디지털산업정보학회 논문지 제12권 제3호-2016년 9월
http://dx.doi.org/10.17662/ksdim.2016.12.3.033

정보보호관리체계(ISMS)를 이용한 중소기업 기술보호 개선방안 연구*

김 정 은** · 김 성 준***

Study on Plans to Improve Small and Medium Corporations' Technological Protections Using Information Security Management System (ISMS)

Kim Jungeun · Kim Seongjun

〈Abstract〉

In the modern society based on information and communication, which is exposed to the risks of a lot of information security breaches, corporate information assets may be an economical scale in a country. Most of damages derived from corporate technological information leak often occur in small and medium corporations. Although many information security managers in corporations have focused on certification systems such as information security management system, small and medium corporations are poorly aware of the information security, and their environments surrounding it should be also improved. In addition, it is difficult to expect spontaneous participations in it, since the sustainable information security management systems are often not forced to be certified.

Thus, the purpose of this study is to examine plans to improve small and medium corporations' technological protections by using some component of the information security management system. On the basis of this examination, it also attempts to discuss some methods for effective and efficient information security in the small and medium corporations' technological protections.

Key Words : Small and Medium Corporations' Technological Protections, Improvement Plans

Ⅰ. 서론

오늘날 정보통신 사회의 지속적인 발달은 인터넷의 급격한 성장과 동시에 정보의 유출 및 탈취, 기업들의 기술 유출 등 수많은 정보 보안사고 발생의 위협에 노출되어 있다. 이에 따라 국내에서는 기업의 정보보호 역량을 강화하고, 이를 체계적으로 유지 및 관리하는 방법 중의 하나로 한국인터넷진흥원에서 정보보호 관리체계(Information Security Management System, 이하 ISMS) 인증을 부여 하도록 하고 있다[1].

정보보호 관리체계는 정부에서 시행하는 인증제도로서 정보통신서비스제공자, 정보통신서비스를 위해 물리적 시설을 제공하는 자, 민간사업자 등 인증대상

* 이 논문은 2016년도 산업통상지원부 산업보안 특성화학과 육성사업 지원을 받아 수행된 연구임.
** 남서울대학교 복지경영대학원 석사과정(주저자)
*** 남서울대학교 산업보안학과 교수(교신저자)

기관이 수립·운영하고 있는 정보보호 관리체계의 기술, 물리, 관리적 정보보호대책이 인증심사기준에 적합한지 평가하는 제도라고 할 수 있다[2].

우리나라에서는 방송통신위원회 산하기관인 한국인터넷진흥원(Korea Internet & Security Agency, 이하 KISA)으로부터 평가 및 인증을 받도록 하고 있으며, 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 제47조에 근거를 두고 있다. 최근 기업이 보유하고 있는 다양한 정보자산의 중요도가 높아짐에 따른 최고 경영층의 정보보호의 책임과 역할이 강조되고 있어 정보보호 관리체계의 중요성은 계속해서 증가하고 있다[3].

한국인터넷진흥원[4]에 의하면, 정보통신망법 개정(13.2.18)에 따른 정보보호 관리체계 인증을 의무화하고 금융, 공공 등 타 분야로 인증 대상을 확대하면서 실제 정보보호 관리체계 인증을 받은 업체의 수가 2010년 83건에서 2014년 377건으로 급격히 증가하였다. 하지만 국가정보원 산업기밀보호센터에 의하면 2005년부터 2012년 까지 국내 첨단기술을 해외로 불법유출 또는 시도한 사건은 약 300건 정도로 집계 되었다. 특히 피해 기업 중 중소기업의 비율은 71%에 달하는 것으로 나타났다.

개인정보 및 기업의 정보자산에 대한 취약성 그리고 보안 사고에 대한 기술적 대응의 한계점 인식에 따라 많은 기업의 정보보호 담당자들은 정보보호 관리체계의 구축에 주목하고 있다. 하지만 국내 기업의 대다수를 차지하고 있는 중소기업들의 경우 전반적으로 정보보안에 대한 인식이 부족하며, 열악한 환경을 가지고 있는 실정이다. 또한 기업의 정보자산을 보호하기 위한 단발성의 시스템은 구축하고 있다 할지라도 지속적인 관리가 가능한 정보보호 관리체계는 인증 의무화 대상 기준에 들지 않는 경우가 대다수이기 때문에 자발적인 참여를 기대하기 어렵다. 이에 따라 이를 이용한 중소기업 기술보호 개선 방안과 실증연구 또한 거의 없는 실정이다.

최근까지 진행된 정보보호 관리체계 관련 연구들은 중소기업의 특성을 고려한 연구가 드문 실정이다[5-9]. 또한 정보보호 관리체계의 인증이 조직의 성과에 미치는 영향에 초점을 둔 연구가 진행되어 왔으며, 정보보호 관리체계의 항목 개선에만 이루어진 실정이다[10-12].

본 연구의 차별점은 이상의 논의를 바탕으로 크게 2가지로 구분된다. 첫째, 중소기업의 보유 기술 특징, 보안 환경, 보안 의식 수준 등에 대한 명확한 분석을 통해 정보 보호 방안에 대해 전략적인 제언을 하고자 한다. 둘째, 중소기업의 기술 정보 유출 사례를 통해 정보 유출의 주요 특성들을 살펴보고, 정보보호 관리체계를 적용시켜 지속적인 기술 보호를 유도할 수 있는 방안을 논의하고자 한다.

이에 따른 본 연구의 목적은 정보보호 관리체계의 구성 항목들을 이용하여 중소기업의 기술 보호 개선 방안을 연구하고자 한다. 이를 통해 중소기업 기술보호에서의 효과적이고 효율적인 정보 보안 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 제Ⅱ장에서는 중소기업 기술보호의 정의와 특성 그리고 정보보호 관리체계 프레임 워크를 정리하고, 기존 중소기업 기술보호 선행연구를 살펴본다. 제Ⅲ장에서는 연구 프레임워크 및 가설을 설정하고, 제Ⅳ장에서는 변수 정의와 연구대상 및 분석단위를 기술하였다. 제Ⅴ장에서는 가설검증 및 결과분석을 기술하였고, 마지막으로 제Ⅵ장에서는 연구결과 및 시사점, 향후 연구방향에 대해 논의하였다.

Ⅱ. 이론적 배경

2.1 중소기업 기술보호

중소기업은 「중소기업기본법」 제2조 제1항 1호에

서 “업종별로 상시 근로자 수, 자본금, 매출액 또는 자산총액 등이 대통령령으로 정하는 기준에 맞고 영리를 목적으로 사업을 하는 기업”이라고 정의하고 있다. 그리고 기술이란 넓은 의미의 노하우(know-how)로서, 기업의 관점에서는 제품 또는 서비스의 생산 및 판매에 요구되는 정보로서[13], ‘상품적 가치’를 전제로 하는 지식이며, 또한 법적으로 그 소유권을 보호받을 수 있는 지적재산권, 특허, 상표, 저작권, 컴퓨터 소프트웨어, 영업권, 노하우 등의 자산으로서의 가치를 지니는 무형자산을 모두 포함한다[14]. 이를 보호하는 ‘기술보호’라는 용어는 김경선[15]의 연구에서는 기술보호의 의미를 ‘산업보안’, ‘기업보안’과 유사한 개념으로 해석하기도 하였다.

중소기업 기술 유출의 유형은 크게 4가지로 첫째, 인력이동에 의한 산업기술의 유출, 둘째, 부품 및 장비에 체화된 경험지식 이전, 셋째, 기술거래에 의한 산업기술 유출, 그리고 넷째로는 산업스파이에 의한 산업기술 유출이 있다[16]. 이러한 중소기업의 기술 유출의 원인으로는 보안인프라 투자 곤란, 보안 업무 관련 지식부족, 기술보호전담직원의 미 보유, 법・제도적 장치 미흡, 핵심기술인력 처우 미개선 등을 들 수 있다. 또한 기술유출피해 중소기업 중 절반 정도가 다시 동일한 피해를 경험하고 있는 것이 특징이다[17].

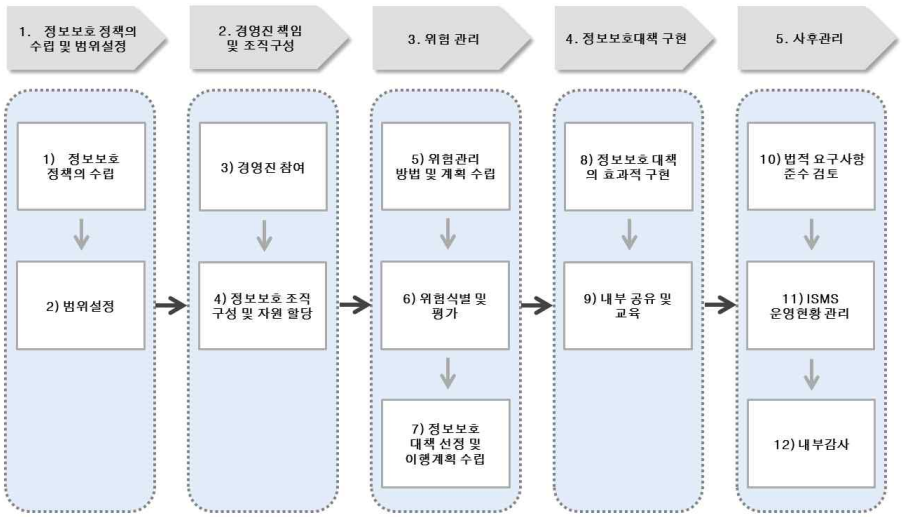
우리나라는 이러한 중소기업의 기술유출 방지를 위하여 직접적으로는 「중소기업기술 보호지원에 관한 법률」과 이와 밀접하게는 「부정경쟁방지 및 영업비밀보호에 관한 법률」, 「산업기술의 유출방지 및 보호에 관한법률」, 「특허법」, 「실용신안법」, 「상표법」, 「디자인보호법」으로 중소기업의 기술을 보호하고 있으며, 그밖에 「발명진흥법」, 「대외무역법」 등의 법률 내에 기술유출 방지 관련 조항을 명시하여 중소기업 기술을 보호하고 있다[18].

중소기업 기술보호와 관련된 선행연구로 이장훈 외[19]의 연구에서는 기술유출을 경험한 기업들의 패턴을 분석한 기술보호 개선방안을 제시하였다. 또한 김기호 외[20]의 연구는 신정보화환경에서의 중소기업 기술유출에 대한 보안인식과 관리 실태를 측정하여, 대기업과 중소기업 간의 수준 비교분석을 통해 기술유출 방지대책을 위한 정책의 기초자료를 제시하였다. 그리고 이규안[21]의 연구는 중소기업에서 발생하고 있는 첨단기술 유출 사례를 살펴보고 원인과 대책을 연구하여 디지털 포렌식을 이용한 첨단기술 유출 혐의자의 추적과 혐의 입증방안을 제안하였으며, 홍준석 외[22]의 연구에서는 중소기업청에서 실시한 2013년 중소기업 기술보호 역량 및 수준조사를 바탕으로 중소기업의 기술유출 경험유무와 기술보호 요인을 분석하여 정부지원을 통한 기술유출방지 효과를 극대화 할 수 있는 핵심 요인을 도출하였다. 또한 김인관 외[23]의 연구에서는 산업기술 보호와 관련된 국제표준의 역할에 주목하여 중소기업에 대한 ISMS의 효과와 성과에 미치는 영향요인을 분석하였다.

2.2 정보보호관리체계(ISMS)

정보보호관리체계(ISMS)는 정부에서 시행하는 인증제도로서 정보통신서비스제공자, 정보통신서비스를 위해 물리적 시설을 제공하는 자, 민간사업자 등 인증대상기관이 수립・운영하고 있는 정보보호관리체계의 기술, 물리, 관리적 정보보호대책이 인증심사 기준에 적합한지 평가하는 제도라고 할 수 있다[2].

우리나라에서는 방송통신위원회 산하기관인 한국인터넷진흥원(KISA)으로부터 평가 및 인증을 받도록 하고 있으며, 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 제47조에 근거를 두고 있다. 최근 기업이 보유하고 있는 다양한 정보자산의 중요도가 높아짐에 따른 최고 경영층의 정보보호의 책임과 역할이 강조되고 있어 정보보호관리체계의 중요성은 계



<그림 1> ISMS 프레임워크

속해서 증가하고 있다[3].

국내의 정보보호관리체계는 조직 내·외부의 위험 변화와 새로운 취약점 발견 등 지속적으로 변화하는 환경에 대응하기 위하여 위의 <그림 1>과 같은 프레임워크[24]에 따라 다섯 단계로 나뉘어져 실행되고 있다.

구체적인 내용을 살펴보면, 첫 번째 정보보호 정책의 수립부터 두 번째 경영진의 책임 및 조직 구성 단계에서는 조직 전반에 걸친 상위 수준의 정보보호정책을 수립하고, 이를 수행하기 위한 조직 내 각 부문의 책임을 설정한 후, 정보보호관리체계의 범위를 설정하고 범위 내 정보자산을 식별하여 범위를 명확히 한다. 다음으로 세 번째, 위험관리 단계에서는 조직문화와 정보 자산에 적절한 위험관리 전략과 계획을 수립하고, 이에 따라 위험을 분석하고 평가하여 대응이 필요한 위험과 우선순위를 결정한 후 위험을 수용 가능한 수준으로 감소시키기 위해 필요한 정보보호대책을 선택하고 구현할 계획을 수립한다. 또한 네 번째 구현 단계에서는 수립된 정보보호계획에 따라 정보보호대책을 효과적으로 구현하고, 필요한 교육과 훈련을 진행하게 되며, 마지막 사후관리 단계에서는 정보보호 관리체계의 운영 과정에서 지속적인 모니터링을 수행하고, 정기적인 내부 감사를 통해 정책 준수를 확인하는데, 이러한 결과를 기반으로 하여 정보보호관리체계를 재검토하여 개선이 이루어지게 된다[6].

정보보호관리체계 관련 선행 연구로 이영준[25]은 이러한 프레임 워크는 각 단계별로 각기 다른 문서화에 따라 연결 관계가 부족하므로 높은 정보보호관리체계의 상호연계성과 기존의 통제수립개념에서 벗어난 적절한 관리기법의 필요성을 강조하며, 정보보호 관리체계에 대한 시나리오 기법의 적용과 이를 효과적으로 표현하기 위한 UML 모델링과 템플릿을 제안하였다. 또한 김지숙 외[8]의 연구는 민간부문과 공공부문에서 시행하고 있는 정보보호 관리체계 통제항목에 대한 비교와 함께 그간 실시한 평가 미흡사항을 분석하여 이를 토대로 한 효율적인 정보보호 관리체계 구축방안을 살펴보았다. 그리고 장상수 외[24]의 연구는 국내 ISMS 인증 취득기업 정보보호 담당자에 대한 설문조사를 통해 ISMS 인증이 기업의 정보보호

성과에 긍정적인 영향을 미친다는 것을 입증하였으며, 홍성혁 외[26]는 정보보호관리체계 평가방법론의 연구를 위해 관리 지침, 평가 기준 산정 방법, 통제 항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분 등을 기준으로 국내·외 정보보호관리체계들을 비교 및 분석하여 국내 환경에 적합한 정보보호관리체계 평가 방법론을 제안하였다. 그리고 배영식[12]은 정보보호관리체계의 인증이 기업의 경영성과에 긍정적인 영향을 미친다는 것을 입증하였다.

Ⅲ. 정보보호 관리체계 기반의 중소기업 기술보호 개선안

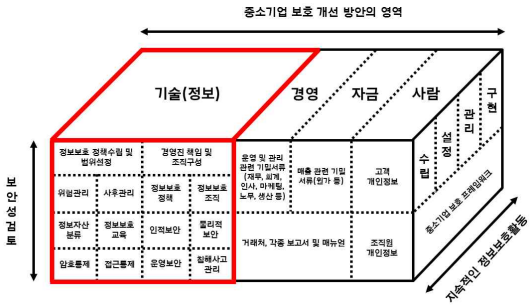
3.1 중소기업 기술보호 개선의 필요성과 영역의 정의

3.1.1. 중소기업 기술보호 개선의 필요성

오늘날 기업과 경제 성장의 원동력인 중소기업의 기술 정보는 그 주체가 기업뿐만 아니라 국내, 국외까지 확대될 정도로 중요해지고 있다. 하지만 꾸준히 증가하고 있는 기업의 기술 유출 피해는 기업의 성장을 저해시키는 것은 물론이고, 이는 곧 국가 경제에 큰 손실을 미치게 된다.

우리나라는 정보보호에 대한 체계적·지속적인 관리체계를 구축할 수 있도록 한국인터넷진흥원으로부터 정보보호 관리체계의 평가 및 인증을 받도록 하고 있다. 기존의 정보보호 관리체계의 인증 의무 대상은 정보통신 제공자, ISP, IDC와 같은 ICT 분야의 100억 또는 이용자수 100만 명 이상인 사업체에 한정되어 있었으나, 이제는 2016년 개정안에 따라 매출액 또는 세입 등이 1,500억 원 이상인 전체 금융회사 및 의료기관, 일일 평균 이용자수 1만 명 이상인 전체 사업체로 확대되었다. 국내 주요 정보유출 사고 발생 기업의 상당수가 비ICT 기업이라는 점과 많은 기업들의 정보자산 중요도가 증가함에 따라 정보보호 관리체계의 중요성 또한 증가한 것이다.

하지만 대다수 중소기업들의 경우 기술 유출 사고의 비중과 피해금액이 대기업에 비해 높은 편인데도 불구하고 전반적으로 정보보안에 대한 인식이 부족하며, 열악한 환경을 가지고 있는 실정이다. 또한 기업 정보자산의 지속적인 관리가 가능한 정보보호 관리체계는 인증 의무화 대상 기준에 들지 않는 경우가 많기 때문에 자발적인 참여를 기대하기 어려운 실정이다.



<그림 2> 중소기업 운영 영역의 특징

중소기업 기술 유출의 특징은 기술의 가치를 잘 인지하고 있으며, 접근 권한이 있는 내부 관계자가 유출을 시도하고 있으므로 내부인력에 대한 보안의 강화가 가장 중요하며, 또한 중소기업의 규모가 작을수록 기술보호 인식과 보안관리, 감독체계, 인력관리 등이 취약하다는 것이다. 또한 무엇보다 실제현장에서는 체계에 대한 접근과 활용이 더 쉬워야한다는 것이 중요하다. 이러한 중소기업의 현실을 고려하여 정보보호 관리체계가 비교적 단순한 구조로 개선되어 적절히 수행되는 것이 필요하다.

3.1.2. 중소기업 기술보호 개선의 영역

본 논문의 2장의 선행연구를 통해 중소기업의 운영 영역을 위의 <그림 2>와 같이 기술(정보) 및 경영, 그리고 자금과 사람으로 구분하였다.

4개의 영역 중 경영, 자금, 사람의 경우 정보자산의 측면보다 운영자산 측면에서 고려되는 부분으로 본 논문에서는 중소기업 운영요소 중에서 중소기업 기술 보호지침 개선의 영역을 기술(정보)로 범위를 정하였다. 그리고 앞서 언급하였듯이 중소기업의 현실을 고려한 정보보호 관리체계 수행과, 중소기업의 기술유출 특징에 따라 정보보호 관리체계의 정보보호 관리과정 5개의 분야 중 정보보호대책 구현을 제외한 4개 분야의 7개의 세부관리과정과 정보보호 대책의 13개 분야 중 외부자 보안, 시스템 개발 보안, IT 재해복구를 제외한 10개의 통제항목과 60개의 세부점검항목을 검토하고, 중소기업의 특성을 고려하여 개선 및 추가하였다. 이를 정리하면 다음 <표 1>과 같다.

<표 1> 보안 지침의 개선에 사용된 ISMS 점검항목

분야		통제 항목	세부 점검 항목	사용 여부	통제 항목/ 세부점 검항목
정보 보호 관리 과정	**1. 정보보호 정책 수립 및 범위 설정**	**2**	**4**	**사용**	**1/1**
	2. 경영진 책임 및 조직 구성	**2**	**4**	**사용**	**2/2**
	3. 위험 관리	**3**	**11**	**사용**	**1/1**
	4. 정보보호대책 구현	2	3		
	5. 사후관리	**3**	**6**	**사용**	**2/3**
정보 보호 대책	**1. 정보보호 정책**	**6**	**13**	**사용**	**4/4**
	2. 정보보호 조직	**4**	**7**	**사용**	**3/3**
	3. 외부자 보안	3	4		
	4. 정보자산 분류	**3**	**7**	**사용**	**3/4**
	5. 정보보호 교육	**4**	**10**	**사용**	**4/7**
	6. 인적보안	**5**	**11**	**사용**	**4/7**
	7. 물리적 보안	**9**	**21**	**사용**	**6/8**
	8. 시스템 개발 보안	10	22		
	9. 암호통제	**2**	**8**	**사용**	**1/2**
	10. 접근통제	**14**	**46**	**사용**	**10/11**
	11. 운영 보안	**22**	**56**	**사용**	**7/9**
	12. 침해사고 관리	**7**	**14**	**사용**	**5/5**
	13. IT재해복구	3	6		
총계		101	247	14	53/67

3.2 정보보호 관리체계 기반의 중소기업 기술영역 보호 항목

3.2.1. 중소기업 기술의 보호 개선항목

(1) 정보보호 관리과정의 점검항목

정보보호 관리과정은 ISO27001의 PDCA 라이프사이클에 따른 정보보호 관리체계의 보안정책 수립, 구현 및 운영, 모니터링 및 검토, 관리 및 개선 단계에 대한 내용의 인증기준을 정해놓은 것이다. 중소기업이 정보보호 관리체계 관리과정 항목을 모두 점검하기에는 시간과 비용이 많이 소모되어 현실적으로 어렵기 때문에 이를 고려하여 단순한 구조를 가져야 할 것이다. 따라서 기존 정보보호 관리체계의 정보보호 관리과정 중 정보보호대책 구현 부분을 제외한 나머지 관리과정의 세부 점검 항목을 추출하였으며, 정보보호대책 구현 과정을 삭제하는 대신 사후관리의 점검항목에 “내부감사”에 대한 2개 항목을 구체적으로 새로 추가하여 간소화하였다. 이를 정리하면 다음 <표 2>와 같다.

(2) 정보보호 정책의 점검항목

정보보호 대책에 있어서 정보보호 정책은 중소기업의 정보자산 보호에 있어 반드시 필요한 기본적인 분야이다. 대부분의 기업 정보 유출은 보안 관리자의 인식부족, 관리 지침 및 절차가 미흡하여 발생하고 있기 때문에 이를 위해서는 정보보호 관리체계의 도

<표 2> 정보보호 관리과정의 보안점검 항목

관리과정	세부 관리과정	점검항목		비고
정보보호 정책 수립 및 범위 설정	정보보호 정책의 수립	1	조직이 수행하는 모든 정보보호 활동의 근거가 될 수 있는 최상위 수준의 정보보호정책이 있는가?	
경영진 책임 및 조직구성	경영진 참여	2	경영진 또는 경영진의 권한을 위임받은 자가 정보보호 관리체계 내 중요한 활동 내용을 보고 받고 의사결정에 참여하고 있는가?	
	정보보호 조직 구성 및 자원 할당	3	최고경영자는 정보보호 관리체계 구축·운영에 소요되는 자원을 평가하여 필요한 예산과 인력을 승인하고 있는가?	
위험관리	위험관리 방법 및 계획 수립	4	매년 위험관리를 수행하기 위하여 전문 인력 구성, 기간, 대상, 방법, 예산 등을 구체화한 위험관리 계획을 수립·이행하고 있는가?	
사후관리	법적 요구사항 준수 검토	5	조직이 준수해야 하는 개인정보 및 정보보호 관련 법적 요구사항(법규명, 관련 조항, 세부내용 등)의 준수여부를 주기적(최소 연 1회 이상)으로 검토하고 있는가?	
	내부감사	6	정보보호 관리체계가 효과적으로 운영되는지 감사의 기준과 범위, 절차, 주기, 방법 등을 규정·준수하고 있는가?	추가
		7	내부감사 규정에 따른 주기로 감사를 수행하고 있는가?	추가

<표 3> 정보보호 정책의 보안점검 항목

통제분야	통제항목	점검항목		비고
정책의 승인 및 공표	정책의 승인	1	정보보호정책 제·개정 시 최고경영자의 승인을 받고 있는가?	
	정책의 공표	2	정보보호정책 및 정책시행 문서를 관련 임직원에게 이해하기 쉬운 형태로 전달하고 최신본으로 제공하고 있는가?	
정책의 유지관리	정책의 검토	3	정보보호정책 및 정책시행 문서의 정기적 타당성 검토 절차를 수립하고 있는가?	
	정책문서 관리	4	정보보호정책 및 정책시행 문서는 최신본으로 관리하고 있는가?	

입도 중요하지만, 각 조직 환경에 적합한 보안 지침을 수립·이행하는 것 또한 매우 중요하다. 따라서 기존 정보보호 관리체계 통제 분야에서 정책의 승인 및 공표와 유지관리 분야를 추출하였다. 이는 정보보호 정책의 제·개정 시 최고 경영자의 승인을 받고 임직원에게 공표하며 이는 정기적으로 타당성 검토를 받아 최신본으로 관리되는 것이 중요하다. 이를 정리하면 다음 <표 3>과 같다.

(3) 정보보호 조직의 점검항목

중소기업의 경우 정보보호 조직을 구성하기에는 열악한 환경을 가지고 있거나 그 필요성을 인식하지 못해 결성이 미비한 실정이다. 하지만 전문 조직을 통한 정보자산의 보호는 안정적인 기업 경영을 가능하게하기 때문에 대규모의 조직을 구성하기 어려운 중소기업의 특성을 반영하여 4가지 통제항목 중 정보보호위원회 통제항목을 삭제하고, 정보보호 최고책임자의 지정, 전문성 있는 구성원 임명 여부, 역할 및 책임에 대한 3가지 세부점검항목으로 축소하였다. 이를 정리하면 다음 <표 4>와 같다.

(4) 정보자산 분류의 점검항목

중소기업의 보유 기술들은 다양한 형태로 존재할 수 있으므로, 그 중요도에 따라 분류기준을 수립·식별·관리되어야 한다. 이를 위해 정보보호 관리체계의 3개의 통제항목과 4가지 세부점검항목을 그대로

적용하고, 다만 통제 분야 중 정보자산의 식별 여부를 점검하는 항목을 더 구체적으로 개선하여 추가하였다. 이를 정리하면 다음 <표 5>와 같다.

(5) 정보보호 교육의 점검항목

대부분 중소기업들의 정보보호 교육은 비정기적으로 수행되고 있으며, 교육훈련 실시 결과의 기록 및 관리적 측면의 문서화가 되어있지 않는 상태이다[27]. 특히 내부관계자에 의한 유출 건수가 높은 중소기업 기술정보의 유출은 사전예방이 우선이므로 정보보호 교육은 중소기업의 기술 유출 예방에 있어서 중요한 부분이라고 할 수 있다. 따라서 기존 정보보호 교육의 세부점검항목 중 정보보호 인식제고를 위한 홍보계획 수립 여부와 교육 및 훈련대상, 교육의 내용 그리고 정보보호 조직의 별도 교육 및 훈련 여부에 관한 항목을 구체적으로 개선 및 추가하였다. 이를 정리하면 다음 <표 6>과 같다.

(6) 인적보안의 점검항목

중소기업은 대기업에 비해 자금력과 기술력이 상대적으로 미흡한 현실이나 그에 반해 단순한 조직 형태로 인한 의사 결정의 신속성, 기동성, 비관료적, 뛰어난 기회 포착 등의 장점이 있다[28]. 즉 중소기업의 임직원들은 대부분 주요 기술정보자산에 접근이 가능한 인가자인 것이다. 하지만 이러한 장점은 점점 중소기업의 정보자산을 위협하는 주요 요인으로 작용하고 있다. 실제 대부분의 기업 정보 유출 사례들은 중소기업의 정보 보안이 외부에 의한 위협보다 내부인력에 대한 보안을 강화해야 한다는 것을 시사하고 있으므로 기존 정보보호 관리체계 인적보안 세부점검항목에 신규 채용자, 재직자, 퇴직자, 외부위탁업체 및 외부자 등의 제3자를 구분하여 정보보호서약서를 징구하고, 제3자의 경우 서약서 위반 시 처벌 규정에 관해 따로 명시해야한다는 항목을 추가하였다. 이를 정리하면 다음 <표 7>과 같다.

<표 4> 정보보호 조직의 보안점검 항목

통제분야	통제항목	점검항목		비고
조직 체계	정보보호 최고책임자 지정	1	최고경영자는 조직의 정보보호 관련 업무를 총괄 관리할 수 있는 임원급의 정보보호 최고책임자(CISO)를 지정하고 있는가?	
	실무조직 구성	2	정보보호 전문성을 고려하여 실무조직 구성원을 임명하고 있는가?	
역할 및 책임	역할 및 책임	3	정보보호 최고책임자와 정보보호 관련 담당자의 역할 및 책임을 정의하고 있는가?	

<표 5> 정보자산 분류의 보안점검 항목

통제분야	통제항목	점검항목		비고
정보자산 식별 및 책임	정보자산 식별	1	조직의 보유 기술을 조사하여 중요도에 따라 분류기준을 수립하고 식별하고 있는가?	추가
	정보자산별 책임할당	2	식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정하고 있는가?	
정보자산의 분류 및 취급	보안등급과 취급	3	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산의 중요도를 평가하기 위한 기준을 수립하고 있는가?	
		4	정보자산별로 중요도를 평가하고 각 자산별 특성에 적합한 보안등급 부여하고 보안등급을 쉽게 확인할 수 있도록 하고 있는가?	

<표 6> 정보보호 교육의 보안점검 항목

통제분야	통제항목	점검항목		비고
교육 프로그램 수립	교육 계획	1	정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호교육 계획을 수립하고 있는가?	
		2	정보보호 인식제고를 위한 홍보 계획을 수립하고 있는가?	추가
	교육 대상	3	정보보호 교육 및 훈련대상은 조직의 기술정보자산에 직·간접적으로 접근하는 임직원 및 외부자를 모두 포함하고 있는가?	개선
	교육 내용 및 방법	4	조직의 기술정보자산에 직·간접적으로 접근하는 임직원 및 외부자를 대상으로 한 기본 정보보호 교육 및 훈련에는 다음의 내용을 포함하고 있는가? - 정보보호의 필요성 - 정보보호 정책 - 보안 요구사항 - 정보보호 관련 법률 - 정보보안 사고 대응 방안 및 절차	개선
		5	정보보호 관리자, 정보보호 및 IT 전담부서 임직원은 정보보호와 관련하여 직무별 전문성 제고를 위하여 필요한 별도의 교육 및 훈련을 받고 있는가?	개선
교육 시행 및 평가	교육 시행 및 평가	6	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 기본 정보보호 교육을 수행하고 있는가?	
		7	임직원 및 외부자 신규 채용 계약 시, 업무 시작 전에 정보보호 교육을 시행하고 있는가?	

<표 7> 인적보안의 보안점검 항목

통제분야	통제항목	점검항목		비고
정보보호 책임	주요 직무자 지정 및 감독 직무 분리	1	조직 내 중요 정보자산(정보, 시스템 등)을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정하고 있는가?	
	비밀유지서약서	2	임직원에게서 정보보호 책임이 명시된 정보보호서약서를 받아 관리하고 있는가?	
		3	직원별로 구분하여 다음과 같은 사항이 명시된 정보보호서약서를 받고 있는가? 1. 신규 채용자, 재직자, 퇴직자 구분 2. 보안서약서 징구 3. 보안점검 실시 사항 4. 보안성과 평가, 포상, 징계 5. 단계적 퇴직 6. 이·취직 제한 합의서 징구 7. 이·취·퇴직 시 지급 물품 및 정보 반납 8. 퇴직자 관리 데이터 등록 및 관리	추가
		4	임시직원 혹은 외주용역과 같은 외부자에게 정보자산에 대한 접근권한을 부여할 경우, 정보보호에 대한 책임을 계약서에 명시하고 이에 대한 정보보호서약서를 받고 있는가?	
		5	외부위탁업체 및 외부자 등의 제3자 보안 관리를 위하여 계약서 및 보안서약서에 위반 시 처벌규정을 명시하고 있는가?	추가
인사규정	퇴직 및 직무변경 관리	6	조직 내 인력(정규직 임직원, 임시직원, 외주용역업체 직원 등)의 직무변경 혹은 퇴직 시 정보자산 반납, 접근권한 조정·회수, 결과 확인 등 수립된 절차에 따라 지체 없이 이행하고 있는가?	
	상벌규정	7	인사규정에 임직원이 정보보호 책임과 의무를 충실히 수행했는지 여부에 따른 상벌규정이 문서로 명시화 되어 있는가?	

(7) 물리적보안의 점검항목

중소기업청[29]에 따르면 중소기업의 기술유출 관계자의 83.4%가 '현·퇴직 임직원'이었으며, 기술유출 수단은 '복사 및 절취'가 전체 중 42.1%, 그리고 '핵심인력 스카우트 또는 매수'(36.0%), '휴대용 저장장치'(USB 등)(34.0%)의 순으로 높게 나타나고 있다. 이러한 특성을 반영하여 기존 정보보호 관리체계 항목 중 보호설비 항목에서 물리적 접근통제에 관한 세부점검항목을 추가하여 외부로부터의 침입과 내부자에 의한 유출을 예방하고자 한다. 이를 정리하면 다음 <표 8>과 같다.

(8) 암호통제의 점검항목

중소기업뿐만 아니라 정보유출에 있어서 ID 및 비밀번호의 공동 사용, 비밀번호 생성 규칙 미 준수, 특히 대량의 자료를 DB에 평문 형태로 저장되는 경우 등은 대표적인 보안 취약점이라고 할 수 있다. 하지만 이러한 취약점을 예방하기 위해 중소기업이 그 특성과 환경에 따라 모든 암호통제 점검항목들을 쉽게 적용하는 것은 힘들 수 있으므로 기본적인 암호 정책의 수립 및 점검 이행 여부를 항목을 개선 및 새롭게 추가하였다. 이를 정리하면 다음 <표 9>와 같다.

<표 8> 물리적보안의 보안점검 항목

통제분야	통제항목	점검항목		비고
물리적 보호구역	보호구역 지정	1	주요 설비 및 시스템을 보호하기 위하여 물리적 보호구역을 다음과 같이 정의하고 구역별 보호대책을 수립·이행하고 있는가? - 접견구역: 외부인접견구역 - 제한구역: 사무실 지역 등 - 통제구역: 주요정보처리설비 및 시스템구역 등	
	보호설비	2	각 보호구역의 중요도 및 특성에 따라 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립·관리하고 있는가?	
		3	CCTV System, 경비원, ID카드, 비밀번호 입력 도어, 생체인식 등의 접근통제 방안을 수립 및 이행하고 있는가?	추가
	출입통제	4	각 보호구역별 내·외부자 출입통제 절차를 마련하고 출입 가능한 임직원 현황을 관리하고 있는가?	
		5	각 보호구역에 대한 내·외부자 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가? - 업무목적에 적합한 출입권한 부여 - 절차에 따른 출입권한 부여 - 퇴직자 또는 직무변경자 출입권한 삭제·조정 및 출입증 회수 - 업무시간 외 출입 - 비인가자의 출입 시도 등	
	모바일기기 반출입	6	노트북, 패드 등 모바일 기기 반출입 시 반출입 통제 및 보안사고 예방 절차를 수립하고 있는가?	
사무실 보안	개인 업무 환경 보안	7	개인 업무 환경에서의 정보보호에 대한 정책을 수립·이행하고 있는가? - 자리이석 시 중요문서 및 저장매체 방치 금지 - 자리이석 시 컴퓨터 화면보호기 및 패스워드 설정 - 개인용 컴퓨터 보안 설정 -중요문서 파기 대책 등	
	공용업무 환경 보안	8	팩스, 복사기, 프린터, 공용 PC, 파일서버, 문서고 등 공용으로 사용하는 사무장비 및 시설에 대한 보호대책을 수립·이행하고 있는가?	

<표 9> 암호통제의 보안점검 항목

통제분야	통제항목	점검항목		비고
암호 정책	암호 정책 수립	1	서비스 이용자 및 내부 사용자(임직원 등)는 조직 내 중요정보의 전송 및 저장, 송·수신 및 비밀번호 저장 시 암호화 정책을 수립·이행하고 있는가?	추가
		2	정보유출에 대비하기 위한 암호 정책의 정기 점검이 이루어지고 있는가?	추가

<표 10> 접근통제의 보안점검 항목

통제분야	통제항목	점검항목		비고
접근통제 정책	접근통제 정책 수립	1	접근통제 영역을 정의하고 접근통제 영역별로 접근통제 정책을 수립·이행하고 있는가? -접근통제 영역 별 통제규칙, 방법, 절차 등 -예외사항에 대한 안전한 관리 절차 -공식적인 사용자 등록 및 해지 절차	추가
사용자 인증 및 식별	사용자 인증	2	기술정보에 대한 접근은 사용자 인증(ID와 비밀번호, 생체 인식 등), 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하고 있는가?	추가
	사용자 식별	3	기술정보가 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?	
	사용자 패스워드 관리	4	기술정보에 대한 안전한 사용자 패스워드 관리절차를 수립·이행하고 있는가?	
		5	패스워드 정책의 주요 내용은 다음과 같은 내용을 포함하고 있는가? -패스워드 최소길이, 변경 주기, 임계값 및 복잡도 설정 등 -중요도 및 심각도에 따른 세부적 관리 -채널 암호화 시스템(가상사설망, 암호화 통신 프로토콜 등) 도입 -응용 프로그램 암호화 시스템(웹,문서,전자우편,데이터베이스보안시스템) 도입	추가
접근통제 영역	네트워크 접근	6	접근통제 정책에 따라 분리된 네트워크 영역 간에 침입차단시스템 등을 통한 접근통제를 하고 있는가?	
	서버 접근	7	서버별로 접근이 허용된 사용자를 명확하게 식별·인증하고 안전한 접근수단을 적용하고 있는가?	
	응용 프로그램 접근	8	응용프로그램(웹, 문서, 전자우편, 데이터베이스 보안 시스템) 및 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 접근권한을 차등 부여하고 있는가?	추가
	데이터 베이스 접근	9	중요정보를 포함하고 있는 데이터베이스의 경우 데이터베이스 계정 또는 오브젝트(테이블, 뷰 또는 컬럼 등)수준에서 사용자 접근을 통제하고 있는가?	
	모바일 기기 접근	10	모바일기기에 대한 보안 통제 정책을 마련하고 이에 따라 이행하고 있는가? -모바일기기 허용기준 -모바일기기를 통한 업무사용 범위 -모바일기기 사용 시 승인절차 및 방법 -모바일기기 인증(MAC인증 등) -모바일기기 이용에 따른 보안설정 정책 및 오남용 모니터링대책	
	인터넷 접속	11	인터넷 PC와 내부 업무용 PC를 분리하고 있는 경우 PC간의 자료전송을 통제하고 있는가?	

<표 11> 운영보안의 보안점검 항목

통제분야	통제항목	점검항목		비고
운영절차 및 변경 관리	운영절차 수립	1	조직 내 기술보호 문제에 대한 진단과 평가를 바탕으로 정보시스템 운영을 위한 운영절차(또는 매뉴얼)를 수립하고 있는가?	추가
시스템 및 서비스 운영 보안	보안 시스템운영	2	조직에서 운영하고 있는 보안시스템 운영절차를 수립하고 있는가?	
		3	다음과 같은 보안 시스템을 포함하여 운영하고 있는가? - 메일, 메신저 보안 - 통합보안시스템, 문서보안 등 - DB 보안 - 네트워크 보안 시스템(침입차단, 침입탐지, 바이러스 등)	추가
	백업관리	4	백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립·이행하고 있는가?	
		5	수립된 백업 및 복구절차에 따라 정기적인 관리, 백업과 테스트를 시행하고 있는가?	추가
매체 보안	휴대용 저장매체 관리	6	주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 휴대용 저장매체 사용을 제한하고 있는가?	
악성코드 관리	악성코드 통제	7	백신프로그램 등을 통한 최신 악성코드 예방, 탐지 활동을 지속적으로 수행하고 있는가?	
	패치관리	8	서버, 네트워크 장비, 보안시스템, PC 등 자산 중요도 또는 특성에 따라 OS, 소프트웨어 패치관리 정책 및 절차를 수립·이행하고 있는가?	
로그관리 및 모니터링	침해시도 모니터링	9	외부로부터의 침해시도가 의심되는 이상 징후를 지체 없이 인지할 수 있도록 모니터링 체계 및 절차를 수립하고 있는가?	

<표 12> 침해사고 관리의 보안점검 항목

통제분야	통제항목	점검항목		비고
절차 및 체계	침해사고 대응절차수립	1	기술유출사고 대응절차가 수립되어 있고 대응절차에는 다음과 같은 사항을 포함하고 있는가? -기술유출사고의 정의 및 범위(중요도 및 유형포함) -긴급 연락체계 구축 -담당 조직 비상연락체계 -기술유출사고 대응절차 -기술유출사고 복구조직의 구성 및 책임, 역할 -재발방지 대책 이행 및 관리	추가
	침해사고 대응체계 구축	2	침해사고가 유형 및 중요도에 따라 분류되어 있고 이에 따른 보고체계를 정의하고 있는가?	
대응 및 복구	침해사고 훈련	3	침해사고 대응절차에 관한 모의훈련계획을 수립하고 이에 따라 주기적으로 훈련을 실시하고 있는가?	
	침해사고 처리 및 복구	4	침해사고가 발생한 경우 절차에 따라 처리 및 복구를 수행하고 그 기록을 남기고 있는가? -처리 및 복구일시 -담당자 -처리 및 복구방법 -처리 및 복구수행 경과내용(예: 시작부터 종료까지 시간순으로 작성)	
사후관리	침해사고 분석 및 공유	5	침해사고가 종결된 후 사고의 원인을 분석하고 그 결과를 보고하고 있는가?	

(9) 접근통제의 점검항목

장상수 외[30]의 연구에 따르면 정보보호관리체계에 있어서 2007~2009년 동안 주요 패스워드 관리 미흡으로 인한 결함건수가 결함건수의 25~30%를 차지했다. 따라서 본 연구는 접근통제 정책 분야의 항목을 수정하고, 사용자 패스워드 관리 항목을 추가하였다. 또한 세부항목 간소화를 통해 중소기업의 이행이 용이하도록 하였다. 이를 정리하면 다음 <표 10>과 같다.

(10) 운영보안의 점검항목

중소기업의 운영보안은 보안대책을 효율적으로 운영하기 위해 보안 시스템의 운영 절차 수립부터 침해시도 모니터링까지 총 7개의 통제항목과 9개의 세부점검 항목을 개선 및 추가하였다. 이를 정리하면 다음 <표 11>과 같다.

(11) 침해사고 관리의 점검항목

보안사고의 정의, 대응절차 수립, 복구 절차 등의 관리를 위해 정보보호 관리체계 에서는 7개의 통제항목과 14개의 세부점검항목을 제시하고 있다. 본 논문에서는 중소기업의 용이한 수행을 위하여 침해사고 대응절차 수립 항목의 개선된 세부점검항목을 포함하여 5개의 통제항목과 세부점검항목을 제시하고 있다. 이를 정리하면 다음 <표 12>와 같다.

Ⅳ. 정보보호 관리체계 기반의 중소기업 기술보호 개선안 검증

정보보호관리체계를 기반으로 한 중소기업의 기술보호 지침 개선을 위해 본 논문에서는 정보보호관리체계의 점검 항목과 추가로 도출한 항목들의 적합성을 검증 하고자 한다. 이를 위해 중소기업에서 근무하는 임직원들을 대상으로 설문을 실시하였다.

4.1 설문조사 방법과 표본응답자 구성

4.1.1 설문조사 방법

설문기간은 2016년 4월 30일 ~ 2016년 7월 7일까지 설문을 위한 부가적인 설명과 함께 온라인으로 진행되었으며 총 42명이 응답하였다.

4.1.2 표본응답자 구성

설문조사 대상으로는 <표 13>과 같이 선정하였으며, 담당 업무는 운영/개발(28.57%), 보안(23.81%), 영업(14.29%), 경영/관리(14.29%), 교육/정책(11.9%), 생산(7.14%)으로 구성되었다.

<표 13> 표본 응답자의 구성

구분	운영/개발	보안	영업	경영/관리	교육/정책	생산
비율	12명 (28.57%)	10명 (23.81)	6명 (14.29%)	6명 (14.29%)	5명 (11.9%)	3명 (7.14%)

4.2 설문결과

4.2.1 표본집단의 특성에 관한 설문 결과

(1) 응답자의 직무경력 및 기술(정보)보호 경력에 대한 설문결과

설문 응답자의 직무경력에 대한 질문은 3년 이하, 3년 이상~7년 이하, 7년 이상~10년 이하, 10년 이상~15년 이하, 15년 이상으로 구분하였고 다음 <표 14>와 같이 응답 하였다. 또한 설문 응답자의 기술(정

보)보호 경력에 대한 질문은 없음, 3년 미만, 3~5년 미만, 5~10년 미만, 10년 이상으로 구분하였으며 다음 <표 15>와 같이 응답 하였다.

<표 14> 설문 응답자의 직무 경력

구분	없음	3년 미만	3~5년 미만	5~10년 미만	10년 이상
비율	15명 (35.71%)	12명 (28.57%)	6명 (14.29%)	5명 (11.9%)	4명 (9.52%)

<표 15> 설문 응답자의 기술(정보)보호 경력

구분	없음	3년 미만	3~5년 미만	5~10년 미만	10년 이상
비율	15명 (35.71%)	12명 (28.57%)	6명 (14.29%)	5명 (11.9%)	4명 (9.52%)

(2) 정보보호관리체계 및 정보유출 피해 경험, 보호조치 필요성에 대한 설문결과

중소기업의 기술보호 개선 방안을 위해 본 논문에서 도출한 항목의 적합성 여부 판정에 앞서, 설문 응답자들의 정보보호관리체계의 수행 여부와 정보유출 피해 경험, 보호조치 필요성 인식에 대해 알아보기 위하여 첫째, 정보보호관리체계의 운영 및 평가 수행 경험 여부에 대한 질문, 둘째, 정보 유출 피해 경험에 대한 질문, 셋째, 기술(정보)보호 개선의 필요 여부에 대한 질문으로 총 3개의 질문을 구성 하였다.

설문 응답자 중 정보보호관리체계의 운영 및 평가 수행 경험 여부에 대해서는 27명이 “아니오”라고 답하였으며, 정보 유출 피해 경험에 대해서는 35명이 “없음”이라고 답하였다. 또한 중소기업의 기술보호 개선을 고려한 보호조치의 필요 여부에 대한 질문은 33명이 필요하다”고 응답하였다.

4.2.2 상세 지침항목의 적합성 검증 설문결과

본 논문에서는 중소기업의 기술보호 개선과 관련

<표 16> 정보보호관리체계의 운영 및 평가 수행 경험

구분	예	아니오
비율	15명 (35.71%)	27명 (64.29%)

<표 17> 정보 유출 피해 경험

구분	내부자(퇴직자, 외주업체, 협력업체 등)	외부자(방문자, 스카우트, 해킹 등)	피해경험 없음
비율	4명 (9.52%)	3명 (7.14%)	35명 (83.33%)

<표 18> 중소기업의 기술보호 개선을 고려한 보호조치의 필요 여부

구분	필요하다	필요하지 않다
비율	33명 (78.57%)	9명 (21.43%)

하여 정보보호관리체계 수립 시 보안성을 보장하기 위해 11개의 통제항목을 도출하였다. 도출된 통제항목의 세부 점검 항목 적합성을 검증한 설문 결과는 다음과 같다.

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 정보보호 관리과정의 7개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 최상위 수준의 정보보호정책 존재 여부에 관한 항목에서 92.85%, 권한 위임자의 의사결정 참여에 관한 항목에서 88.09%, 최고경영자의 정보보호관리체계 예산 및 인력 승인에 관한 항목에서 83.33%, 위험관리 계획의 수립 및 이행에 관한 항목에서 83.33%, 정보보호 관련 법 준수 여부의 검토에 관련한 항목에서 85.72%, 정보보호관리체계 감사 준수 여부에 관련한 항목에서 88.09%, 주기적 내부감사 수행에 관련한 항목에서 85.71%의 적합 판정을 받았다. 이를 정리하면 다음 <표 19>와 같다.

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 정보보호 정책의 4개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과

<표 19> 중소기업의 기술보호 지침 개선 시
정보보호 관리과정의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	2명 (4.76%)	14명 (33.33%)	12명 (28.57%)	13명 (30.95%)
2	1명 (2.38%)	4명 (9.52%)	11명 (26.19%)	12명 (28.57%)	14명 (33.33%)
3	1명 (2.38%)	6명 (14.29%)	12명 (28.57%)	12명 (28.57%)	11명 (26.19%)
4	1명 (2.38%)	6명 (14.29%)	15명 (35.71%)	11명 (26.19%)	9명 (21.43%)
5	0명 (0%)	6명 (14.29%)	10명 (23.81%)	17명 (40.48%)	9명 (21.43%)
6	0명 (0%)	5명 (11.9%)	15명 (35.71%)	15명 (35.71%)	7명 (16.67%)
7	2명 (4.76%)	4명 (9.52%	10명 (23.81%)	14명 (33.33%)	12명 (28.57%)

반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 최고경영자의 정보보호 정책 승인과 관련한 항목에서 90.48%, 정보보호 정책 및 정책시행 문서의 최신본 제공과 관련한 항목에서 85.71%, 정보보호 정책 및 정책시행 문서의 정기적인 타당성 검토 절차 수립과 관련한 항목에서 88.09%, 정보보호 정책 및 정책시행 문서의 최신본 관리와 관련한 항목에서 83.33%의 적합 판정을 받았다. 이를 정리하면 다음 <표 20>과 같다.

<표 20> 중소기업의 기술보호 지침 개선 시
정보보호 정책의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	3명 (7.14%)	11명 (26.19%)	16명 (38.1%)	11명 (26.19%)
2	1명 (2.38%)	5명 (11.9%)	11명 (26.19%)	14명 (33.33%)	11명 (26.19%)
3	1명 (2.38%)	4명 (9.52%)	13명 (30.95%)	12명 (28.57%)	12명 (28.57%)
4	1명 (2.38%)	6명 (14.29%)	13명 (30.95%)	9명 (21.43%)	13명 (30.95%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 정보보호 조직의 3개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 정보보호최고책임자(CISO)의 지정 여부와 관련한 항목에서 83.33%, 정보보호 전문성을 고려한 실무조직 구성원의 임명에 관련한 항목에서 85.71%, 정보보호최고책임자와 정보보호 관련 담당자의 역할 및 책임 정의에 관련한 항목에서 83.33%의 적합 판정을 받았다. 이를 정리하면 다음 <표 21>과 같다.

<표 21> 중소기업의 기술보호 지침 개선 시
정보보호 조직의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	2명 (4.76%)	5명 (11.9%)	12명 (28.57%)	10명 (23.81%)	13명 (30.95%)
2	1명 (2.38%)	5명 (11.9%)	12명 (28.57%)	12명 (28.57%)	12명 (28.57%)
3	2명 (4.76%)	5명 (11.9%)	12명 (28.57%)	11명 (26.19%)	12명 (28.57%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 정보자산 분류의 4개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 중요도에 따른 정보자산 분류 기준 수립 및 식별에 관련한 항목에서 88.09%, 식별된 정보자산에 대한 담당자 지정에 관련한 항목에서 88.1%, 정보자산 중요도 평가 기준 수립에 관련한 항목에서 80.95%, 정보자산 별 중요도 평가와 특성에 따른 보안등급 부여에 관련한 항목에서 85.71%의 적합 판정을 받았다. 이를 정리하면 다음 <표 22>와 같다.

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 정보보호 교육의 7개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과

<표 22> 중소기업의 기술보호 지침 개선 시 정보자산 분류의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	4명 (9.52%)	12명 (28.57%)	15명 (35.71%)	10명 (23.81%)
2	1명 (2.38%)	4명 (9.52%)	11명 (26.19%)	17명 (40.48%)	9명 (21.43%)
3	1명 (2.38%)	7명 (16.67%)	10명 (23.81%)	15명 (35.71%)	9명 (21.43%)
4	1명 (2.38%)	5명 (11.9%)	11명 (26.19%)	13명 (30.95%)	12명 (28.57%)

반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 연간 정보보호교육 계획 수립에 관련한 항목에서 83.33%, 정보보호 홍보 계획 수립에 관련한 항목에서 78.57%, 정보보호 교육 및 훈련 대상에 관련한 항목에서 83.33%, 정보보호 교육 및 훈련의 내용에 관련한 항목에서 83.33%, 정보보호 관리자, 전담 부서 임직원의 교육 및 훈련에 관련한 항목에서 88.09%, 정보보호관리체계 범위 내 임직원 및 외부자를 대상으로 한 교육 수행에 관련한 항목에서 88.03%, 임직원 및 외부자 신규 채용 계약 시 정보보호 교육 시행에 관련한 항목에서 83.33%의 적합 판정을 받았다. 이를 정리하면 다음 <표 23>과 같다.

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 인적보안의 7개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 정보자산 취급 직무자의 지정에 관련한 항목에서 90.48%, 임직원의 정보보호서약서에 관련한 항목에서 83.34%, 정보보호서약서의 내용과 관련한 항목에서 83.33%, 정보자산에 대한 접근권한 부여 시 정보보호서약서 제출에 관한 항목에서 83.33%, 제3자를 위한 보안 서약서의 처벌 규정 명시에 관련한 항목에서 88.09%, 조직 내 인력의 직무 변경 또는 퇴직

<표 23> 중소기업의 기술보호 지침 개선 시 정보보호 교육의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	3명 (7.14%)	4명 (9.52%)	13명 (30.95%)	11명 (26.19%)	11명 (26.19%)
2	1명 (2.38%)	8명 (19.05%)	15명 (35.71%)	6명 (14.29%)	12명 (28.57%)
3	1명 (2.38%)	6명 (14.29%)	11명 (26.19%)	13명 (30.95%)	11명 (26.19%)
4	1명 (2.38%)	6명 (14.29%)	13명 (30.95%)	11명 (26.19%)	11명 (26.19%)
5	1명 (2.38%)	4명 (9.52%)	12명 (28.57%)	11명 (26.19%)	14명 (33.33%)
6	2명 (4.76%)	5명 (11.9%)	10명 (23.81%)	10명 (23.81%)	15명 (35.71%)
7	1명 (2.38%)	6명 (14.29%)	11명 (26.19%)	11명 (26.19%)	13명 (30.95%)

시 정보자산의 반납 등에 관련한 항목에서 85.71%, 정보보호 상벌규정의 문서 명시화에 관련한 항목에서 85.71%의 적합 판정을 받았다. 이를 정리하면 다음 <표 24>와 같다.

<표 24> 중소기업의 기술보호 지침 개선 시 인적보안의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	3명 (7.14%)	10명 (23.81%)	16명 (38.1%)	12명 (28.57%)
2	1명 (2.38%)	6명 (14.29%)	9명 (21.43%)	10명 (23.81%)	16명 (38.1%)
3	1명 (2.38%)	6명 (14.29%)	9명 (21.43%)	13명 (30.95%)	13명 (30.95%)
4	1명 (2.38%)	6명 (14.29%)	9명 (21.43%)	13명 (30.95%)	13명 (30.95%)
5	1명 (2.38%)	4명 (9.52%)	10명 (23.81%)	12명 (28.57%)	15명 (35.71%)
6	1명 (2.38%)	5명 (11.9%)	9명 (21.43%)	14명 (33.33%)	13명 (30.95%)
7	1명 (2.38%)	5명 (11.9%)	13명 (30.95%)	11명 (26.19%)	12명 (28.57%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 물리적보안의 8개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 물리적 보호 대책의 수립 및 이행에 관련한 항목에서 83.33%, 보호구역의 중요도 및 특성에 따른 필요 설비와 운영절차의 수립 및 관리에 관련한 항목에서 83.33%, 접근통제 방안의 수립 및 이행에 관련한 항목에서 90.47%, 보호구역별 출입통제 절차의 마련과 출입가능 임직원 현황관리에 관련한 항목에서 83.33%, 내·외부자 출입 기록의 보존과 출입권한의 주기적 검토에 관련한 항목에서 90.47%, 모바일 기기의 반·출입 시 통제 및 보안사고 예방 절차의 수립에 관련한 항목에서 83.33%, 개인 업무 환경에서의 정보보호 정책 수립 및 이행에 관련한 항목에서 83.33%, 공용 사무장비 및 시설에 대한 보호대책의 수립 및 이행과 관련한 항목에서 80.95%의 적합 판정을 받았다. 이를 정리하면 다음 <표 25>와 같다.

<표 25> 중소기업의 기술보호 지침 개선 시 물리적보안의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	6명 (14.29%)	8명 (19.05%)	14명 (33.33%)	13명 (30.95%)
2	1명 (2.38%)	6명 (14.29%)	11명 (26.19%)	11명 (26.19%)	13명 (30.95%)
3	2명 (4.76%)	2명 (4.76%)	10명 (23.81%)	15명 (35.71%)	13명 (30.95%)
4	2명 (4.76%)	5명 (11.9%)	11명 (26.19%)	11명 (26.19%)	13명 (30.95%)
5	2명 (4.76%)	2명 (4.76%)	14명 (33.33%)	14명 (33.33%)	10명 (23.81%)
6	2명 (4.76%)	5명 (11.9%)	14명 (33.33%)	8명 (19.05%)	13명 (30.95%)
7	1명 (2.38%)	6명 (14.29%)	11명 (26.19%)	15명 (35.71%)	9명 (21.43%)
8	1명 (2.38%)	7명 (16.67%)	10명 (23.81%)	14명 (33.33%)	10명 (23.81%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 암호통제의 2개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 기업 서비스 이용자 및 내부 사용자의 암호화 정책 수립 및 이행에 관련한 항목에서 76.19%, 암호 정책의 정기점검 수행 여부에 관련한 항목에서 71.43%의 적합 판정을 받았다. 이를 정리하면 다음 <표 26>과 같다.

<표 26> 중소기업의 기술보호 지침 개선 시 암호통제의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	3명 (7.14%)	7명 (16.67%)	9명 (21.43%)	11명 (26.19%)	12명 (28.57%)
2	1명 (2.38%)	11명 (26.19%)	9명 (21.43%)	8명 (19.05%)	13명 (30.95%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 접근통제의 11개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 접근통제 영역의 정의와 정책 수립 및 이행에 관련한 항목에서 83.33%, 사용자 인증 절차 통제에 의한 기술정보 접근에 관련한 항목에서 80.95%, 기술정보의 사용자 구분에 관련한 항목에서 88.09%, 사용자 패스워드 관리절차의 수립 및 이행에 관련한 항목에서 88.09%, 패스워드 정책의 주요 내용과 관련한 항목에서 83.33%, 네트워크 영역 간 접근통제에 관련한 항목에서 90.47%, 서버별 허용된 사용자의 명확한 식별·인증과 안전한 접근수단의 적용에 관련한 항목에서 90.48%, 사용자의 업무에 따른 접근권한 차등 부여에 관련한 항목에서 88.09%, 데이터베이스 계정 또는 오브젝트 수준에서의 사용자 접근 통제에 관련한 항목

에서 88.09%, 모바일기기에 대한 보안 통제 정책의 수립 및 이행에 관련한 항목에서 80.95%, PC간의 자료 전송 통제에 관련한 항목에서 76.19%의 적합 판정을 받았다. 이를 정리하면 다음 <표 27>과 같다.

<표 27> 중소기업의 기술보호 지침 개선 시 접근통제의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	6명 (14.29%)	11명 (26.19%)	11명 (26.19%)	13명 (30.95%)
2	1명 (2.38%)	7명 (16.67%)	9명 (21.43%)	11명 (26.19%)	14명 (33.33%)
3	1명 (2.38%)	4명 (9.52%)	15명 (35.71%)	10명 (23.81%)	12명 (28.57%)
4	1명 (2.38%)	4명 (9.52%)	11명 (26.19%)	11명 (26.19%)	15명 (35.71%)
5	1명 (2.38%)	6명 (14.29%)	9명 (21.43%)	13명 (30.95%)	13명 (30.95%)
6	1명 (2.38%)	3명 (7.14%)	12명 (28.57%)	14명 (33.33%)	12명 (28.57%)
7	1명 (2.38%)	3명 (7.14%)	12명 (28.57%)	10명 (23.81%)	16명 (38.1%)
8	0명 (0%)	5명 (11.9%)	12명 (28.57%)	12명 (28.57%)	13명 (30.95%)
9	1명 (2.38%)	4명 (9.52%)	11명 (26.19%)	13명 (30.95%)	13명 (30.95%)
10	1명 (2.38%)	7명 (16.67%)	13명 (30.95%)	11명 (26.19%)	10명 (23.81%)
11	0명 (0%)	10명 (23.81%)	8명 (19.05%)	14명 (33.33%)	10명 (23.81%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 운영보안의 9개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부적으로 확인해보면 정보시스템 운영절차의 수립에 관련한 항목에서 80.95%, 보안시스템 운영절차의 수립에 관련한 항목에서 88.09%, 보안시스템 운영의 내용에 관련한 항목에서 80.95%, 백업 및 복구절차의 수립 및 이행에 관련한 항목에서 85.71%, 수립된 백업 및 복구절차에 따른 정기적 관리와 테스트 시행에 관련한 항목에서 85.71%, 통제구역, 제한구역 등에서의 휴대용 저장매체 사용 제한에 관련한 항목에서 83.33%, 백신프로그램의 지속적 사용에 관련한 항목에서 88.09%, OS, 소프트웨어 패치관리 정책 및 절차의 수립 및 이행에 관련한 항목에서 88.09%, 외부로부터의 침해시도 또는 이상 징후에 대한 모니터링 체계 및 절차 수립에 관련한 항목에서 80.95%의 적합 판정을 받았다. 이를 정리하면 다음 <표 28>과 같다.

<표 28> 중소기업의 기술보호 지침 개선 시 운영보안의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	7명 (16.67%)	7명 (16.67%)	13명 (30.95%)	14명 (33.33%)
2	1명 (2.38%)	4명 (9.52%)	10명 (23.81%)	14명 (33.33%)	13명 (30.95%)
3	1명 (2.38%)	7명 (16.67%)	12명 (28.57%)	9명 (21.43%)	13명 (30.95%)
4	1명 (2.38%)	5명 (11.9%)	11명 (26.19%)	14명 (33.33%)	11명 (26.19%)
5	1명 (2.38%)	5명 (11.9%)	10명 (23.81%)	14명 (33.33%)	12명 (28.57%)
6	1명 (2.38%)	6명 (14.29%)	10명 (23.81%)	15명 (35.71%)	10명 (23.81%)
7	1명 (2.38%)	4명 (9.52%)	12명 (28.57%)	13명 (30.95%)	12명 (28.57%)
8	1명 (2.38%)	4명 (9.52%)	11명 (26.19%)	13명 (30.95%)	13명 (30.95%)
9	1명 (2.38%)	7명 (16.67%)	10명 (23.81%)	11명 (26.19%)	13명 (30.95%)

정보보호관리체계 기반의 중소기업의 기술보호 개선 수행과 관련하여 도출한 침해사고 관리의 5개 세부 점검 항목에 대한 적합성 검증은 모든 항목이 과반수로 보통 이상으로 적합하다고 응답하였다. 세부

적으로 확인해보면 기술유출사고 대응절차의 수립과 내용에 관련한 항목에서 76.19%, 침해사고의 분류 및 이에 따른 보고체계 정의에 관련한 항목에서 83.33%, 침해사고 대응절차에 관한 모의훈련계획의 수립과 실시에 관련한 항목에서 76.19%, 침해사고 처리 및 복구 수행과 그 기록에 관련한 항목에서 78.58%, 침해사고 원인 분석과 결과 보고에 관련한 항목에서 80.95%의 적합 판정을 받았다. 이를 정리하면 다음 <표 29>와 같다.

<표 29> 중소기업의 기술보호 지침 개선 시 침해사고 관리의 세부 점검 항목 적합성 검증

점검항목	적합성평가				
	매우 부적합	부적합	보통	적합	매우적합
1	1명 (2.38%)	9명 (21.43%)	10명 (23.81%)	12명 (28.57%)	10명 (23.81%)
2	1명 (2.38%)	6명 (14.29%)	13명 (30.95%)	11명 (26.19%)	11명 (26.19%)
3	1명 (2.38%)	9명 (21.43%)	9명 (21.43%)	12명 (28.57%)	11명 (26.19%)
4	2명 (4.76%)	7명 (16.67%)	9명 (21.43%)	16명 (38.1%)	8명 (19.05%)
5	2명 (4.76%)	6명 (14.29%)	9명 (21.43%)	14명 (33.33%)	11명 (26.19%)

Ⅴ. 결론 및 향후 연구과제

5.1 결론

본 연구는 정보보호관리체계의 구성 항목들을 이용하여 중소기업의 기술 보호 개선 방안을 연구하고자 하였다. 그리고 이를 통해 중소기업 기술보호에서의 효과적이고 효율적인 정보 보안 방안을 논의하고자 하였다. 즉, 중소기업에 대한 명확한 분석을 통해 정보보호 방안에 대해 논의하고 이를 통해 중소기업 정보 유출의 주요 특성들을 살핀 후 정보보호관리체계를 적용시켜 지소적인 기술보호를 유도할 수 있는 개선방안을 제시하고자 하였다. 이를 위해 정보보호 관리체계를 기반으로 각 단계에서 필요한 중소기업 정보 보호 점검 항목을 설계하였으며 본 논문을 실증 검증하기 위한 설문조사는 중소기업에서 근무하고 있는 임직원들을 대상으로 실시하였다.

연구결과 중소기업 정보보호 관리체계의 정보보호 관리과정 5개의 분야 중 정보보호대책 구현을 제외한 4개 분야의 7개의 세부관리과정과 정보보호 대책의 13개 분야 중 외부자 보안, 시스템 개발 보안, IT 재해복구를 제외한 10개의 통제항목과 60개의 세부점검 항목이 대부분 “보통이다”라고 나타났다. 이는 중소기업 정보보호가 임직원들이 생각하기에 개선방안이 필요하긴 하나 전사적으로 정보보호를 개선하기가 어렵다는 것을 확인할 수 있다.

중소기업청(2007)[31]에 따른 대표적인 중소기업의 기술유출 사례의 유형을 구분해보면 첫째, 전·현직 현지(외국인 고용) 직원에 의해 새로 개발 중인 핵심 기술이 유출된 사례가 있다. A사에서 근무하는 외국인 기술훈련생 B는 실력을 인정받아 A사의 부설연구소에서 프로젝트 연구개발에 참여할 수 있게 되었는데, 몇 달 뒤 어머니가 위독하시다는 핑계로 휴가를 내고 모국으로 돌아갔다. 그 후 A사는 나중이 되어서야 B가 자국 업체에 A사의 핵심기술 노하우를 넘긴 사실을 알게 되었다.

둘째, 경쟁업체 종사자에 의한 유출 사례가 있다. 주차장 내 자동승강기 로봇을 개발하는 C사의 생산공장에 외부인이 무단 침입하여 로봇 사진을 찍고 달아났으며, 수소문 끝에 유출된 로봇 사진을 회수하였으나 이미 경쟁업체에 설계 도면이 넘어간 후였다. 경쟁업체는 세부 설비구조만 조금씩 변형시키는 방법으로 관련 처벌규정을 피해가면서 유사제품을 제작 및 판매하였다.

셋째, 특히 대-중소기업간 기술유출 사례가 있다.

중소기업 D사가 개발한 휴대폰 비상알림 서비스 기술을 대기업 E사가 탈취하여 D사는 특허무효심판에 대해 승소하였으나 손해배상청구소송에서 패소하여 사옥매각, 수출계약 파기, 핵심연구인력 이직 등 경제적으로 막대한 피해가 발생하기도 하였다. 또한 대기업과 중소기업은 거래를 통해 기술자료를 공유하는 부분에서 정보가 유출될 수도 있다. 따라서 중소기업은 기술자료 임치제도를 도입하는 것도 좋은 방안이 될 것이다. 기술자료 임치제도는 거래관계에 있는 대기업과 중소기업이 일정한 조건하에 서로 합의하여 핵심 기술자료를 신뢰성 있고 임치설비를 갖춘 대·중소기업협력재단에서 보관함으로써, 중소기업은 기술유출 위험을 줄일 수 있고 대기업은 해당 중소기업의 파산·폐업 시 임치물을 이용하여 관련기술을 안전하게 활용 할 수 있도록 하는 제도이다(대·중소기업협력재단, 2013) 이를 통해 대·중소기업간 기술자료 보호를 통해 상호 간 공동 자료 공유 및 신뢰를 높일 수 있는 방안으로 가야할 것이다. 또한 주별로 보안상황을 점검하고 분기별로 중소기업 정보보호를 개선할 수 있는 평가가 도입이 되어야 할 것이다.

본 연구의 학문적, 실무적 시사점은 다음과 같다. 본 연구에서는 중소기업의 특성을 기준으로 정보보호관리체계에 대한 연구를 수행했다는 점에서 학문적 기여도가 크다고 할 수 있다. 그리고 실무적 시사점으로 중소기업들은 중소기업의 특성을 고려한 점검항목으로 정보보호관리체계 참여율을 크게 높여 중소기업의 기술 유출 피해를 방지할 수 있을 것이다.

5.2 향후 연구 과제

본 연구의 의의와 한계점, 추후 연구방향은 다음과 같다. 본 연구는 첫째, 표본 응답자의 수가 많이 부족하였다. 향후 연구에서는 응답자의 수를 높여 폭넓은 연구를 진행할 필요가 있다. 또한 심층면접, 인터뷰 등을 활용하여 연구결과의 타당성 및 신뢰성을 향상시켜야 할 것이다. 둘째, 중소기업의 업종별 특성을 고려한 세심한 연구가 필요하다. 업종별로 어떤 기술정보를 다루고 있는지, 이러한 기술정보의 보호는 어떤 부분을 특별히 신경써야하는지 그 특성을 다루지 못하였다. 향후 연구에서는 첫째, ISMS에 맞게 중소기업 기술보호 할 수 있는 인증 시스템 개발과 DRM 인증 설계가 필요하다[32-34] 둘째, 정보기술 업종별 각 특성을 연구하여 효율적인 중소기업 기술보호 개선방안 연구가 이루어져야 할 것이다.

참고문헌

[1] 박경태·김세헌, “ISMS 인증 기대 요인 및 인증 의도에 관한 연구,” 한국정보보호학회, 정보보호학회논문지, 제25권, 제2호, 2015, pp. 375-381.

[2] 조용현, “ISMS 인증시 결함요소에 대한 관리체계 수립 방안,” 건국대학교 석사학위논문, 2010.

[3] 최재훈, “정보보호 관리체계를 이용한 그린 데이터센터 운영 보안지침 개선방안의 연구,” 건국대학교 석사학위논문, 2015.

[4] 한국인터넷진흥원, “ISMS 사업추진현황 소개,” 2015.

[5] 조중기, “정보보호 관리체계(Information Security Management System)인증 취득 후 기업가치의 변화에 관한 연구,” 충북대학교 석사학위논문, 2016.

[6] 정대령·정회경, “전자정부 정보보호관리체계(G-ISMS)를 활용한 공공기관 정보보호 거버넌스 수립방안에 관한 연구,” 배재대학교 석사학위논문, 2013.

[7] 유승한·정대령·정회경, “전자정부 정보보호관

리체계(G-ISMS)를 활용한 공공기관 정보보호 거버넌스 수립방안," 한국정보통신학회, 한국정보통신학회논문지, 제17권, 제4호, 2013, pp. 769-774.

[8] 김지숙・이수연・임종민, "민간기업 공공기관의 정보보호 관리체계 차이 비교," 한국정보보호학회, 정보보호학회논문지, 제20권, 제2호, 2010, pp. 117-129.

[9] 추연철・최진영, "스마트 모바일 오피스 환경에서의 정보보호관리체계 (ISMS)를 확장한 정보보호모형 연구," 한국정보과학회, 학술발표논문집 (B), 제37권, 2B호, 2010, pp. 95-99.

[10] 장상수・김상춘, "정보보호 관리체계(ISMS)가 기업성과에 미치는 영향에 관한 실증적 연구," 한국융합보안학회, 정보・보안논문지, 제15권, 제3호, 2015, pp. 105-112.

[11] 고유찬, "정보보호 관리체계 (ISMS) 인증제도의 개선을 위한 연구 : 통제항목의 탄력적 적용," 동국대학교 석사학위논문, 2014.

[12] 배영식, "정보보호관리체계[ISMS] 인증이 조직성과에 미치는 영향에 관한 연구," 한국산학기술학회, 한국산학기술학회논문지, 제13권, 제9호, 2012, pp. 4224-4233.

[13] Capon, N. and R. Glazer, "Marketing and Technology : A Strategic Coalignment," Journal of Marketing, Vol. 51, 1987, pp. 1-14.

[14] 변병문, "기술가치평가기법에 대한 검토 및 새로운 제안," 한국기술혁신학회, 한국기술혁신학회 2002년도 추계학술대회, 2002, pp. 263-276.

[15] 김경선, "기술보호활동이 기업성과에 미치는 영향에 관한 실증연구," 성균관대학교 박사학위논문, 2016.

[16] 장항배, "중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계," 한국멀티미디어학회, 한국멀티미디어학회논문지, 제13권, 제1호, 2010, pp. 111-121.

[17] 정재승, "중소기업 기술유출 및 기술인력 방지제도에 관한 연구," 한국통상정보학회, 통상정보연구, 제17권, 제3호, 2015, pp. 133-152.

[18] 국신욱, "중소기업 기술유출 방지를 위한 법제 연구," 한국지식재산학회, 산업재산권, 제46호, 2015, pp. 201-239.

[19] 이장훈・신완선・박현주, "중소기업 기술보호 개선방안에 대한 연구," 한국산업경영시스템학회, 산업경영시스템학회지, 제37권, 제2호, 2014, pp. 77-84.

[20] 김기호・하규수, "신정보화 환경에서 중소기업 기술유출에 대한 인식과 관리 실태에 관한 연구," 한국디지털정책학회, 디지털융복합연구, 제11권, 제11호, 2013, pp. 305-312.

[21] 이규안, "중소기업 첨단기술 유출사고의 문제점과 디지털 포렌식을 이용한 해결방안," 한국전자통신학회, 한국전자통신학회 학술대회지, 제5권, 제2호, 2011, pp. 43-47.

[22] 홍준석・박원형・김양훈・국광호, "로지스틱 회귀분석을 이용한 중소기업 기술보호 요인 분석," 한국전자거래학회, 한국전자거래학회지, 제20권, 제3호, 2015, pp. 1-10.

[23] 김인관・박재민・전중양, "중소기업에 대한 ISMS 인증효과와 영향요인에 관한 연구," 한국디지털정책학회, 디지털융복합연구, 제11권, 제1호, 2013, pp. 47-60.

[24] 장상수・노봉남・이상준, "정보보호 관리체계 운용이 정보보호 성과에 미치는 영향," 한국정보과학회, 정보과학회논문지, 제40권, 제1호, 2013, pp. 58-69.

[25] 이영준, "모델링과 템플릿 기반의 시나리오 기법을 이용한 효과적인 정보보호관리체계 연구," 고려대학교 석사학위논문, 2008.

[26] 홍성혁 · 박종혁 · 서정택, "국내환경에 적합한 정보보호관리체계 평가 방법론에 대한 연구," 한국항행학회, 한국항행학회논문지, 제12권, 제4호, 2008, pp. 384-391.
[27] 김정덕 · 장항배 · 류성렬, "중소기업 정보보호 특성을 고려한 정보보호 관리체계 연구," 한국중소기업학회, 중소기업연구, 제28권, 제2호, 2006, pp. 267-294.
[28] 강푸름, "중소기업 기술유출 방지를 위한 핵심인력 관리 방안에 관한 연구," 경기대학교 석사학위논문, 2013.
[29] 중소기업청, "중소기업 기술보호 지원계획," 2015.
[30] 장상수 · 이호섭, "정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구," 한국정보보호학회, 정보보호학회논문지, 제20권, 제1호, 2010, pp. 31-38.
[31] 중소기업청, "중소기업 기술유출 사례 및 대응전략," 2007.
[32] 최영현 · 엄정호 · 정태영, "RBAC을 이용한 정보유출 방지를 위한 보안성이 강화된 문서 DRM 구현," 디지털산업정보학회, 디지털산업정보학회지, 제7권, 제4호, 2011, pp. 57-66.
[33] 엄정호, "국방 정보시스템 환경에서 정보유출 방지를 위한 보안성이 강화된 문서 DRM 설계에 관한 연구," 디지털산업정보학회, 디지털산업정보학회지, 제7권, 제1호, 2011, pp. 41-49.
[34] 양선옥, 최낙귀, 박재표, 최형일, "H/W 정보의 인증을 통한 내부정보유출 방지 기법," 디지털산업정보학회, 디지털산업정보학회지, 제5권, 제1호, 2009, pp. 71-81.

■ 저자소개 ■

김 정 은
Kim Jungeun

2015년 3월~현재 남서울대학교 복지경영대학원 산업보안학과 석사과정
2015년 2월 남서울대학교 국제통상학과(학사)

관심분야 : 산업보안, 개인정보보호, 사물인터넷
E-mail : queen78787@hanmail.net

김 성 준
Kim Seongjun

2014년 2월~현재 남서울대학교 산업보안학과 조교수
2014년 2월 연세대학교 정보대학원(박사수료)
2009년 2월 동국대학교 법학과(박사)
2006년 8월 동국대학교 법학과(석사)
2003년 2월 동국대학교 법학과(학사)

관심분야 : 개인정보, 개인정보보호법, 정보보호, 사물인터넷, 빅데이터
E-mail : mvstar@hanmail.net

논문접수일: 2016년 7월 12일
수 정 일: 2016년 7월 25일
게재확정일: 2016년 8월 2일