산업기술 보안의식과 정보보안 투자가 ISMS 인증에 미치는 영향분석

김인관* · 이승현** · 박재민***

Ⅰ. 서 론

우리나라의 연구개발 투자비율은 '08년 국내총생산 대비 3.37%로 경제협력개발기구(OECD) 가입국 가운데 스웨덴(3.6%), 핀란드(3.5%), 일본(3.4%)에 이어 네 번째 높은 수준이다. 우리나라는 짧은 산업의 역사 속에서 선진국의 기술을 도입하여 빠른 시간 내에 기술을 습득하였고 이 과정에서 많은 기술능력을 축적하여 IT 등 여러 분야에서 세계적으로 우수한 기술력을 보유하게 되었다. 80년대 이후 연구개발에 대한 투자를 지속적으로 증가시켜왔고, 90년대 이후에는 대폭적으로 기술개발을 지원하고 있다. 이에 따라 우리나라는 과거 추격형 모델에서 이제는 일부 기술 분야에서 오히려 추격의 대상이 되는 선도형 모델국가가 되었다.

Solow(1956,1957)는 20세기 전반 미국 경제성장의 80%가 기술발전에 의해 이루어졌고 노동과 자본에 의한 성장은 한계를 보이지만 기술에 의한 성장은 계속적인 성장이 가능하다고 하였다. 세계시장은 기술혁신에 의한 경쟁이 확대·심화되고 있다. 기술격차가 점차 줄어들면서 기술혁신을 추진하는 국가와 기업이 증가하고 있다. 기술혁신의 가속화로 신기술·신제품의 생존주기가 단축되고 있다. 신제품의 시장 진입을 단기간 내에 실현하기 위해서는 주요시장에 동시에 출시하는 경향이 강화되고 있다. 또 냉전체제 붕괴이후 각국은 산업정보의 수집에 관심을 집중하고 있다. 미국을 비롯한 주요 선진국은 기술유출 사례가 점차 증가함에 따라 경제스파이 법 등을 제정·시행하는 등 자국의 기술을 보호하기 위한 강력한 조치를 취하고 있는 실정이다.

우리나라는 그동안 기술개발에 치중하여 상당한 첨단기술력을 보유하고 있지만 체계적인 기술보호에 대해서는 소극적으로 대응하여 기술유출방지를 위한 시스템 이 미흡한 실정이었다. 1998년 1월 삼성전자의 반도체 기술유출사건을 계기로 산업기술보호를 위한 관리 필요성이 제기되어 1998년 12월 「부정경쟁방지 및 영업비밀보호에 관한 법률」이 제정되었고, 2007년에는 핵심기술의 적극적인 보호를 위해 「산업기술보호의 유출방지 및 보호에 관한 법률」이 제정되었다. 하지만 일부 대기업 등을 제외하고 인적·물적 자원이 열악한 중소기업은 기술보호에 대한 지식과 경험이 부족하고 기술유출방지를 전담할 조직이 없어 기술자산에 대한 보호를 위한 효과성을 기대하기 어려운 실정이다.

산업기술의 방지를 위한 대응은 첫째, 지재권 등 제도적인 보호수단에 의존하는 것이다. 둘째, 연구인력 등에 대한 충분한 인센티브를 제공하는 것이다. 셋째, 기술보호에 대한 통합보안관리 시스템을 구축하는 것이다. 산업기술의 보호는 이들 어느 하나만이 아니라 세 가지 측면 모두를 이행해야 가능하다고 볼 수 있다.

본 연구는 산업기술 보호와 관련하여 국제적 표준인 ISO/IEC 27001를 토대로 한 ISMS(Information Security Management System)을 중소기업에 적용할 경우 효과적인 활용에 영향을 미치는 요인을 분석하고자 한다.

* 김인관, 건국대학교 경영대학 기술경영학과 석사과정, kimik@mke.go.kr
** 이승현, 건국대학교 경영대학 기술경영학과 석사과정, karomjin@yahoo.co.kr
*** 박재민, 건국대학교 경영대학 기술경영학과 부교수, jpark@konkuk.ac.kr

Ⅱ. 이론적 고찰

「산업기술혁신촉진법」에서 “산업기술”이란 「산업발전법」제2조에 따른 산업, 「광업법」 제3조제2호에 따른 광업, 「에너지법」 제2조제1호에 따른 에너지와 관련한 산업, 「신에너지 및 재생에너지 개발·이용·보급 촉진법」 제2조제1호에 따른 신·재생에너지와 관련한 산업 및 「정보통신산업진흥법」 제2조제2호에 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 기술 ① 국내에서 개발된 독창적인 기술로서 선진국 수준과 동등 또는 우수하고 산업화가 가능한 기술 ② 기존제품의 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. 윤석철(2003)은 산업기술은 ① 특허권이나 공업소유권과 같은 지적소유권 형태로 보유되는 지식 ② 설계도면이나 시방서, 컴퓨터 프로그램이나 작업 매뉴얼 같은 유형의 용기 속에 담겨진 지식 ③ 특수공구나 기계 같은 hardware 속에 체현시켜 놓은 기술 ④ 몇몇 개인이나 작업집단(조직)속에 경험이나 기능의 형태로 보유된 Know-How 등 이라고 정의하였다.

기술유출은 해당국가의 특허전략이나, 지적재산권 보호 전력과 밀접한 관계를 갖는다. 해당 국가에서 기술유출을 어떻게 규정하고, 국가 정책적으로 보호해야할 기술을 어떻게 하는가에 따라 기술유출이 되거나 기술이전 등이 될 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> 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 비밀유지 의무가 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

산업기술의 유출 대상은 특허로 보호를 받는 기술이 아닌 영업비밀이나 기술개발과정의 기술이라고 볼 수 있다. 즉, 특허 받은 기술은 정보공개를 바탕으로 독점권을 부여 받고 있지만 영업비밀은 경제적 가치가 있는 정보에 대한 비공개와 비밀관리를 전제로 법적인 보호를 받기 때문에 정보자산에 대한 유출방지 대상이 되는 것이다. 중소기업청의 “기술유출 대응 매뉴얼”에서 기술유출은 국가, 기업, 기술개발자 등 각 이해관계자의 시각에 따라 기술거래, 기술협력 혹은 직업선택의 자유 등과 그 개념이 혼동되고 있다. 기술유출의 개념을 명확히 정립하기 위해서는 불법성 여부와 보호해야 할 가치, 정당한 대가의 지급 및 라이센스의 허용, 국가의 정책적 면의 고려 등을 우선적으로 규정해야 한다.

<표 2> 특허제도와 영업비밀보호제도 비교

구 분	특허제도	영업비밀
보호대상	기술적 발명	경제적 가치를 지닌 경영상·기술상 모든 정보
보호요건	신규성·진보성·산업적 이용가능성	비공지성·비밀관리성 경제적 유용성
보호기간	출원일후 20년간	비밀로 관리되는 기간
공개여부	공개	비공개
이전여부	실시권(통상, 전용) 부여	이전 불가

자료 : 노민선·이삼열 (2010)

산업보안과 정보보안은 실무적으로는 혼용해서 사용하지만 엄밀한 의미에서는 상당히 구분되는 개념이라고 볼 수 있다.

국가정보대학원(2006)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. 최선태(2009)는 산업자산의 안전성을 유지하는 모든 주체 및 관련조직들이 경쟁력 확보와 이윤추구를 위해 필요한 기술이나 경영상의 필수정보 등과 관련된 유·무형의 자산을 각종 침해요소로부터 보호하기 위한 자율적이고 예방적인 조치라고 정의하고 있다. 노민선 외(2010)는 산업체에서 직접보유하거나 산업활동과 관련된 물리적 자산, 인적자산, 기술상·경영상의 정보를 중요도에 따라 각종 위해요소로부터 보호하는 모든 활동이라고 정의하고 있다.

정보보안은 관찰이나 측정을 통해 수집된 자료를 실제 문제에 도움이 될 수 있도록 분석하여 정리된 지식을 안전하게 지키는 활동이다(Eloff, 2000). NIST는 정보시스템 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability)을 유지하기 위하여 정보시스템에 취해진 보호조치라고 정의하고 있다. 미 연방정보보안관리법은 ‘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 행위라고 말한다. 법제연구원(2007)은 정보보안에서 개인정보 보호와 영업비밀 보호와 같은 정보의 내용에 대한 보호는 제외하고 있다.

산업보안과 정보보안은 의미상에서는 차이가 있다고 볼 수 있지만, 실제적으로 산업보안대상이나 정보보안 대상이 상이한 것은 아니라고 본다. 즉 모든 산업이 IT와 연결되고 이를 활용한 산업이 점차 증대하고 있는 실정에서 이를 구분하는 것은 커다란 의미를 갖지 못한다고 판단된다.

Ⅲ. 산업기술보호관련 표준제도

ISO/IEC 27001은 1995년 영국의 기업에서 수년간 보안 업무를 수행한 전문가들이 모여 정보보호에 꼭 필요하고, 그 효과성이 있다고 판단되는 대응책(안전대책)들을 모아 "Code of practice for information security management" 문서를 작성하여 영국표준(British Standard 7799;BS 7799)으로 정하여 사용하게 하는 것에서부터 시작되었다.

이들 표준문서 중 가장 핵심이 되는 문서는 ISO/IEC 27001과 ISO/IEC 27002이다. 모든 것이 네트워크로 연결되어 있는 오늘날에는 1개 내지 2개의 주요 기업만이 정보보호를 한다고 그 기업의 보안이 확보되지 않는다는 것이다. 1개 내지 2개의 주요기업에 서비스를 제공하는 수십 개의 작은 기업들이 있으며, 이들 밑에는 수백 개의 더 작은 기업들이 필요한 서비스를 제공하고, 이들 기업들 간에 관련 정보들이 컴퓨터와 네트워크를 통하여 공유되어 업무가 수행되고 있기 때문이다.

따라서 네트워크를 통해 연결된 기업들이 다 같이 일정 수준 이상의 정보보호활동을 수행하지 않으면, 효과적인 정보보호가 안 된다는 것이다.

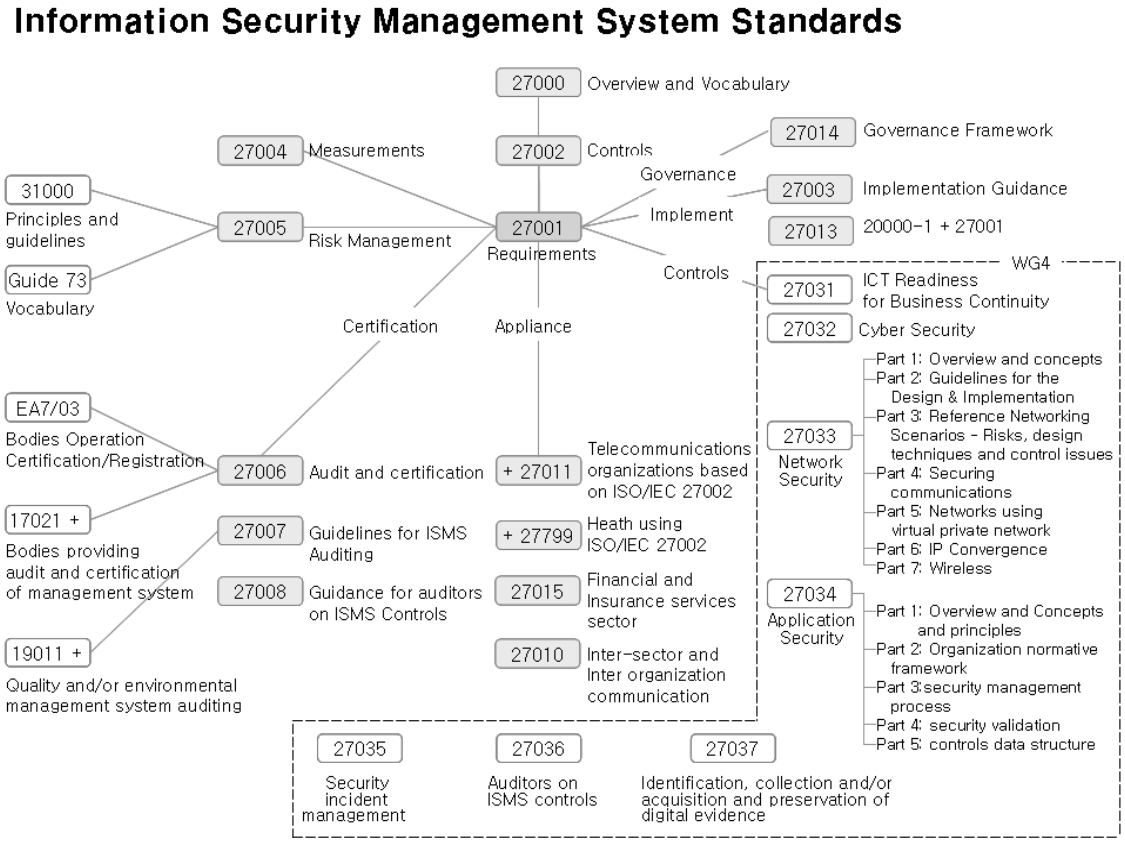
영국 정부와 전문가들은 이를 위한 가장 효과적인 접근 방법은 정보보호에 대한 인증 제도를 만들고 관련 기업들이 인증을 획득하게 하는 것이라고 인식하였다. 이러한 인증 제도를 위해서는 최소한 2가지 문서가 필요하다, 첫 번째는 인증 심사 시 기준이 되는 인증규격이며, 두 번째 문서로는 이들 인증 규격을 보다 자세히 설명해 놓은 일종의 해설서 역할을 하는 문서이다.

따라서 기존의 문서인 “Code of practice for information security”는 BS 7799 Part 1로 명명하여 해설서의 역할을 하게하고, 이를 바탕으로 1998년에 인증에 필요한 규격인 “Specification of information security management system”을 BS 7799 Part 2로 제정하여 영국 내에서 인증 제도를 시작하게 되었다.

영국에서 시작한 인증제도가 다른 국가에서도 도입하고 싶다는 요구가 있어 영국 정부는 국제표준화를 위하여 1999년도에 BS 7799 Part1과 Part2를 개정을 하였다.

이 개정판을 국제표준화기구(ISO)에 상정하여 여러 국가들과의 토론 및 수정과정을 통하여 2000년에 일단 BS 7799 Part1이 ISO 17799로 명명되어 국제표준이 되었다. 2005년도에는 BS7799 Part2를 ISO/IEC 27001로 만드는 작업이 진행되었으며, 이 내용을 반영하여 ISO 17799도 함께 개정되었다. 2006년도에 BS 7799 Part2가 국제표준이 됨으로써 전 세계적으로 인증을 확산할 수 있는 최소한의 관련 문서 및 시스템이 구비되었다. 또한 ISO 17799도 다른 문서들과의 조화와 통일성을 위하여, 2007년에 ISO/IEC 27002로 이름이 바뀌었다.

ISMS family 표준 문서는 현재 모두 15개의 문서로 구성되어 있으며 점점 그 수가 증가하고 있다.



(그림 1) ISMS 표준도

자료 : ISO/IEC

ISMS family 표준 문서 중 일부는 이미 국제 표준 문서로 확정되었으나 일부는 아직도 개발 중에 있으며 향후에도 점점 늘어날 것으로 예상되고 있다. 아래의 문서명 뒤에 연도가 표시되어 있는 것은 해당 연도에 국제표준이 된 것을 의미하며 CD 혹은 WD로 표기되어 있는 문서들은 현재 개발 중인 문서이다.

① <ISO/IEC 27000:2009> : Information technology - Security techniques - Information security management systems - Overview and vocabulary

이 문서는 ISMS family라고 불리는 표준 문서들에 대한 소개, 정보보호경영시스템(ISMS; Information Security Management System)의 개요, 그리고 PDCA (Plan-Do-Check-Act) 프로세스와 ISMS Family 표준 문서들에서 사용되는 용어에 대한 정의 및 설명을 담고 있다.

② <ISO/IEC 27001:2005> : Information technology - Security techniques - Information security management systems - Requirements

이 문서는 ISO/IEC 270xx 시리즈 표준 문서의 가장 핵심이 되는 것으로서 인증 심사 시 기준이 되는 정보보호경영시스템 요구 사항을 담고 있다. 문서는 본문과 첨부항목으로 구성되어 있으며 본문에서는 정보보호경영시스템(ISMS)의 수립, 구성, 운영, 관찰, 검토, 유지와 지속적 개선 체계에 대한 정보를 제공하고 있다. 특히 정보보호와 관련된 이슈들에 대하여 효과적인 의사결정에 필요한 위험 분석, 평가의 필요성과 관련 요구사항들이 명시되어 있으며, 첨부항목에는 11개 분야, 39개의 통제 목표와 이들 통제 목표를 달성하는데 필요한 133개의 통제항목(안전대책)에 대한 요구사항들이 명시되어 있다.

Ⅳ. 분석자료 및 분석모형

1. 분석자료

본 조사는「ISMS : Information Security Management System(정보보안경영시스템) 국제표준 도입 및 인증의 효과성에 대한 실태조사」라는 제목으로 ISO/IEC 27001 인증기관으로부터 동 국제표준에 의해 인증을 획득한 기업과 정보보안과 관련된 학계, 산업계, 인증심사원 및 컨설턴트를 대상으로 실시되었다.

설문내용은 인증기업 및 전문가 별로 별도로 작성되었으며, 설문대상 별 분석편차를 확인하기 위하여 일부 동일한 내용을 각각의 설문에 포함하였다.

설문항목은 인증기업이 7개 분야 174항목으로 구성 되었으며, 설문형태는 대부분이 단일선택형이고, 일부 효과성에 대한 설문의 누적평가를 위한 다중순위선택형을 채택하였다. 아래의 표에 설문대상별 설문항목을 대분류 중심으로 소개하였다.

<표 3> 설문응답기업 일반현황

	구 분	기업수	비율(%)		구 분	기업수	비율(%)
업종	전체	55사	100.0	기업규모	전체	55	100.0
	제조업	22사	40.0		100인미만	12	21.8
					100인~300인	9	16.4
					300인~500인	3	5.5
	비제조업	33사	60.0		500인 이상	29	52.7
					무응답	2	3.6

자료 : 한국인정원(2010)

ISO/IEC 27001 인증을 획득한 119개 국내기업 및 기관(이하 “기업”, “조직” 또는“인증기업”이라 한다.) 전체를 설문대상으로 하여 55개 기업이 응답하였고, 회수율은 46.2%를 나타냈다. 이 중 제조업은 22개(40%)였으며, 비제조업은 33개(60%)의 구성분포를 보였다. 또한 기업의 규모는 무응답 2개를 제외하고 아래의 <표 3>와 같이 나타났다. 전체적으로 ISO/IEC 27001 인증기업은 중견기업 이상의 규모가 많은 것으로 나타났으며, 이는 응답기업의 경우도 500인 이상의 사업장이 52.7%로 과반수를 넘는 것으로 나타났다.

데이터 분석을 위한 기본 방법은 정보보안경영시스템의 도입 및 운영성과 그리고 애로사항 등의 분석을 위하여 주로 5개 항목 중 1개 또는 복수를 강제로 선택하도록 하는 리커트척도(Likeret Scales)를 사용하였으며, 척도의 크기는 1점에서 5점까지의 5단계로 적용하고 데이터 분석 시에는 100점 만점으로 환산하여 분석을 용이하도록 하였다. 본 실태조사 분석에서는 이러한 서술적인 내용과 정확한 실체를 확인하기 힘든 기타 의견은 제외하였다. 기업규모와 관련하여 300인~500인 기업의 모집단 개체수가 3개사에 불과하여 일부 분석 시 100인~300인 규모의 기업과 합산하여 분석을 실시하였다.

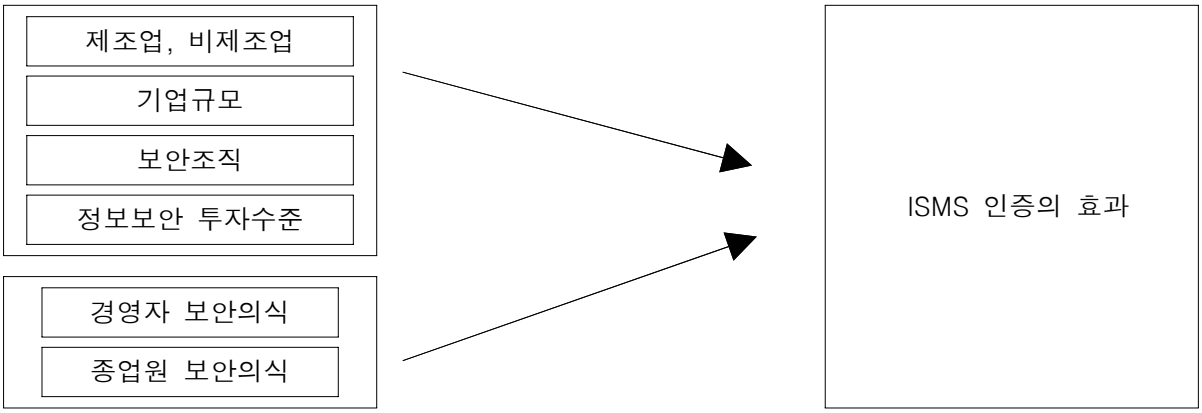
본 조사는 인증기업은 7개 분야 174항목, 전문가는 5개 분야 102항목으로 나누어 조사하였다.

인증기업의 조사 분야를 보면 첫째, 기업의 일반현황으로 매출액 대비 보안투자비용, 기술보유현황, 보안부서 유무, 종업원 수, 인증현황, 연구개발조직, 연구원 수 등 일반사항에 대한 정보를 조사하였다. 둘째, 중요정보자산 및 기술 보호관리 일반현황으로 중요 정보자산, 유출위협요인, 보안수준, 보안비용 투자, 전문가 컬설팅, 유출경험 및 경로 등에 대한 정보를 수집하였다. 셋째, ISMS 인증 추진과정에서 동기, 구축 경로, 컨설팅 효과 등을 조사하였다. 넷째, ISMS 인증의 효과 및 성과와 관련하여 경영성과, 운영성과, 인증심사의 효과 등에 대해 조사하였다. 다섯째, 인증유지 시 애로사항으로 경영진 관심, 타부서 협조, 운영상 괴리, 전문성 부족 등 17개 문항을 조사하였다. 여섯째, ISMS 인증 시스템의 운영성숙도 평가와 관련하여 정보보호 관련 각종 규정의 문서화 정도, 조직체계, 역할과 책임 등 총 39개 문항에 대해 조사를 하였다. 또한 정보보호관리체계의 성숙도와 관련 시스템 개선, 경영층 역할, 위험분석/평가, 정보자산 관리체계, 각종 규정, 조직 체계 등에 대해 조사를 하였다.

2. 분석모형 설계

정보보호를 위한 대부분의 선행연구는 우리나라의 산업기술보호를 위한 제도가 정착된 기간이 짧아 주로 산업기술보호, 정보보호를 위한 법적, 제도적 문제점이나 지원 등에 관심을 주로 다루었고, IT산업의 확산에 따른 정보보호 등을 위한 제도에 미치는 영향요인을 분석한 선행연구는 거의 없다.

본 연구에서의 연구 분석모형은 정보보호를 위해 국제적 표준으로 활용되고 있는 ISO/IEC27000 시리즈의 단계적 도입을 위해 마련한 ISMS 인증기업을 대상으로 조사한 “중소기업의 기술보호관리체계 국제표준의 효과적인 활용 및 산업체 확산지원 방안 연구” 자료를 활용하여 ISMS 인증을 받은 기업이 평가하는 ISMS 인증에 미치는 영향요인 무엇인지를 알고자 하는 것이고, 실증적인 규명을 위해 관련 선행연구와 이론을 기반으로 기업의 규모와 전담조직, 제조·비 제조 유무, 보안의식, 투자수준 등 독립변수가 종속변수에 해당하는 ISMS 인증의 효과성 및 성과에 미치는 영향을 분석해 보고자 한다.



(그림 2) 분석 모형

3. 기초통계

분석자료는 ISMS 인증기업의 ①중요자산 보호방법, ②중요 정보자산, ③중요정보자산 유출 위험정도, ④정보자산 유출경로, ⑤경영진 정보보안 관심정도, ⑥정보자산 유출사고 발생원인, ⑦정보자산 및 기술보호를 위한 ISMS 인증의 도움정도, ⑧중요정보자산 및 기술보호 보완/강화 부문, ⑨ISMS 인증 유지계획 ⑩ ISMS 인증취득 관련 애로사항 ⑪ ISMS 인증효과(경영측면/ 운영측면) 등을 조사한 내용을 기초로 하였다.

첫째, 기업이 주로 사용하는 출입통제시스템은 98%가 카드키시스템, 홍채/지문인식시스템 및 CCTV를 이용하는 것으로 나타났다. 또한 비제조업의 경우 “홍채/지문인식시스템”의 비율이 높게 나타났다. 기업규모가 클수록 출입통제시스템에 대한 투자가 많은 것으로 나타났고 다수의 인원을 통제할 경우, 출입에 대한 통제가 중요한 것으로 인식되고 있다. 둘째, 인증기업의 보호대상 중요정보자산은 복잡한 구조를 갖는 생산제조기술이나 법적으로 보호를 받고 있는 산업재산권에 비하여 유출이 용이한 “영업비밀/노하우(34.5%)” 및 “연구개발기술결과(27.3%)” 등이 상대적으로 더 중요하다고 인식하고 있었다. 제조업의 경우는 “연구개발기술 결과”가 63.6%, 비제조업의 경우는 “영업비밀 또는 노하우”가 34.5%로 중요한 정보자산으로 나타났다. 셋째, 인증기업의 정보자산의 유출경로와 관련하여서는 “내부로부터의 유출(81.8%)”이 “외부로부터의 유출(16.4%)”에 비해 압도적으로 높은 가능성을 보이고 있다. “내부로부터의 유출 가능성”은 제조업이 86.4%로 비조제업 78.7%에 비하여 약간 높게 나타났으며, 기업규모별로는 77.3%에서 100.0%까지 특별한 경향을 보이지 않는 고른 분포를 나타내고 있다. 넷째, 정보보안업무에 대한 경영진 및 직원들의 관심, 즉 보안의식과 관련하여 전체적으로 보안의식은 “경영진”이 69.1%, “직원”이 50.9%로 경영진이 다소 높은 인식을 보유한 것으로 보였다. 경영진의 경우 비제조업이 75.8%, 제조업이 59.1%였으며, 직원은 비제조업이 57.5%, 제조업이 40.9%로 비제조업이 높은 보안의식을 나타냈다. 기업규모 별로는 500인 이상의 기업 경영진이 75.9%로 규모가 작은 기업에 비해 비교적 높은 보안의식을 보였으며, 직원의 경우도 규모가 클수록 보안의식이 높은 것으로 나타났다. 다섯째, 기업의 ISMS 인증이 정보자산의 보호에 도움이 되는 것인가에 대해서는 설문에 응한 인증기업의 98.2%가 ISMS 인증이 기업의 정보자산 보호에 긍정적이라는 결과를 보이고 있으며, 도움이 되지 않는다는 부정적인 답변은 없는 것으로 나타났다. 제조업 및 비제조업이 동일한 수준으로 긍정적인 답변을 하였으며, 기업규모별로는 큰 차이를 보이고 있지 않으나, 기업규모가 클수록 ISMS 인증의 효과가 더 큰 것으로 나타나고 있다. 여섯째, ISMS 인증을 지속적으로 유지할 것인지에 대해 설문에 응한 55개중 53개 기업(96.4%)이 유지할 것으로 응답하였다. 일곱째, ISMS 인증획득 추진 시 “인증규격 내용의 이해가 어려움”에 대해서는 어렵지 않은 것으로 설문한 경우가 41.8%, 어려움이 있었던 것으로 설문한 경우가 58.2%로 나타났으며, 이는 ISMS 시스템 구축 시 주요한 애로사항 중 “인증규격 내용의 이

해가 어려움'이 주요한 요인이었음을 보여주고 있다. 특히, 제조업의 경우 68.1%의 경우가 어려웠다고 답변을 하여 비제조업(51.5%) 비하여 높은 비율을 보이고 있다. 기업규모별로는 100인~500인이 75%로 100인 미만(50.0%)과 500인 이상(51.7%)의 경우 보다 인증규격 내용의 이해가 어렵다고 응답했다. 일곱째, ISMS 인증효과의 경영성과 측면 중 "고객 및 이해관계자의 신뢰"를 높이는지에 대해서는 ISMS 인증이 "고객 및 이해관계자의 신뢰증가에 효과적"이다 라고 응답한 비율은 55개 기업 중 41개 기업(74.5%)으로, "효과적이지 않다"라고 응답한 2개 기업(3.6%)에 비해 상대적으로 매우 높은 차이를 보이고 있다. 특히 비제조업의 경우는 효과적이지 않은 비율이 0.0%로 나타났으며, 78.8%가 ISMS 인증효과에 대한 강한 긍정을 보이고 있으며, 제조업(68.2%)에 비하여 다소 높은 비율을 보이고 있다.

V. 실증분석 결과

1. 요인분석

ISMS 인증의 효과 중 경영성과 측면과 운영적 측면에 대한 요인 추출방법으로는 주성분분석법을 사용하였다. 주성분분석법(Principal Component analysis)은 상관관계가 높은 변수들을 조합해서 그 변수들의 정보를 가능한 많이 함축하고 있는 새로운 인위적인 변수를 만들어 내기 위한 기법으로 많은 자료를 단순화하고 요약·정리하기 때문에 "자료 축약기법"이라고도 한다.

주성분 분석에서 고유치(eigenvalue)가 1이상이 되는 요인그룹을 선택하였고 요인회전방식은 베리맥스(Varimax)방법[1]을 사용하였다.

경영성과 측면에 대한 총 설문문항 7개에 대p해서 요인은 2개가 추출되었으며, 요인 전체의 총분산에 대한 설명비율은 59.76%로 우수한 설명력을 가진 것으로 판단되었다.

<표 4> 경영성과 측면 요인의 초기 고유값 및 설명되는 총분산값

성분	초기 고유값			추출 제곱합 적재값		
	전체	% 분산	% 누적	전체	% 분산	% 누적
1	2.993	42.753	42.753	2.993	42.753	42.753
2	1.190	17.007	59.760	1.190	17.007	59.760
3	0.817	11.672	71.432			
4	0.736	10.512	81.943			
5	0.512	7.316	89.259			
6	0.427	6.093	95.352			
7	0.325	4.648	100.000			

ISMS 인증의 효과 중 경영성과 측면에 대한 요인추출 시 세부 문항 중 1개(전반적으로 경영성과에 효과적)는 다른 7개 문항과는 다른 성격의 문항으로 전반적인 평가를 묻는 질문이므로 요인추출을 위한 주성분분석의 대상에서 제외하였다.

1) 각 요인의 적재값이 높은 변수의 수를 최소화, 단순화

<표 5> 경영성과 측면 문항의 요인분석 결과

경영성과 측면 설문문항	요인1	요인2
법규준수에 효과적	0.847	-0.030
고객 및 이해관계자의 신뢰 증가	0.805	0.137
매출액 증가	0.562	0.499
보안투자의 효율성 증가	0.497	0.601
시장 점유율 및 시장경쟁력 강화	0.371	0.648
전반적으로 보안투자 비용 감소	0.111	0.734
정보 유출 등 보안사고 감소	-0.120	0.709

경영성과 측면의 설문문항에 대한 첫 번째 요인은 '법규준수에 효과적'이며 '고객 및 이해관계자의 신뢰 증가' 등 『기업의 외부환경성과』로 그룹화될 수 있으며, 두 번째 요인은 '보안투자의 효율성 증가'와 '보안투자비용 감소', '보안사고 감소' 등 『기업의 내부환경성과』로 그룹화 될 수 있다.

ISMS 인증의 효과 중 운영적 측면에 대한 총 설문문항 18개에 대해서 요인은 5개가 추출되었으며, 요인 전체의 총분산에 대한 설명비율은 70.64%로 우수한 설명력을 가진 것으로 판단되었다.

<표 6> 운영적 측면 요인의 초기 고유값 및 설명되는 총분산값

성분	초기 고유값			추출 제곱합 적재값		
	전체	% 분산	% 누적	전체	% 분산	% 누적
1	7.109	39.493	39.493	7.109	39.493	39.493
2	1.705	9.472	48.965	1.705	9.472	48.965
3	1.488	8.267	57.231	1.488	8.267	57.231
4	1.289	7.163	64.395	1.289	7.163	64.395
5	1.124	6.243	70.637	1.124	6.243	70.637

주 : 지면관계상 나머지 요인에 대한 추정값 생략

<표 7> 운영적 측면 문항의 요인분석 결과

운영적 측면 설문문항	요인1	요인2	요인3	요인4	요인5
보안사고 예방에 효과적	0.648	0.284	0.122	0.272	0.150
보안업무의 체계적 관리에 효과적	0.631	0.095	0.115	0.507	0.092
보안업무에 대한 일관된 방침 및 목표 관리 능력 향상	0.685	-0.184	0.082	0.172	0.444
경영진의 보안에 대한 관심과 인식의 증가	0.487	0.240	0.125	-0.143	0.485
직원들의 보안에 대한 인식 제고 및 기업 내 보안 문화 형성	0.525	0.333	0.373	0.047	0.182
보안업무의 규정화로 보안 준수 방법 명확화	0.653	0.228	0.456	-0.080	0.079
일회적이 아닌 지속적인 보안관리에 효과적	0.729	0.391	0.133	0.263	-0.267
프로세스 접근방식의 운영으로 계획 및 목표 달성이 원활	0.093	0.612	0.539	0.137	0.180
시스템적 운영방식이 활성화되어 운영에 대한 효과성 및 효율성 향상	0.386	0.625	0.389	0.240	0.139
정량화된 성과 측정을 통해 시스템 개선을 위한 정보 수집 및 분석 능력 향상	0.329	0.760	0.127	0.013	0.223
데이터에 근거한 의사결정을 통해 기업 운영 및 성과에 대한 결과가 예측 가능	0.102	0.831	-0.097	0.278	0.180
보안업무에 대한 책임과 권한이 명확해짐	0.075	0.098	0.821	0.169	0.205
보안업무를 위해 부서간 연계 협력체계가 수립됨	0.274	0.016	0.753	0.030	0.071
물적자원관리(물리적 보안)에 효과적	0.164	-0.077	-0.022	0.635	0.539
IT 등의 관리(기술적 보안)에 효과적	0.177	0.137	0.053	0.860	0.064
협력업체(외주업체) 관리에 효과적	0.060	0.341	0.209	0.683	-0.043
고객과의 의사소통 채널 및 피드백 관리구조 개선	0.082	0.357	0.267	0.224	0.656
인적자원관리(인원보안)에 효과적	0.147	0.388	0.266	0.027	0.681

ISMS의 운영적 측면 설문문항에 대한 첫 번째 요인은 '보안사고 예방과 보안업무의 체계적 관리에 효과적'이며 '일관된 목표관리 능력'과 '지속적 보안관리' 등을 포괄하는 『전사적 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 '고객과의 의사소통' 및 '기업 내부의 인적자원관리' 등 『대·내외 인적관리보안』등으로 구분될 수 있다.

<표 8> ISMS인증의 효과 및 성과의 요인분석 결과(요약)

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

따라서, ISMS 인증의 효과 및 성과에 대한 모형은 크게 2구분(경영성과 측면과 운영적 측면), 7개 요인(기업 외부환경성과, 기업 내부환경성과, 전사적 보안관리, 시스템적 보안관리, 보안업무체계, 자원관리보안체계, 대·내외적 인적관리보안)등으로 추출됨을 확인하였다.

<표 9> 통계적 검정을 위한 대상 및 세부내용

구분	검정대상	세부내용
응답기업 특성	업종구분	제조업/비제조업
	기업규모	100인 미만/100~300인 미만/300~500인 미만/500인 이상
	보안전담조직 보유 여부	보안전담조직 보유/보안전담조직 미보유
주요 핵심문항	경영진의 보안의식 수준	높음/보통/낮음
	종업원의 보안의식 수준	높음/보통/낮음
	정보보안에 대한 투자수준	높음/보통/낮음

ISMS인증에 대한 효과 및 성과를 세부적으로 분석하기 위해서 55개 응답기업의 특성(업종구분, 기업규모, 보안전담조직 보유 여부)와 경영진 및 종업원의 보안의식 수준 등 주요 핵심 문항을 중심으로 ISMS 인증에 대한 효과 및 성과 점수의 t-검정, F-검정을 실시하여 통계적으로 유의한지에 대해 검정하였다.

2. 가설검증에 대한 분석결과

<가설 1> 제조업, 비제조업에 따라 ISMS 인증 효과에 차이가 있다.

업종구분에 따른 ISMS인증 효과 및 성과의 차이에 대하여 t-검정을 실시한 결과, 운영적 측면이나 경영성과 측면 모두 통계적으로 유의하지 않은 것으로 분석되었다. 따라서 ISMS인증의 효과 및 성과는 업종에 따라서 차이가 있지 않은 것으로 판단된다.

<표 10> 업종구분에 따른 ISMS인증의 경영성과 측면 효과/성과 차이 검정 결과

구분	업종별	N	평균	표준편차	평균의 표준오차	t-값	P-value
기업 외부환경성과	제조업	22	3.288	0.677	0.144	-0.483	0.631
	비제조업	33	3.364	0.489	0.085		
기업 내부환경성과	제조업	22	3.091	0.521	0.111	-0.777	0.441
	비제조업	33	3.197	0.479	0.083		

<표 11> 업종구분에 따른 ISMS인증의 운영적 측면 효과/성과 차이 검정 결과

구분		Levene의 등분산 검정		평균의 동일성에 대한 t-검정		
		F	유의확률	t-value	자유도	유의확률
전사적 보안관리	등분산이 가정됨	0.273	0.603	-0.545	53	0.588
	등분산이 가정되지 않음			-0.548	46.092	0.586
시스템적보안 관리	등분산이 가정됨	0.062	0.804	-0.247	53	0.806
	등분산이 가정되지 않음			-0.246	44.938	0.806
보안업무체계	등분산이 가정됨	0.002	0.961	0.636	53	0.527
	등분산이 가정되지 않음			0.627	42.808	0.534
자원관리보안 체계	등분산이 가정됨	4.177	0.046	-0.682	53	0.498
	등분산이 가정되지 않음			-0.650	37.733	0.520
대내외적인적 관리보안	등분산이 가정됨	0.160	0.691	-1.143	53	0.258
	등분산이 가정되지 않음			-1.152	46.289	0.255

<가설 2> 기업규모에 따라 ISMS 인증 효과에 차이가 있다.

기업규모 구분에 따른 ISMS인증 효과 및 성과의 차이에 대하여 3개 이상의 집단에 대한 평균 차이검정법인 F-검정을 실시한 결과, 운영적 측면이나 경영성과 측면 모두 통계적으로 유의하지 않은 것으로 분석되어 기업규모는 ISMS인증의 효과나 성과에 크게 영향을 미치지 못하는 것으로 결론이 내려졌다.

<표 12> 기업규모에 따른 ISMS인증 효과/성과 차이 검정 결과

구분		제곱합	자유도	평균제곱	F	유의확률
기업 외부환경성과	집단-간	0.296	3	0.099	0.296	0.828
	집단-내	17.041	51	0.334		
	합계	17.337	54			
기업 내부환경성과	집단-간	0.610	3	0.203	0.825	0.486
	집단-내	12.576	51	0.247		
	합계	13.186	54			
전사적 보안관리	집단-간	0.189	3	0.063	0.349	0.790
	집단-내	9.215	51	0.181		
	합계	9.404	54			
시스템적보안관리	집단-간	0.065	3	0.022	0.083	0.969
	집단-내	13.294	51	0.261		
	합계	13.359	54			
보안업무체계	집단-간	0.515	3	0.172	0.535	0.660
	집단-내	16.366	51	0.321		
	합계	16.882	54			
자원관리보안체계	집단-간	0.717	3	0.239	1.327	0.276
	집단-내	9.194	51	0.180		
	합계	9.912	54			
대내외적인적관리보안	집단-간	1.201	3	0.400	2.270	0.092
	집단-내	8.999	51	0.176		
	합계	10.200	54			

<가설 3> 보안조직이 있는 기업이 ISMS 인증 효과가 있다.

기업 내 보안전담조직 유무에 따라 ISMS인증 효과 및 성과의 차이를 t-검정을 통해 분석한 결과, 시스템적 보안관리 요인과 자원관리보안체계에 대해서는 보안전담조직 유무에 따라 통계적으로 유의미한 차이가 있는 것으로 분석되었다.

<표 13> 보안전담조직 유무에 따른 ISMS인증 효과/성과 차이 검정 결과

구분		Levene의 등분산 검정		평균의 동일성에 대한 t-검정		
		F	유의확률	t	자유도	유의확률
전사적 보안관리	등분산이 가정됨	0.289	0.593	1.357	53	0.181
	등분산이 가정되지 않음			1.281	14.434	0.220
시스템적보안 관리	등분산이 가정됨	7.406	0.009	1.798	53	0.078
	등분산이 가정되지 않음			2.918	43.397	0.006
보안업무체계	등분산이 가정됨	2.922	0.093	0.660	53	0.512
	등분산이 가정되지 않음			0.917	28.170	0.367
자원관리보안 체계	등분산이 가정됨	2.546	0.117	2.051	53	0.045
	등분산이 가정되지 않음			2.331	18.476	0.031
대내외적인적 관리보안	등분산이 가정됨	0.186	0.668	0.308	53	0.760
	등분산이 가정되지 않음			0.333	17.133	0.743

<가설 4> 경영진의 보안의식 수준이 높은 경우 ISMS 인증 효과가 있다.

경영진의 보안의식 수준에 따라 ISMS인증 효과 및 성과의 차이를 F-검정을 통해 분석한 결과,

전사적 보안관리 요인과 보안업무체계 요인에 대해서는 경영진의 보안의식 수준에 따라 통계적으로 유의미한 차이가 있는 것으로 분석되었다.

<표 14> 경영진의 보안의식 수준에 따른 ISMS인증 효과/성과 차이 검정 결과

구분		제곱합	자유도	평균제곱	F	유의확률
기업 외부환경성과	집단-간	1.853	2	0.927	3.112	0.053
	집단-내	15.484	52	0.298		
	합계	17.337	54			
기업 내부환경성과	집단-간	0.997	2	0.498	2.126	0.130
	집단-내	12.190	52	0.234		
	합계	13.186	54			
전사적 보안관리	집단-간	1.318	2	0.659	4.239	0.020
	집단-내	8.086	52	0.155		
	합계	9.404	54			
시스템적보안관리	집단-간	1.119	2	0.560	2.378	0.103
	집단-내	12.240	52	0.235		
	합계	13.359	54			
보안업무체계	집단-간	2.196	2	1.098	3.887	0.027
	집단-내	14.686	52	0.282		
	합계	16.882	54			
자원관리보안체계	집단-간	0.409	2	0.204	1.118	0.335
	집단-내	9.503	52	0.183		
	합계	9.912	54			
대내외적인적관리보안	집단-간	0.691	2	0.346	1.891	0.161
	집단-내	9.509	52	0.183		
	합계	10.200	54			

<가설 5> 종업원의 보안의식 수준이 높은 경우 ISMS 인증 효과가 있다.

종업원의 보안의식 수준에 따라 ISMS인증 효과 및 성과의 차이를 F-검정을 통해 분석한 결과, 전사적 보안관리 요인에 대해서 통계적으로 유의미한 차이가 있는 것으로 분석되었다.

<표 15> 종업원의 보안의식 수준에 따른 ISMS인증 효과/성과 차이 검정 결과

구분		제곱합	자유도	평균제곱	F	유의확률
기업 외부환경성과	집단-간	1.009	2	0.505	1.607	0.210
	집단-내	16.328	52	0.314		
	합계	17.337	54			
기업 내부환경성과	집단-간	0.665	2	0.332	1.380	0.261
	집단-내	12.522	52	0.241		
	합계	13.186	54			
전사적 보안관리	집단-간	2.148	2	1.074	7.698	0.001
	집단-내	7.256	52	0.140		
	합계	9.404	54			
시스템적보안관리	집단-간	0.392	2	0.196	0.787	0.461
	집단-내	12.967	52	0.249		
	합계	13.359	54			
보안업무체계	집단-간	0.817	2	0.408	1.322	0.275
	집단-내	16.065	52	0.309		
	합계	16.882	54			
자원관리보안체계	집단-간	0.231	2	0.116	0.621	0.541
	집단-내	9.680	52	0.186		
	합계	9.912	54			
대내외적인적관리보안	집단-간	0.635	2	0.318	1.727	0.188
	집단-내	9.565	52	0.184		
	합계	10.200	54			

<가설 6> 정보보안에 대한 투자수준에 따라 ISMS인증의 효과가 있다.

정보보안에 대한 투자수준에 따른 ISMS인증 효과 및 성과의 차이에 대하여 F-검정을 실시한 결과, 운영적 측면이나 경영성과 측면 모두 통계적으로 유의하지 않은 것으로 분석되어 기업규모는 ISMS인증의 효과나 성과에 크게 영향을 미치지 못하는 것으로 결론이 내려졌다.

<표 16> 정보보안에 대한 투자수준에 따른 ISMS인증 효과/성과 차이 검정 결과

구분		제곱합	자유도	평균제곱	F	유의확률
기업 외부환경성과	집단-간	0.844	2	0.422		
	집단-내	15.048	50	0.301	1.403	0.255
	합계	15.892	52			
기업 내부환경성과	집단-간	1.498	2	0.749		
	집단-내	11.306	50	0.226	3.313	0.045
	합계	12.804	52			
전사적 보안관리	집단-간	0.760	2	0.380		
	집단-내	8.499	50	0.170	2.235	0.118
	합계	9.259	52			
시스템적보안관리	집단-간	0.083	2	0.041		
	집단-내	12.995	50	0.260	0.159	0.853
	합계	13.078	52			
보안업무체계	집단-간	1.515	2	0.757		
	집단-내	15.004	50	0.300	2.524	0.090
	합계	16.519	52			
자원관리보안체계	집단-간	1.000	2	0.500		
	집단-내	8.829	50	0.177	2.831	0.068
	합계	9.829	52			
대내외적인적관리보안	집단-간	0.096	2	0.048		
	집단-내	9.932	50	0.199	0.243	0.786
	합계	10.028	52			

중요자산 보호 및 기술보호와 관련한 ISMS인증의 성과 및 효과에 대한 세부분석을 위해 응답기업의 특성 및 핵심 문항을 중심으로 ISMS인증 성과 및 효과를 t-검정, F-검정을 실시한 결과, 보안전담조직이 있을 경우 시스템적 보안관리체계 및 회사자원관리 보안체계에 대한 성과 및 효과가 보안전담조직이 없을 때보다 통계적으로 유의미한 차이가 있었으며, 경영진 및 종업원의 보안의식수준이 높으면 높을수록 전사적 보안관리에 대한 ISMS인증의 성과 및 효과가 높았던 것으로 결론지어졌으며, 경영진의 보안의식수준과 관련해서는 보안업무체계에도 ISMS인증의 성과가 있던 것으로 판단된다.

Ⅵ. 결론 및 시사점

우리나라는 기술개발이 지속적으로 추진되고, 세계적인 기술들이 개발됨에 따라 최근 산업기술유출이 점차 증가하고 있다. 그 동안 기술개발과 관련된 연구는 제도, 방법 등 많은 분야에서 활발하게 이루어졌으나 이를 지키고 보호해야 하는 기술유출방지 분야에서 아직까지 초보적인 단계인 것 같다.

본 논문은 중소기업의 산업기술보호를 위 국제표준의 효과적 활용에 미치는 영향요인이 무엇인지를 찾아보고 이러한 영향 요인을 분석하여 중소기업의 산업기술보호에 필요한 ISMS의 효율적인 활용방안을 제시하고자 한다. 우선 가설검증을 바탕으로 종합적인 평가를 내려 보면 다음과 같이 평가할 수 있다.

첫째, 제조업, 비제조업에 따라 ISMS 도입에 차이가 있을 것이라는 가설에 대해서 검증한 결과, 유의하지 않은 것으로 분석되었다. 이는 설문조사에서 보는 바와 같이 ISMS를 도입한 기업이 비제

조업이 훨씬 많은 점 등으로 고려할 때 차이가 없는 것으로 판단된다.

둘째, 기업규모에 따라 ISMS 인증의 효과나 성과에 차이가 있는 가설을 설정하고 이를 분석한 결과 커다란 영향을 미치지 못하는 것으로 나타났다. 노민선이 2010년도에 분석한 “중소기업의 산업보안 역량에 대한 영향요인 평가”에서는 기업규모가 산업보안 역량수준과 유의미한 관계로 나타난 것과는 대조적인 결과가 나왔다. 이는 ISMS 인증을 받은 기업은 대부분 정보보호에 대한 인식이 높다고 볼 수 있다.

셋째, ISMS 도입이 중소기업의 보안업무를 체계적으로 관리하는데 대해 긍정적인 효과를 가질 것이라는 가설을 검토한 결과 유의미한 상관관계가 있는 것으로 나타났다. ISMS는 기술적, 물리적 지원 뿐만 아니라 관리적 지원까지 포함하여 시스템적으로 이루어져 기업의 산업기술보호에 효과적이라는 것을 알 수 있다.

넷째, 경영진 및 종업원의 보안의식이 ISMS 인증에 차이를 가질 것이라는 가설을 설정하였다, 분석결과 ISMS 인증의 전사적 보안관리 및 보안업무 체계에 대해 효과가 있는 것으로 나타났다

다섯째, ISMS에 대한 투자수준이 ISMS 인증효과 및 성과에 차이를 가져올 것이라는 가설에 대해서는 통계적으로 유의미하지 않은 것으로 분석되었다. 기술적, 물리적 투자와 함께 관리수준에 대한 인식제고가 필요하다고 볼 수 있다.

많은 기업들이 내부의 기술자산 등을 보호하기 위하여 보안장비 및 기술 등을 도입하여 적용하는 등 노력을 하고 있다. 정부에서도 기술유출방지를 위한 제도 등이 지속적으로 개선되면서 중소기업의 유출방지를 지원하고 있지만, 물리적·기술적 지원은 한계가 있기 때문에 이를 어떻게 효율적으로 관리하는냐가 중요하다.

기술유출 특징을 보면 우선, 소수의 연구자에게 기술이 집중되어 이들이 퇴사하거나 기술을 유출하는 경우 기업의 경쟁력이 상실될 뿐만 아니라 기업의 존폐가 결정된다. 둘째, 보안수준이 낮다는 것이다. 기술개발 등에는 관심이 높지만 기술유출방지는 추가적인 부담으로 생각하여 관심을 두지 않는 것이다. 셋째, 기술유출방지를 기술적인 문제로 인식하고 저장매체 제한, 이메일 감시 등 기술적인 대응만 구현하고 있다. 또 조직이 지속적인 발전을 하기 위해서는 조직은 수없이 많이 연결된 다양한 활동들을 관리하여야 한다. 이를 위해서는 프로세스적인 접근방법이 요구된다, 프로세스 접근방법은 프로세스의 결합 및 상호작용에 대해서 뿐만 아니라 프로세스에 구성된 시스템 내의 개별 프로세스 간의 연결 및 상호작용 등의 관리까지를 제공한다. 그리고 정보보안 관리방법은 정보를 보호하기 위한 하나의 물리적 또는 기술적 수단으로 치부되는 경향이 있으나, 정보보안은 기업 경영시스템에 자연스럽게 포함되어야 하는 경영시스템 상의 프로세스로 적용하여야 한다.

본 연구의 분석결과에서 정책적인 함의는 두 가지 관점에서 살펴볼 수 있다. 먼저 기술유출방지를 위한 내부적인 요인에 관한 것이다. 앞에서 본 바와 같이 기술유출방지는 물리적, 기술적 수단과 관리적 수단 등이 시스템적으로 이루어져야 한다는 것이다. 둘째는 외부적 요인과의 지속적인 관계를 통해 환경변화에 맞는 대응책을 마련해야 한다는 것이다. 하지만 현실적으로 중소기업이 ISO/IEC27001 도입을 위해서는 조직, 인력, 자금 등 여러 가지 면에서 열세이다. 또한 보안관리를 부차적인 것으로 생각하고 있다.

본 연구는 전체 기업을 대상으로 하기보다는 ISO/IEC27001 인증을 받은 기업을 대상으로 ISMS 도입에 대한 효과성을 분석하였기 때문에 전체 기업의 ISMS 도입에 대한 효과성 전체를 논하기에는 다소 한계를 지니고 있다고 하겠다.

향후 기술유출방지를 위한 많은 자료와 연구모형이 개발되어 기술유출의 인과관계를 측정하기 위한 연구들이 진행되고 이들 연구결과가 정책에 반영되어 기술유출방지를 위한 많은 제도개선과 지원이 있어야 한다고 본다.

참고문헌

(참고문헌은 지면관계상 생략함)