of Economics, Vol. 70, pp.65-94.
[30] Solow, R. (1957), "Technical Change and the Aggregate Production Function". Review of Economics and Statistics, Vol. 39, pp.321-320.
[31] Van de Ven, A. H. and D. L. Ferry (1980), "Measuring and Assessing Organizations", New York: John Wiley & Sons.

김 인 관

· 2011년 2월 : 건국대학교 기술경영학(경영학석사)
· 2012년 2월 ~ 현재 : 지식경제부 에너지안전팀장
· 관심분야 : 정보보안, 기술정책
· E-Mail : kimik@mke.go.kr

박 재 민

· 1992년 2월 : 서울대학교 경제학사
· 1997년 6월 : 미 오하이오주립대학교 기술경제학(M.S.)
· 1999년 9월 : 미 오하이오주립대학교 기술경제학(Ph.D.)
· 2007년 3월 ~ 현재 : 건국대학교 상경대학, 경영대학 교수

· 관심분야 : 기술경영, 디지털정책
· E-Mail : jpark@konkuk.ac.kr

전 중 양

· 2006년 2월 : 한국외대 경영정보학(경영학석사)
· 2008년 8월 : 한국외대 경영정보학(경영학박사과정수료)
· 2011년 8월 : 건국대학교 기술경영학(경영학박사과정수료)

· 관심분야 : 기술정책, 기술혁신, R&D관리
· E-Mail : bpr@hanmail.net