경 영 학 석 사 학 위 논 문

보안역량진단이 기술보호대응책을 매개로 보안성과에 미치는 영향

2018년 2월

부경대학교 경영대학원

경영학과(정보관리전공)

김 종 원

경 영 학 석 사 학 위 논 문

보안역량진단이 기술보호대응책을 매개로 보안성과에 미치는 영향

지도교수 김 하 균

이 논문을 경영학석사 학위논문으로 제출함

2018년 2월

부경대학교 경영대학원

경영학과(정보관리전공)

김 종 원

김종원의 경영학석사 학위논문을 인준함

2018년 2월 일

위원장 경영학박사 최 태 영 (인)

위 원 경영학박사 전 재 균 (인)

위 원 경영학박사 김 하 균 (인)

목 차

표 목 차

표 목 차

A Study of the Impact Analysis of Security Capability Diagnosis on Security Performance Through Technical Protection Response

Jong-Won Kim

Major in Information Management
Graduate School of Business Administration
Pukyong National University

Abstract

As Korea's technological competitiveness has recently raised to enter a global level, there is a trend that the number of cases where cutting-edge technologies own by companies leak is increasing, and costs of damage caused by the leak are also increasing rapidly. Prior to 2010, large enterprises were targets for a leak of a targeted technology. Meanwhile, from 2010 onwards, small and medium enterprises have been main targets such that leaks of their technologies have mainly occurred. So, in 2013, the technology protection capability of small and medium enterprises was in the low level at 43.3 points. It was investigated that the (small and medium) enterprises experiencing leaks of their technologies occupied 10.2 % during the last three years, and costs of damage per case were 1.69 billion won. As such, the small and medium enterprises are in a situation with a difficulty in improving their security level due to problems such as human resource management, security investment costs or the like. Although the small and medium business administration and the related organizations have supported the small and medium enterprises, and investigations and researches were conducted to obtain a resolution method and improve a related system in order to prevent their technologies from leaking, there was no remarkable improvement. In this paper, diagnosis items of a small and medium enterprise-security capability diagnosis table are sorted out to conduct surveys to the employees of small and medium enterprises, and factors influencing the security performance of the small and medium enterprises are analyzed by proving an effect on security countermeasures by

the security capability diagnosis items and an effect on the security performance by the security countermeasures, thereby providing useful suggestions to the small and medium enterprises and the related personnel of them and contributing to the security performance of them.

Key words : security performance, security capability diagnosis, technical protection response

Ⅰ. 서 론

1.1 연구의 배경

2013년 우리나라의 65개 품목이 세계 수출시장 점유율 1위를 차지하고 세계 순위는 12위이며, 반도체, 메모리, 자동차 부품 등이 1위 품목으로 조사 되었다. 그러나 2013년 세계 수출시장 점유율 1위를 차지하고 있는 우리나라 제품 65개 중 미국, 일본, 중국 등이 2위를 차지하고 있으며, 우리나라는 2위인 미국, 일본, 중국과 1위 제품 중 약 50%를 차지하는 37개 품목에 대하여 경쟁하고 있는 것으로 조사 되어 세계시장에서 점유율 1위를 차지하기 위하여 국가 간에 끊임없는 경쟁을 하고 있다(Mun, B. K., 2015). 기업과 정부에서는 지속적인 R&D 투자를 통하여 기술의 발전을 이루고 있다. OECD 국가 중 전체 R&D 투자의 국내총생산 (GDP) 대비 비중은 1위 이스라엘 4.38%, 2위 한국 4.03%, 3위 핀란드 3.78%, 4위 일본 3.39% 이며, 민간 R&D 투자의 GDP 대비 비중은 1위 이스라엘 3.51%, 2위 한국 3.09%, 3위 핀란드 2.66%, 4위 일본 2.61% 이다(OECD, 2013). 우리나라 대기업과 중소기업은 국가차원의 전폭적인 R&D 투자를 통하여 기술력이 지속적으로 발전하여 왔다. 우리나라의 경제에서 중소기업은 많은 역할을 하고 있다. 2013년 기준으로 우리나라 중소기업 업체 수는 약 341만개로 전체 업체의 99.9%이고 근로자 수는 1,342만 명으로 전체업체 근로자 수의 87.5%

를 차지하고 2012년 기준으로 중소제조업의 생산액은 717.2조원으로 전체제조업의 생산액 대비 45.7%로 부가가치는 239.3조 원이다(Hong, S. C., 2014). 우리나라에서 중소기업이 차지하는 경제측면의 비중이 커지고 있지만 중소기업의 기술보호를 위한 보안역량수준은 상당히 취약하다. 국가정보원에서는 2009년부터 2013년까지 우리나라 기업의 전체 기술유출은 209건이 발생하였으며, 중소기업의 기술유출 발생 건수는 151건으로 전체 기술유출 건수의 73%에 해당하는 것으로 조사되었고(National Industrial Security Center, 2014), 중소기업청에서는 기술유출 건당 피해금액이 2008년에는 9.1억 원이었으나 2013년에는 대폭 증가하여 16.9억 원으로 조사되었다(Small and Medium Business Administration, 2014). 중소기업의 기술유출 건수와 피해금액이 증가하면서 정부차원에서 다양한 대책으로 중소기업의 기술보호 강화를 위하여 지원을 하고 있다. 산업자원통상부는 산업기술유출방지법을 제정하여 산업보안교육과 인력양성, 산업기술보호 실태조사 등을 지원하고 있으며, 공정거래위원회는 하도급거래에서 기술탈취 여부를 조사 지원하고 경찰청은 산업기술유출수사 지원팀을 운영하여 지원하고 있다. 특허청은 표준관리시스템 보급, 원본증명제도, 영업비밀보호법 사업을 지원하고 있다. 중소기업청에서는 중요자료의 상담.컨설팅, 기술임치, 기술유출방지시스템 지원사업, 온 라인보안관제 등 사업을 지원하고 있다.

그러나 지금까지는 사후대응측면의 기술유출방지대응전략이 운영 되었으

며, 현재 중소기업청과 관련기관에서 운영되고 있는 기술유출방지사업의 성과를 향상하기 위하여 중소기업의 기술보호수준에 대한 적절한 평가를 기반으로 기술유출방지효과를 증대할 수 있는 부분에 대한 체계적인 지원이 필요하다.

중소기업청에서는 해마다 중소기업기술보호역량 및 수준조사를 실시하여 중소기업의 기술보호수준과 기술유출실태를 조사하고 있으며, 도출된 결과를 기반으로 중소기업의 기술보호지원방안과 관련정책을 수립하는데 활용하고 있다.

1.2 연구의 목적

본 연구는 중견·중소기업 보안역량 진단표에서 도출한 주요보안역량 진단항목에 대한 설문자료를 통계분석 툴을 이용하여 중소기업의 보안과 관련된 보안역량진단과 보안대응 방안 및 보안성과를 실증하고자 하며, 중소기업의 보안성과에 영향을 주는 요인을 분석함으로써 보안실무자에게 유용한 시사점을 제공하고 중소기업의 보안성과 향상에 기여하고자 한다.

Ⅱ. 이론적 배경

2.1 보안의 유형

2.1.1 관리적 보안

기업의 정보보호와 운영에 대해 기본적인 보안정책을 수립하여 기업과 임직원이 대내외적 경영활동 수행 시 기업이 보유하고 있는 핵심자산과 기업정보를 체계적으로 보호 및 관리하는 활동이다. 일반적으로 기업 내부 인원의 채용, 퇴직, 재직 시 수행할 보안대책, 외부기관 및 협력업체 직원들의 출입 시 보안대책에 관련한 사항을 말한다. 중소기업청의 중소기업보호매뉴얼을 참조하여 관리적 보안 관리방안을 <표 1>과 같이 분석하였다.

<표 1> 관리적 보안 관리방안

구분	유형	세부항목
보안정책 수립 및 세부 규정의 제정	유형별 정책 수립	① 정보보호조직 정책 ② 정보자산관리 정책 ③ 인적보안 정책 ④ 물리 및 환경적 보안 정책 ⑤ 기술적 보안 정책 ⑥ 정보보호 운영관리 및 사고대응 정책
자산관리	자산의 분류	① 정보자산 ② 문서자산 ③ 소프트웨어자산 ④ 물리적 자산 ⑤ 인적 자산

	위험성 평가	① 자산에 대한 취약점을 및 자산에 대한 위협을 평가 ② 위협의 발생 가능성과 위협에 대한 노출이 조직에 미치는 영향을 평가 ③ 보안대책 평가와 잔여위험 평가도 포함 ④ 위험성 평가의 국제 기준으로 ISO/IEC27005가 있으며, 산업기술보호종합지원포탈(www.is-portal.net)에서 이에 부합하는 평가솔루션 서비스 제공
비밀문서 관리	사전계획에 의한 생산	① 최초 기안단계에서부터 배포계획을 수립하여 비밀에 첨부하고 결재 ② 가능한 한 내용을 형상화 시키지 말 것
	최소 생산, 최소 배포	① 현재 시점에서 배포처에 따라 필요한 최소한의 양만 생산, 예비용 금지 ② 업무와 직접 관계가 있는 부서에 국한하여 최소 부수 배포
	비밀의 등급 분류	① 가치와 중요성에 따라 등급을 결정
	비밀의 표시	① 등급표시 ② 관리번호/사본번호/페이지 표시 ③ 예고문 표시 ④ 비밀문서의 재분류
인적 자원 관리	비밀유지서약서(보안서약서)의 제출 입·퇴사자 관리 사원증 관리	-

기술보호 교육	교육대상	전 임직원 대상으로 업무별, 직급별, 직책별 분리하고 교육빈도와 시기, 교육시간을 적절하게 조정
	교육운영	보안규정(세부규정)을 비롯하여 사내외에서 발생했던 보안사고 사례, 보안의무 위반 시 벌칙 등을 교육
보안실태 점검	형태	① 팀별 자체 점검활동 ② 정기 보안감사 ③ 비정기(불시) 보안감사
	점검주기	① 일일점검, 매월점검, 분기점검, 매년 보안감사 등이 있으며 기업환경에 맞게 조정 ② 목표 미달성 또는 문제점이 있는 경우에는 개선 후 반드시 재점검
	보안점검 시 준수사항	① 공정하고 증거에 의한 점검 및 감사 ② 업무 수행상 지득한 비밀의 유지
	보안점검 시 지적사항	① 보안규정 및 지침 등의 지속적 또는 중대 위반 ② 정당한 사유 없이 정보자산 분류 및 관리를 1개월 이상 미시행 ③ 보안교육에 참석하지 않고 교육내용 미이행 ④ 이전 보안점검 지적사항에 대한 시정조치 노력 미진 ⑤ 간단하게 시정 조치가 가능한 사항도 포함
	보안점검 보고서	① 지적사항 위주 작성, 개선 및 재발방지 방향 포함 ② 목적, 수감팀, 감사법위, 일시, 확인된

		위반사항 및 관련규정이 포함 ③ 문제점에 대해서는 충분한 근거자료를 토대로 조사내용을 제시
	보안점검 사후관리	① 수감팀은 지적사항을 조사하여 원인을 파악한 후 시정 ② 지적사항 이외에도 유사문제 발생 가능성이 있는 경우 예방조치 ③ 시정/예방조치 상태를 점검하여 완료 확인된 경우에 사후관리 종결
	보안 위규자 처리	① 보안관리 규정에 의거 회사 대표 보고 후 징계위원회에서 처리 ② 만일, 회사에 직간접적으로 끼치는 영향이 지대한 경우에는 민법, 형법, 부정경쟁방지 및 영업비밀보호에 관한 법률 등에 의해 사법처리

출처 : 중소기업청(2014), 중소기업보호매뉴얼 참조

2.1.2 기술적 보안

네트워크상에서 발생하는 스니핑(Sniffing), 스푸핑(Spoofing), DoS, DDoS 공격 등과 같은 해킹 기술을 이해하고, 대응 가능한 네트워크 기반 보안기술에 대해 제시하는 것을 말한다. 사이버 보안 및 PC 보안, 서버보안 등의 관련솔루션을 활용한다. 중소기업청의 중소기업보호매뉴얼을 참조하여 기술적 보안 관리방안을 <표 12>와 같이 분석하였다.

<표 2> 기술적 보안 관리방안

구분	유형	세부항목
통신 네트워크 보안	네트워크 기반 공격 대비	1) 정보 수집 단계 2) 스캐닝(Scanning) 3) 스니핑(Sniffing) 4) 스푸핑(Spoofing) 5) DoS와 DDoS 공격
	무선 통신 기술	무선네트워크 보안정책 수립 - SSID(Service Set Identifier, 서비스 셋 식별자) 설정을 통한 접속 제한 - 폐쇄시스템 운영(SSID 숨김기능) - MAC 주소 인증 - WEP(Wired Equivalency Privacy) 인증 - EAP(Extensible Authentication Protocol) 인증 - AP 장비 물리적 접근 차단 - 무선 네트워크 단말기의 관리 강화 - AP 장비의 전파 출력 조정 - 암호화키 길이 증가
	네트워크 보안 기술	방화벽(Firewall) 침입탐지시스템(Intrusion Detection System, IDS) 가상사설망(Virtual Private Network, VPN)
전산시스템 보안	운영체제 기반 공격	악성 프로그램(Malicious Program) 패스워드 크래킹(Password Cracking) 백도어(Backdoor) NetBIOS를 이용한 공격 버퍼 오버플로우(Buffer Overflow) 공격

	윈도우 보안	윈도우 업데이트(Update) 윔도우 방화벽 계정 관리 파일 및 폴더 관리
	UNIX/LINUX 보안	계정 관리 패치 관리 파일 및 폴더 관리 접근 제어
애플리케이션 보안	인터넷 응용 보안	웹 브라우즈(Web Browser) 보안 메일 보안 인터넷 보안
	웹 애플리케이션 보안	OWASP Top 10 웹 해킹 종류 파악
	보안 솔루션 도입	DRM(Digital Rights Management) DLP(Data Loss Prevention) NAC(Network Access Control)

출처 : 중소기업청(2014), 중소기업보호매뉴얼 참조

2.1.3 물리적 보안

중요설비와 기술정보가 있는 장소를 물리적인 위협으로부터 보호하여 정상적으로 운영할 수 있도록 하는 것을 말한다. 통제구역과 제한구역의 지정, 출입통제시스템 구축, CCTV 설치 등 첨단출입통제장비를 활용하여 출입자 통제와 시설물에 대한 보안활동을 실행하는 가장 기초적인 보안단계이다. 중소기업청의 중소기업보호매뉴얼을 참조하여 물리적 보안 관리방안을 <표 3>과 같이 분석하였다.

<표 3> 물리적 보안 관리방안

구분	유형	세부항목
출입 통제	구역별 보호대책 수립 / 구분	공용구역 기관 내·외부의 모든 인력에게 공개된 구역(출입문, 로비, 대기실, 엘리베이터, 주차장 등) ① 외부인의 출입 시 이름, 주소, 주민등록번호, 연락처, 소속 등 출입자의 주요 정보를 출입관리대장에 기재하고, 내부인력을 통해 안내 ② 과도한 불편을 주어 거부감을 주지 않도록 적절한 수준 유지
		일반구역 내부인이나 출입이 허가된 인원에 한하여 공개된 구역(일반사무실, 회의실 등) ① 주요 정보에 대한 보호의식이 약해지기 쉬워 기술 유출 가능성이 높음 ② 외부인과 내부인을 구별하기 위해 사원증을 패용하도록 함 ③ 자리이탈 시 화면보호기 설정, 책상 정리, 주요문서는 캐비닛 보관 ④ 복사기, 팩스기 등은 사무실 안쪽에 비치
		제한구역 중요 설비가 위치하고 있는 구역(장비실, 전기실, 기계실 등) ① 승인받은 내부인원만이 출입하도록 하며, 외부인의 출입은 반드시 통제 ② 설비의 훼손, 파괴, 오작동 등의 문제에 대한 주의 필요

		통제구역 기술 및 경영상 영업비밀의 상당수를 보유하며, 침해 및 유출시 기업의 운영에 치명적인 영향을 주는 구역(연구소, 중요제품 생산라인, 전산실 등) ① 통제구역은 주요 기술에 대한 개발 및 연구가 이루어지고 주요정보를 보관하고 있으므로, 최상위의 보안대책을 적용 ② 해당 근무자 이외 모든 출입을 금지 ③ 일반직원도 반드시 승인을 받은 후에 출입, 외부인은 절대 출입금지
주요자산 보호	고려사항	보호요소 ① 담장, 벽, 문, 창문, 천장, 바닥 ② 난방과 냉방, 전원 공급 방법, 물과 가스선 ③ 화재 탐지와 진압 장비 ④ 대상물로의 접근 방법 및 경로(동선), 대상물의 위치 및 이동경로
		위험요소 대비 ① 강도, 절도, 진입 ② 정전, 통신 장애 - Backup UPS(Uninterruptible Power Supply) 구비 ③ 물리적 피해(장비, 문서 등의 손괴 및 절도) ④ 기타 시스템 무결성 손상 ⑤ 허가되지 않은 사람에 의한 불법적 정보 유출

	보안 대책	물리적 보안 대책 ① 출입문 잠금장치, 컴퓨터단말기 잠금장치, 경비원 및 감시카메라 ② 출입통제 시스템, 임직원 신원보증 및 사원증(ID Card) ③ 출입구 단일화, 정보시스템, 중요 구역의 이중 출입문 설치 ④ 중요 시설 위치 선정 시 고려사항 - 가시성(Visibility), 옆 건물 유형, 지역 범죄율 - 공공기관(경찰, 의료기관, 소방서 등)과의 인접성 - 자연재해의 발생 가능성
		시설별 보안관련 법적 의무 사항 준수 승강기, 화재경보기, 소화전, 비상구, 피난구, 통신시설, 전기시설 관련
		권고사항 권고 ① 기업 활동 및 결과물 보호 관련 사항 - 물리적 보안시스템, 데이터백업, 시스템의 HW 설정 ② 과다 지출 없이 보호를 강화할 수 있는 매커니즘 - 잠금장치, 경비실, 철조망
	전산 시설 보안	전산 Backup 장비 ① 예측 불가능한 상황에 대비, 지속적이고 일관적인 백업 수행 ② Backup 장치의 서비스, 하드웨어, 생명 등에 지장 초래하는 환경 개선

		시설 구성 시 고려 사항 ① 공개구역에는 침입차단시스템을 통하지 않고 내부 네트워크에 접속되는 컴퓨터가 없어야 함 ② 서버실은 반드시 잠그고, 출입통제시스템과 CCTV시스템을 항상 운영 ③ 전원차단, 절도, 홍수, 폭발, 지진 등 재해에 대비한 비상계획 수립
		시설접근통제 ① 고려사항 - 데이터의 중요성, 접근 가능자 식별, 회사에 중요한 직무와 근무지 ② 사용자 인증 필수 - 보안 요원에 의한 인식, 열쇠, 스마트카드, 지문, 홍채 인식 등

출처 : 중소기업청(2014), 중소기업보호매뉴얼 참조

2.2 보안역량진단

중소기업이 자체적으로 기업의 보안수준을 점검하고 진단할 수 있도록 중소기업청과 대·중소기업·농어업협력재단에서 <표 4>와 같이 중소 중견기업 보안역량 진단표를 지원하고 있다. 중소·중견기업 보안역량 진단표를 활용하여 보안역량을 자가진단하며, 이를 토대로 보안의 필요성을 인식하고 자발적으로 보안수준 향상을 위한 개선방안을 수립하여 추진이 가능하다. 또한 기업이 자체적으로 추진이 어려운 경우는 대·중소기업·농어업협력재단에서 운

영하는 기술보호센터에 기술보호상담을 신청하여 보안역량 자가진단결과를 기반으로 보안 전문가의 전문적인 컨설팅을 지원 받아 기업의 체계적인 보안수준향상을 위한 계획을 수립하며, 적극적으로 이행하여 기업의 보안체계 강화를 실현하고 보안 사고를 사전에 예방할 수 있다.

중소·중견기업 보안역량 진단표의 보안역량 측정문항은 총 6개 부문, 50개 문항으로 구성되어 있으며, 각 문항별로 가중치를 적용하여 합계 100점으로 구성되었다. 보안역량 측정문항의 총 6개 부문은 보안의 유형별로 관리적 보안과 물리적 보안 및 기술적 보안 3개 부문으로 구분되며, 3개 부문별 배점 현황은 <표 5>와 같다. 보안역량진단을 실시 후 확인되는 진단점수로 기업의 보안수준을 평가하며, 보안수준은 우수, 양호, 보통, 취약, 미흡 5개 기준으로 평가하고 기업 보안수준 평가에 대한 구체적인 기준은 <표 6>과 같다.

중소기업청을 비롯한 정부는 <표 7>과 같이 중소기업의 기술보호역량 향상을 위하여 다양한 기술보호지원사업을 수행하고 있다.

<표 4> 중소·중견기업 보안역량

구분	번호	진단내용	점수
기업의 보안정책	1.1	보안규정을 보유하고 있는가?	2
	1.2	회사의 보안정책, 지침, 절차 등의 내용에 대해 임직원들에게 공지하고 있는가?	1
	1.3	보안전담조직이 존재하는가?	2
	1.4	회사의 주요 정보(기술, 영업 등)는 어떻게 공유되는가?	2
	1.5	임직원의 업무에 기밀사항의 보호 등 보안관련 내용이 포함되어 있는가?	1
	1.6	회사내 보안업무 수행을 위해 팀(혹은 그룹)간 업무 공조체계가 구성되어 있는가?	1

	1.7	정기적으로 보안감사를 실시하고 있는가?	2
	1.8	회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용수준은 어떠한가?	3
	1.9	보안업무 추진을 위해 외부 전담기관의 도움을 받고 있습니까?	1
기업의 자산관리	2.1	회사가 보유한 정보자산에 대해 목록 관리 등을 통한 관리기준을 수립하여 가지고 있는가?	2
	2.2	회사의 정보자산을 그 중요성에 따라 '극비', '대외비', '일반' 등으로 등급을 구분하여 관리하고 있는가?	2
	2.3	회사의 정보자산에 대한 관리책임자를 지정하여 관리하고 있는가?	2
	2.4	회사의 정보자산 분류는 정기적으로 이루어지는가?	2
	2.5	주요 기밀문서의 경우 어떻게 관리하고 있는가?	2
	2.6	특허, 실용신안, 디자인 등 지적재산권에 대한 관리방안이 마련되어 있는가?	2
	2.7	장비, 정보 또는 소프트웨어 등의 회사 자산의 반출은 어떤 식으로 이루어지는가?	1
기업의 인적자원 관리	3.1	신규 입사자에 대해 보안교육을 실시하고 있는가?	1
	3.2	기존 임직원을 대상으로 보안교육을 실시하고 있는가?	2
	3.3	임직원 보안의식을 제고하기 위해 퇴근 시 혹은 자리이탈 시에 다음과 같은 활동을 수행하고 있는가?(PC 전원 Off 여부 확인, 장시간 자리이탈 시 화면보호기 설정 여부 확인, 노트북 방치 여부 확인, 출입문, 캐비넷, 개인서랍 시건 여부 확인, 문서 및 도면 방치 여부 확인)	3
	3.4	신규 입사자에 대해 보안서약서를 징구하고 있는가?	2

	3.5	주요 R&D 프로젝트 참가자에 대해 보안서약서를 징구하고 있는가?	2
	3.6	종업원이 보안정책, 지침, 절차 등을 위반하는 경우 직원에 대한 공식적인 징계 절차가 마련되어 있는가?	2
	3.7	퇴직자에 대해 회사 정보자산의 유출방지를 위한 보안서약서를 징구하고 있는가?	2
	3.8	퇴직자의 향후 진로 및 동향을 파악하고 있는가?	2
	3.9	제3자(협력업체, 외국인 등)에 대한 관리를 하고 있는가?	2
	3.10	회사의 정보자산에 대한 사용자(임직원, 계약자, 제3의 사용자 등)들의 접근 권한은 퇴사, 계약종료, 역할 조정 등의 사유발생시 조정되어지고 있는가?	2
기업의 시설관리	4.1	회사 내 중요시설에 대한 관리기준이 있는가?	2
	4.2	협력업체, 방문객 등 외부인의 회사 내 출입절차가 존재하는가?	2
	4.3	회사 내 중요시설에 대해 출입통제시스템을 설치하여 운영하고 있는가?	2
	4.4	외부인 식별을 위하여 임직원의 사원증 패용을 의무화하고 있는가?	1
	4.5	건물 출입구나 중요시설에 대해 CCTV 등의 감시장치가 설치되어 있는가?	2
	4.6	중요시설 및 통제구역에 대해 화재, 전원, 수해 등으로부터의 보호방안이 강구되어 있는가?	2
	4.7	회사 내 중요시설에 카메라, 비디오카메라 등의 장비반입이 규정에 의해 통제되고 있는가?	1
기업의 IT 보안관리	5.1	다음과 같은 정보처리 설비의 운영절차가 문서화되어 규정되어 있는가? (컴퓨터의 가동과 종료절	3

		차, 백업절차, 유지 보수절차 등)	
	5.2	통신망에 대한 보안점검을 실시하고 있는가?	2
	5.3	서버 및 DB 현황에 대한 보안점검을 실시하고 있는가?	2
	5.4	바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구하고 있는가?	3
	5.5	내부에서 생성된 주요 정보 및 소프트웨어는 백업되어 관리되고 있는가?	2
	5.6	지식관리시스템(KMS), 전자결재시스템 등 회사내 주요 정보에 대한 관리시스템이 존재하는가?	2
	5.7	FD, CD, USB 등 정보의 저장이 가능한 매체에 대한 관리절차가 마련되어 있는가?	2
	5.8	외부로의 전자문서 발송에 대한 통제시스템이 마련되어 있는가?	2
	5.9	PC 및 주요 시스템 사용자에 대한 패스워드 관리를 하고 있는가?	2
	5.10	임직원이 장기간 자리를 이석하는 경우 어떠한 조치를 취하고 있는가?	2
	5.11	내부 통신망과 외부 통신망(인터넷, 협력회사 등)을 분리하여 운영하고 있는가?	2
	5.12	정보시스템의 사용 내용에 대한 로그를 기록하고 유지하는가?	2
	5.13	주요 장애 발생 시 장애내용이 보고되어 신속하게 시정조치가 이루어지는가?	2
	5.14	정보시스템에 대한 유지보수를 실시하고 있는가?	2
기업의 유출사고의 대응	6.1	정보시스템에 대한 재해발생 시 다음과 같은 대응절차가 수립되어 있는가? (비상시 따라야 할 절차와 관련자의 책임규정, 유관기관과의 연락체계 구성여부, 제한된 시간 내에 필수 업무 및 지원서비스를 대체장소로 이전하여 운영하기 위한 절차, 정상적인 사업 활동으로 복귀하기 위한 원상복귀 절차, 위기	5

		관리를 포함한 비상절차 및 프로세스에 대한 임직원 교육)	
	6.2	기술유출 및 침해사고 발생 시 회사 차원의 대응 방안이 마련되어 있는가?	3
	6.3	부정경쟁방지 및 영업비밀 보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률, 국가연구개발사업 공통보안지침 등 기술유출 방지와 관련된 주요 법규에 대해 인지하고 있는가?	2

출처 : 대·중소기업·농어업협력재단, 중소·중견기업 보안역량 진단표 참조 및 연구자가 재구성

<표 5> 보안부문별 배점현황

유형	부문	문항수	부문별 점수	유형별 점수
관리적 보안	기업의 보안정책	9	15	58
	기업의 자산관리	7	13	
	기업의 인적자원관리	10	20	
	기업의 유출사고의 대응	3	10	
물리적 보안	기업의 시설관리	7	12	12
기술적 보안	기업의 IT 보안관리	14	30	30
합계		50	100	100

<표 6> 기업 보안수준 평가 기준

보안수준	점수	보안수준평가
우수	85점 이상	보안에 대한 결점 및 취약성이 거의 없으며, 기술의 유출 및 침해사고 발생시 피해가 최소화되는 상태
양호	70점 이상 ~85점 미만	보안에 대해 심각하지 않은 결점 및 취약성을 내포하며, 회사 차원의 보안업무가 나름대로 이루어지고 있는 상태
보통	55점 이상 ~70점 미만	보안에 대해 일반적인 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 피해가 커질 수 있는 상태
취약	40점 이상 ~55점 미만	보안에 대해 다소 심각한 결점 및 취약성을 내포하며, 기술의 유출 및 침해정도에 따라 치명적인 피해를 가져올 수 있는 상태
미흡	40점 미만	보안에 대해 심각한 결점 및 취약성이 상존하며, 기술의 유출 및 침해정도에 따라 치명적인 피해가 우려되는 상태

<표 7> 중소기업 기술보호 지원사업

서비스명	내용
기술보호상담	• 분야별 보안전문가의 현장방문을 통한 중소기업의 취약점 진단 및 기술 유출 방지 보안컨설팅 • 중소기업의 보안장비 및 보안시설, 서버구축 등 정보화기기 보안관리 요령 • 기술유출 피해기업의 분쟁 대응 및 소송수행 등 법률자문 • 해킹 등 사이버 공격으로 인한 피해 복구 및 대응 지원
기술자료임치제도	• 중소기업의 핵심기술 정보를 대/중소기업 협력재단에 안전하게 보관(임치)

	• 기술유출이 발생하였을 경우, 임치된 기술자료를 이용하여 기술 보유입증 • 중소기업과 함께 기술자료 임치제도를 이용한 대기업 등 거래기업은 해당 기업이 파산/폐업 할 경우, 임치된 기술 자료를 교부받아 사용이 가능
기술지킴이서비스	• 내부 직원으로부터 기술/정보 유출을 사전에 차단하여 보안사각지대로부터 중소기업을 보호 • 온라인 상에서 발생하는 기술 유출 및 사이버 공격에 무방비로 노출된 중소기업의 기술/정보를 보호
기술유출방지시스템 구축	• 개별 기업의 인프라 진단 및 기술 유출 방지를 위한 보안시스템 구축비용 지원

자료: 중소기업연구원(2014). “중소기업 기술보호 지원정책의 현황 및 과제”

2.3 중소기업 보안수준 및 기술유출 실태

2.3.1 중소기업 보안수준실태

중소기업청과 대·중소기업·농어업협력재단은 정부의 기술 유출 방지 지원 방안 및 중장기적인 정책 수립에 활용하기 위하여 중소기업 및 대기업을 대상으로 기술유출 실태를 파악하고 기술보호 역량 수준 진단을 실시하였으며, <표 8>과 같은 기술보호 역량 수준 진단 결과를 도출하였다.

<표 8> 기술보호 역량 수준 진단 결과

구분	진단항목	진단결과
보안정책 수립	임직원 대상 보안규정 보유 여부	‘보안규정 보유, 모든 직원에게 배포’가 53.9%로 나타나며, 임직원 대상 보안규정이 없는 중소기업은 27.6%로 전년도 대비 0.5%p 감소함
	정기적 기술보호 및 보안 규정 개정 여부	대부분 ‘필요에 따라 개정’(61.7%)으로 조사됨
	기술유출관련 사고 대응 절차 마련	‘구체적으로 마련되어 있으며, 숙지하고 있음’이 51.0%로 가장 높으며, 출입자 기술유출관련 사고 대응절차 마련을 전혀 하지 않는다는 중소기업은 26.7%로 전년도 대비 2.2%p 감소함
	보안규정 위반 시 징계 절차 마련	‘징계절차가 마련되어 있으며, 필요 시 징계조치가 이루어짐’이 31.3%로 나타나며, 징계절차 및 징계조치 실적이 모두 없는 중소기업은 21.5%로 전년도 대비 17.6%p 감소함
	보유자산 지침 마련	‘보유자산 지침이 수립'되어 있는 중소기업은 79.0%로 전년(67.9%) 대비 11.1%p 증가한 것으로 나타나며, ‘보유자산 지침이 수립'되어 있는 중소기업 중 65.9%는 ‘지침에 따라 이행'하고, 13.1%는 ‘지침이 수립되어 있지만 이행하고 있지는 않는 것’으로 조사됨
	기술보호 투자액	‘기술보호 인력 인건비’가 2016년 3천 5백만원으로 전년도에 비해 약 1천 1백만원 감소하며, ‘보안 설비 시스템/솔루션 도입 유지 관리’는 2016년 1천 3백

		만원으로 전년도에 비해 약 5백만원 증가하였고 기술보호 투자액은 '보안 설비 시스템/솔루션 도입 유지 관리'가 대기업(5천 2백만원), 중견기업(2천 2백만원), 중소기업(1천 3백만원)으로 조사됨
	기술보호 필요성 인식 수준	중소기업의 기술보호 필요성 인식수준이 높다(매우 높음+높음)는 의견을 직급별로 살펴보면, 'CEO/임원'이 60.2%로 가장 높게 나타났으며, 다음으로 '부서장'(49.6%), '직원'(40.8%) 순으로 조사되며, 전년도에 비해 인식수준이 전반적으로 하락한 것으로 나타남 (각 'CEO/임원' 12.4%p, '부서장' 17.1%p, '직원' 11.7%p 하락)
	기술보호방안/체계 추진의지 수준	중소기업의 기술보호방안/체계 추진의지 수준이 높다(매우 높음+높음)는 의견을 직급별로 살펴보면, 'CEO/임원'이 57.0%로 가장 높게 나타났고 다음으로 '부서장'(48.2%), '직원'(38.2%) 순으로 조사되며, 전년도에 비해 추진의지 수준이 전반적으로 하락한 것으로 나타남 ('CEO/임원' 5.1%p,'부서장' 5.5%p, '직원' 2.0%p)
보안관리	경비시스템 운영	무인경비시스템이 88.2%로 가장 높게 나타났고 다음으로 '자체 CCTV설치'(68.9%), '상주경비인력 근무'(18.3%) 순으로 조사되며, 경비시스템을 전혀 운영하지 않는 중소기업은 4.2%로 전년(9.1%) 대비 4.9%p 감소함.

	외부인 접견실 운영	중소기업의 '외부인 접견실(사무실과 분리된 별도의 공간) 운영' 비율은 71.1%이며, 이는 전년 34.7% 대비 36.4%p 상승한 결과임.
	출입자 통제·관리 경비시스템 운영	'사원증/방문증(ID카드) 또는 지문인식을 통한 관리'가 79.6%로 가장 높게 나타났으며, 다음으로 '출입자 관리대장 작성·관리'(23.1%), 'CCTV등의 감시장치 설치·운영'(10.1%)등의 순으로 나타남. 반면 출입자 통제·관리 경비시스템 운영을 전혀 하지 않는다는 중소기업은 11.7%로 전년도 대비 14.6%p 감소함
	중요자산 보호를 위한 보안시스템 운영	보안시스템을 운영하는 중소기업의 비율은 81.7%로 전년도 67.6% 대비 14.1%p 증가함
	보안시스템 운영 시 관리시스템 종류	기업규모별로 보안시스템 운영 시 관리시스템 종류를 살펴보면, 'CCTV 등 감시장치'가 대기업(93.0%), 중견기업(92.3%), 중소기업(79.2%) 모두 가장 높게 조사됨
	중요자산 보호를 위한 통제구역 운영	'한정된 직원만 출입 가능한 통제구역 운영(CCTV 등 감시장치 설치)'이 30.9%로 가장 높게 나타났으며, '모든 직원 출입 가능한 통제구역 운영(CCTV 등 감시장치 설치)'(17.8%), '모든 직원 출입 가능한 통제구역 운영(CCTV 등 감시장치 미설치)'(6.1%) 등의 순으로 조사됨

		통제구역이 없는 중소기업은 42.2%로 전년(41.9%) 대비 0.3%p 증가함
	정기적인 보안감사 실시 여부	보안감사를 정기적으로 실시하는 중소기업의 비율은 20.7%로 나타났으며, 필요시에만(비정기적) 실시하는 중소기업이 36.9%로 나타남. 실시하지 않는다는 중소기업은 42.4%로 전년 44.0%에 비해 1.6%p 감소함
	보안감사 실시 시 책임자	'대표 이사 및 임원급'이 45.0%로 가장 높게 나타났고, 그 다음으로 '부서별 보안관리자'가 26.8%로 나타남 '보안전담부서/관리자'의 비중은 전년도 39.6%에서 20.3%로 19.3%p 감소함
	정보화기기 반입 및 반출 통제 여부	모든 정보화기기의 반출입을 통제한다는 중소기업이 8.0%, 일부기기에 한해 반출입을 통제한다는 중소기업이 24.0%로 나타남. 반출입 통제가 없는 중소기업은 68.0%로 전년 67.3% 대비 0.7%p 증가함
	내부 네트워크 관리	'무선랜 사용 시 ID/PW를 부여'하여 관리한다는 기업이 44.6%, '내부, 외부 통신망을 분리'하여 관리한다는 기업이 24.6%로 조사됨 무선랜 사용에 대한 제한이 없는 중소기업은 44.7%로 전년 35.7% 대비 9.0%p 증가함
	정보시스템 사용 내용 로그 관리	정보시스템 사용 내용에 대한 로그를 관리하는 기기는 'PC'가 53.4%로 가장 높게 나타났으며, 'E-mail 수발신'(44.0%), '메신저'(30.2%) 순으로 조사

		됨 로그 관리를 전혀 하지 않는 중소기업은 35.1%로 전년 32.1% 대비 3.0%p 증가함
	디지털자산 관리용 보안 솔루션 운영 여부	‘방화벽’이 62.9%로 가장 높게 나타났으며, ‘IDS(침입탐지시스템)’(28.1%), 'DLP(데이터 유출방지 솔루션)'(15.9%), DRM(디지털 저작권 관리)’(10.6%) 등의 순으로 조사됨 보안솔루션 운영을 전혀 하지 않는 중소기업은 33.6%로 전년 5.4% 대비 1.8%p 감소함
	OS 및 백신 최신버전 업데이트	OS 및 백신 최신버전 업데이트 비율은 87.1%로 전년 79.2% 대비 7.9%p 증가함
인력관리	직원 보안교육 실시 여부	‘전 직원을 대상으로 연1회 이상 실시한 정기적인 보안교육 실시’가 52.9%로 가장 높게 나타남. 직원의 보안교육을 실시하지 않는 중소기업은 22.6%로 전년 29.6% 대비 7.0%p 감소함
	직원 보안교육 실시자	‘대표이사 및 임원급’이 45.4%로 가장 높게 나타남. ‘보안전담부서/관리자’는 15.7%로 전년 대비 19.6%p 감소함
	임직원 부재 시 보안활동	중소기업의 임직원 부재 시 보안활동을 실시한다(매우 많이 실시함+많이 실시함)는 의견을 살펴보면, ‘도면 및 문서 방치 여부 확인’(83.0%)이 가장 높게

		나타났으며, 다음으로 '출입문, 캐비닛, 개인서랍 시건 여부 확인'(79.2%), '장시간 자리이탈 시 화면보호기 설정 및 패스워드 사용(77.1%)' 순으로 조사됨. 전반적으로 전년도 대비 보안활동 실시율이 높아진 것으로 나타남
	보안서약서 작성 여부 및 대상자	보안서약서를 작성하여 제출하도록 한 중소기업의 비율은 63.8%로 전년도 57.0% 대비 6.8%p 하락함
	보안서약서 작성 시 구체적 보안 대상 업무 명시 여부	구체적 보안 대상 업무를 명시한 중소기업의 비율은 65.8%로 전년도 76.3% 대비 10.5%p 감소함
	보안서약서 내 준수위반 시 처벌 또는 배상책임 명시 여부	보안서약서 내에 준수위반 시 처벌 또는 배상책임을 명시한 비율은 72.4%로 전년 84.2% 대비 11.8%p 감소함
	경쟁업체 취업금지 서약서 작성 여부	경쟁업체 취업금지 서약서 작성 비율은 39.2%로 전년도 24.7% 대비 14.5%p 증가함
	퇴사자 진로 및 동향 파악	모든 퇴사자의 동향을 파악한다는 중소기업이 6.5%, 주요 임직원에 한하여 동향 파악한다는 중소기업이 30.6%로 나타남 파악하지 않는다는 중소기업은 62.9%로 전년도 52.8% 대비 10.1%p 증가함
	직무발명보상제도 운영 여부	직무발명보상제도 운영 비율은 34.8%로 전년도 24.6% 대비 10.2%p 증가함
보안사고 및 재해관리	위기관리시스템 수립 및 시행 여부	위기관리시스템 수립 및 시행 비율은 63.3%로 전년도 37.2% 대비 26.1%p 증가함

	중요자료 보호대책 수립 및 시행	‘자체적으로 정기적 백업관리’가 43.7%로 가장 높게 나타남. 관리하지 않는다는 중소기업은 22.8%로 전년도 18.5% 대비 4.3%p 증가함

자료 : 중소기업청(2017), “2016년 중소기업 기술보호 수준 실태조사” 참조 및 연구자가 재구성

2.3.2 중소기업기술유출실태

중소기업청과 대·중소기업·농어업협력재단은 2016년도 중소기업 및 대기업을 대상으로 파악한 기술유출 실태와 기술보호 역량 수준 진단을 토대로 <표 9>과 같은 기술유출현황을 도출하였고 최근 3년간(2013~2015년) 기술유출 피해경험이 있는 중소기업은 3.5%로 나타났으며, 이 결과는 전년도 조사(3.3%)보다 0.2%p 증가한 것으로 조사되었다.

<표 9> 기술유출현황

순번	진단항목	진단결과
1	기술정보 유출 피해건수 및 피해금액	최근 3년간 기술유출 경험이 있는 중소기업의 94.2%(49개사)가 ‘1건’의 기술유출 경험이 있는 것으로 조사됨 기술유출 피해 경험이 있는 중소기업 중 실질적인 피해를 입은 기업의 총 피해금액은 1,097억원으로 평균 18.9억원의 기술유출 피해가 있는 것으로 조사됨.
2	기술정보 외부 유출 관계자	기술정보를 외부로 유출시킨 관계자는 ‘전 직원(퇴사자)’이 69.2%로 가장 높았

		으며, ‘경쟁기업’ 17.3%, ‘현 직원(인턴, 임시직 포함)’ 11.5%, ‘협력업체(하도급)’ 5.8% 등의 순으로 조사됨
3	기술정보 유출 이후 관계자의 상태	기술정보 유출 이후 관계자의 상태는 ‘국내 중소기업으로 이직’이 46.3%로 가장 많았으며, 다음으로 ‘창업’ 39.0%, ‘계속 근무’ 12.2% 등의 순으로 조사됨
4	기술유출·탈취 피해 유형	기술유출·탈취 피해 유형은 ‘내부직원의 기술유출’이 76.9%로 가장 많았으며, 다음으로 ‘경쟁사로의 기술유출’ 21.2%, ‘기술인력 빼가기’ 3.8% 등의 순으로 조사됨
5	외부 유출 기술정보 종류	외부로 유출된 기술정보로는 ‘생산 중인 제품’이 42.3%로 가장 많고, 다음으로 ‘연구과제 결과 데이터’ 38.5%, ‘연구과제 개발계획’ 9.6% 등의 순으로 조사됨
6	유출된 비기술자료 종류	외부로 유출된 비기술자료는 ‘영업정보’가 11.5%로 가장 높고, 다음으로 ‘재무정보‘, ’원가분석정보‘, ’사업추진계획‘ 5.8% 등의 순으로 조사됨
7	기술정보 유출 수단	기술정보 유출 수단으로는 ‘핵심인력 스카우트 또는 매수’가 36.5%로 가장 높고, 다음으로 ‘휴대용 저장장치(USB, 외장하드 등)’ 30.8%, ‘E-Mail’, ‘복사, 절취’ 17.3% 등의 순으로 조사됨
8	기술유출 발생 시 외부적 조치	기술유출 발생 시 외부적으로 취한 조치로는 ‘보안 강화 관련 조치 시행’이 23.1%로 가장 높고, 다음으로 ‘관계자

		(사)를 고소, 고발', '수사기관에 수사 의뢰' 9.6% 등의 순으로 조사됨 기술유출이 발생하였지만, 특별한 조치를 취하지 않은 경우는 63.5%로 나타나 대부분의 기술유출 발생 기업에서 특별한 조치를 취하지 않은 것으로 나타남
9	기술유출 발생 시 내부적 조치	기술유출 발생 시 내부적인 조치로는 '직원교육(보안의식) 강화'가 61.5%로 가장 많았으며, 다음으로 '보안관리(자료관리, 출입자 통제 등) 강화' 40.4%, '보안장비 설치 강화' 19.2% 등의 순으로 조사됨

자료 : 중소기업청(2017), "2016년 중소기업 기술보호 수준 실태조사" 참조 및 연구자가 재구성

2.3.3 중소기업 기술유출방지를 위한 관리 실태

<표 10> 중소기업 기술유출방지를 위한 관리 실태

번호	관리항목	관리실태
1	기술 유출 사고 발생 주된 이유	중소기업의 기술 유출사고가 발생하는 주된 이유로는 '보안관리 감독체계 미흡'이 45.8%로 가장 많고, 다음으로 '임직원들의 보안의식 부족' 43.1%, '보안관련 투자 미흡' 26.5% 등의 순으로 조사됨
2	기술유출 방지를 위해 시급한 부분	중소기업의 기술유출 방지를 위해 시급한 부분으로는 '인력관리'가 52.4%로 가장 높았으며, 다음으로 '유출시 처벌 법규 강화' 26.3%, '보안시설 장비도입' 10.7% 등의 순으로 조사됨
3	중요 기술 거래기업 제공 요구	중소기업의 4.5%는 거래기업(대기업 등)으로부터 보유한 중요 기술자료 제공을 요구받은 경험이 있는 것으로 나타남
3.1	제공 요구 시 대응	거래기업으로부터 중요 기술자료 제공 요구를 받은 중소기업의 대응으로는 '쌍방 합의하에 조건부 제공'이 60.6%로 가장 높은 것으로 나타남
3.2	기술 제공 시 대응	중요 기술 제공 시 대응 방법으로 '기술요구 서면요청 및 비밀유지 협약체결'이 중소기업은 60.5%인 반면 대기업은 73.8%로 대기업이 더 높은 것으로 조사됨

4	기술보안 담당 인력	전체 중소기업의 기술보안 담당 인력은 평균 1.0명으로 대기업 평균 8.3명에 비해 낮은 수준인 것으로 나타남
5	핵심인력 외부유출 경험	최근 3년간(2013~2015년) 내부 단순인력을 제외한 핵심인력이 외부로 유출된 경험은 대기업은 4.0%, 중소기업은 3.4%로 나타나며, 대기업이 중소기업보다 핵심 인력의 외부유출 경험이 더 많은 것으로 나타남
5.1	기술 인력 유출 대상	중소기업에서 기술 인력이 유출된 대상으로는 '경쟁업체'가 54.7%로 가장 많고, 기업규모가 클수록 응답비율이 높은 경향이 있음
6	보안관리 애로사항	중소기업의 기술보호를 위한 보안관리에 있어 가장 큰 애로사항(매우 그렇다+그렇다 응답비율 기준)으로는 '보안전담 인력부족'(43.0%), '보안시설 부족'(41.2%), '예산 부족'(36.7%) 등의 순으로 나타남

자료 : 중소기업청(2017), "2016년 중소기업 기술보호 수준 실태조사" 참조 및 연구자가 재구성

2.3.4 유출/비유출 기업 기술보호 역량점수

유출기업의 기술보호 역량점수는 45.0점으로 비유출기업 49.3점 대비 4.3점 낮으며, 평가부문별 역량점수는 모든 부문에서 비유출기업이 유출기업에 비해 상대적으로 높게 나타남. 특히 보안정책 수립 부문에 있어 점수 차가 9.2점으로 가장 크게 나타나고 세부항목별 역량점수는 <표 11>과 같이 확인됨.

<표 11> 유출/비유출 기업 세부항목별 역량점수

(단위 : 점)

평가부문	평가항목	역량점수	
		유출기업	비유출기업
보안정책 수립	보안규정의 제정 및 공표	51.9	65.6
	회사 차원의 대응절차/방안 마련	41.3	63.0
	보안 위반직원에 대한 공식적 징계절차 마련	39.4	55.5
	보유자산에 대한 체계적인 보안관리	51.0	73.6
	기술보호 투자금액	59.2	58.0
	보안관리부서 및 보안관리자 지정·운영	28.4	23.5
	CEO/임원, 부서장, 직원의 기술보호 필요성 인식수준	71.1	63.7
	부문별 종합	49.9	59.1
보안관리	건물입구 유/무인 경비시스템 운영	48.1	58.3
	별도의 외부인 접견실 운영	57.7	71.8
	주요 출입구 관리·통제 경비시스템 운영	28.4	28.2
	주요 정보에 대한 관리시스템 운영	83.7	90.5
	중요 자산의 보호/격리를 위한 구역 지정·운영	55.0	45.2
	정기적인 보안감사 실시	30.8	39.1
	정보화 기기 반입 및 반출 통제	23.1	19.8
	업무용-인터넷용 통신망 분리	37.5	33.9

	정보시스템의 사용 로그 기록·관리	33.5	36.0
	디지털자산 관리용 보안솔루션 운영	17.3	23.7
	OS, 백신 등 업데이트 관리	86.5	87.0
	부문별 종합	40.1	42.0
인력관리	직원 보안교육 실시	62.2	63.0
	퇴근 혹은 자리이탈 시 보안활동 수행	63.5	79.1
	보안서약서 징구 여부	69.2	64.7
	보안서약서 징구대상	18.7	18.1
	핵심인력에 대한 '경쟁업체 전직 금지 서약서' 징구	44.2	39.1
	퇴사자의 진로 및 동향 파악	31.7	21.5
	직무발명 보상제도 운영	30.8	35.5
	부문별 종합	46.3	49.5
보안사고 및 재해관리	중요시설과 통제구역의 홍수, 전기, 화재 등에 대비한 재해방지대책 수립·시행	53.8	63.8
	중요자료 보관(백업) 대책 수립·시행	55.8	50.4
	부문별 종합	55.0	55.7
전체종합		45.0	49.3

자료 : 중소기업청(2017), “2016년 중소기업 기술보호 수준 실태조사” 참조 및 연구자가 재구성

2.4 보안역량진단에 대한 영향요인

지식정보사회로 점차 고도화하는 과정 속에서 현대의 기업은 조직을 운영하는데 보안위험을 장애요소로 인식하고 있으며, 기업의 보안 실패로 인하여 조직이 존폐 될 수 있다(Baker & Wallance, 2007 Johnston & Warkention, 2010). 조직의 보안사고 발생은 대부분 외부인력보다는 내부인력에 의해 일어나고 있으며, 외부요인으로부터 발생되는 보안위협의 파급력 보다 내부인력으로부터 발생되는 것이 더 크다(Bulgurcu et al, 2010). 한편, 조직의 조직원을 대상으로 한 보안인식 교육과 체계적인 보안정책 수립은 조직원에게 보안인식 개선의 동기 제공과 조직 내부의 보안위협을 감소시키므로 조직의 보안성과에 긍정적인 영향을 준다는 것은 다수의 선행논문을 통해 확인한 바 있다. 이러한 추세로 최근의 산업보안연구는 대부분 기술보호와 조직의 보안정책수립을 중심으로 추진되고 있다(정병수 외, 2012). 기업의 상황에 적절한 보안정책의 수립과 체계적인 수행은 기업의 보안성과와 대외적인 경쟁력 확보에도 긍정적인 영향을 미친다(Siponen, 2000 강다연 & 장명희, 2012). 산업보안은 다른 분야보다 보안에 대한 적절한 정책 및 지침의 수립이 중요하고 체계적인 구축으로 보안취약점을 감소시킬 수 있다(Hone & Eloff, 2002). Choi et al.(2008)와 김종기 & 강다연(2008)은 정보보안의 관리적 행동과 정보보안인식에 관한 연구에서 조직원의 정보보안인식 제고에 조직의 정보보안정책이 주요한 영향을 미친다고 했다. Ives et al.(1984)와 Kankanhalli et al.(2003), Werlinger et al.(2009), 오창규 & 김종기(2003)는 경영진의 정보보호에 대한 관심과 지원을 조직의 보안관리에 가장 중요한 요인으로 선정하였고 Post & Kagan(2000)은 정보자산의 중요성을 경영진이 인식하여야 보안투자로 연결되어 조직의 자산보호활동에 긍정적인 영향을 준다고 주장했다. 한편, 특허와 같은 기술전유수단이 기술

유출방지에 긍정적인 영향을 줌을 실증한 논문도 찾아볼 수 있었다. 김병근 & 박성근(2014), 강헌(2014)은 기술보호와 개발을 위하여 특허 등의 법적제도 활용이 필요하다고 주장했다. Arundel(2001), 노민선 & 이삼열(2010)도 특허가 산업보안역량과 기술보호에 긍정적인 영향을 주는 것으로 실증하였다. 박찬수 & 황정하(2013)는 기업의 핵심이슈는 새로운 기술의 개발과 동시에 보유기술을 철저히 보호하는 것이라고 주장했다. 정부와 기업의 R&D가 지속적으로 지원되고 있으며, 기술의 변화는 가속화되고 있지만 기술보호 대책은 미진하다는 것이다. 김범석 외(2013)와 이장우(2011)는 대기업과 중소기업간 양극화를 심화시킨 중요한 요인으로 원가절감을 위한 대기업의 중소기업 대상 기술탈취를 선정했다.

서동진(2016)은 기업의 기술보호역량에 영향을 줄 것으로 생각되는 요인을 특허와 같은 법적제도의 활용, 경영진의 보안에 대한 관심, 조직의 적절한 보안지침 관리와 수립, 거래기업으로부터의 기술탈취위험, 활발한 R&D활동 5가지로 도출하였으며, 기업의 기술보호역량을 향상시키는데 경영진의 의지가 가장 중요한 요인임을 실증하였다.

2.5 보안성과의 정의

홍기향(2004)은 정보보안성과란 조직이 보안관리 활동이나 통제를 통해 취하고자 하는 목적으로 소극적 목적으로 손실 방지와 보안 사고의 예방이 있고 적극적 목적으로 공공이미지, 고객 만족, 경쟁우위와 같이 보안과 관련된 사항이 있다고 하였다.

신한길(2005)은 정보보호 투자에 대한 성과를 자산의 손실검수 감소, 정보보호 사고의 감소, 타사 경쟁 시 손해 감소, 비즈니스 기회손실 감소, 사고

발생 시 신속한 처리, 이미지 실추 건수 감소 등으로 구분하고 성과측정을 하위요인화 하였다.

김경규(2009)는 정보보호 성과를 정보보호 성과와 정보자산성과로 구분하고 정보보호 성과로는 자산손실방지, 이미지 유지, 비즈니스 연속성, 고객유지 및 확보 요인으로, 정보자산 성과는 보안사고, 만족도, 협력사 간 신뢰도, 인식제고, 개인정보 보호로 하위요인화 하였다.

김재수(2014)는 기업의 핵심자산을 보호하는 것을 정보보안이라 정의하고 기업이 보유하는 자산으로는 무형자산, 유형자산, 인적자산으로 구분하고 하위요인을 핵심정보자산의 예로는 경영기획자료, 일반관리, 영업정보, 제조·생산, 연구개발 등으로 구분하였다. 업무 생산성 및 보안성을 고려한 산업보안 환경을 운영하면 업무생산성과 공간활용, 편의성 등의 극대화를 이룰 수 있다고 주장하였다.

이러한 연구를 볼 때 보안성과란 예방성과와 대응성과로 구분되며, 예방성과는 “개인 또는 조직의 성과를 위험, 손실 및 범죄가 발생하지 않도록 보호하는 상태를 지속하여 지정된 목표를 달성하는 것”이며, 대응성과는 피해가 우려 및 발생 시 대응하는 것으로 설명할 수 있다.

2.6 보안활동에 대한 선행연구

기술적 보안에 대한 연구로 노주하(2011)는 기술유출 방지를 위한 보안시스템 구축 방안에 관한 연구에서 기술유출사례의 분석을 통해 보안시스템 구축의 방안과 필요성을 주장하였고 이근주(2014)는 산업기술 유출방지를 위한 보안 감사 시스템 개발에 관한 연구에서 데이터 유출방지시스템, 디지털 포렌식을 통한 보안감사시스템 검증으로 기술적 보안에 대한 중요성을 제시

하였다.

관리적 보안에 대한 연구로 이정수(2011)는 산업보안을 위한 직무발명보상형태에 관한 연구에서 연구원의 설문지와 직무발명보상형태 분석을 실시하여 효과적인 보상제도를 제시하였고, 강푸름(2013)은 기술유출 대응매뉴얼, ISO27001, ISMS에서 요구하는 핵심인력 관리방안 분석을 통한 중소기업의 인력관리 방안을 중소기업 기술유출 방지를 위한 핵심인력 관리방안에 관한 연구에서 제시하였으며, 김학준(2014)은 관리적 보안체계 구축을 통한 산업보안 강화방안을 산업기술 유출사례를 통한 기업조직의 관리적 보안 개선방안에 관한 연구에서 제시하여 기술유출방지를 위한 관리적 방안을 제안하였다.

복합·통합적인 관리방안으로 전승준(2013)은 산업보안지원 요구와 산업기술 보호를 위한 기업의 보안수준강화 연구보안관제시스템을 통한 관리적, 기술적 기업 보안수준강화 방안을 제시하였다.

연희모(2013)는 내부자에 의한 산업기밀 유출방지방안으로 국내기업의 핵심인력관리 및 보상제도 확충을 통한 기술유출방지 방안을 제시하였고 이태규(2011)는 산업정보 유출 방지와 인적 신분, 직무별 관리, 보안인증제도, 보상제도 확충, 처벌강화, 애사심 강화를 통한 기술유출 방지 방안을 제시하였으며 김용찬(2013)은 시스템다이내믹스를 통한 산업기술유출방지정책연구에서 산업기술유출의 순환적 인간관계 분석을 통한 대응방안을 제시하고 기술유출동기가 시간이 지날수록 증가하기 때문에 인적자원 관리가 필요하다고 하였다.

또한 허재영(2009)은 중소기업의 산업보안을 위한 실증적 연구에서 사용자 태도, 산업보안시스템의 품질에 따른 기업의 보안시스템 적용여부에 관한 연구로 실증적인 기업의 보안시스템 구축방안에 대해 논의하였다. 이와 같이 선행연구들은 각 분야별로 적용을 위한 구체적인 방법과 실용성 검증에 대

해 대부분 연구하였으며, 보안활동의 강화는 보안성과 달성과 기술유출방지에 영향이 있는 것을 나타내고 있었다.

2.7 보안성과에 관한 선행연구

신현구(2014)는 산업보안정책 준수의지 영향요인에 관한 연구에서 개인요인에 따른 산업보안정책 준수의지 영향요인을 분석하여 성과를 도출하였고 손태현(2015)은 기업의 정보보호활동이 정보보안과 정보경영 성과에 미치는 영향, 정보보호활동이 정보보안, 정보경영에 유의한 결과를 나타냈다.

채정우(2013)는 산업보안 관리체계의 전략적 우선순위 결정에 대한 연구에서 기업의 산업보안관리 우선순위 제시를 통한 효과적 전략을 제시함으로써 산업보안의 대응방법 및 예방에 대해 구체적으로 논의하였다. 기업의 효율적인 기술유출방지를 위하여 구체적인 방안을 선행연구에서 제시하고 있으며, 이는 보안성과 달성을 위한 보안활동이 이루어지고 있다는 것을 알 수 있었다.

Ⅲ. 연구모형 및 가설

3.1 연구의 모형

본 연구에서는 중소·중견기업의 기술보호를 위하여 기업의 기술보호 역량 진단 시에 활용하는 중소·중견기업 보안역량 진단표에서 실질적으로 중요하다고 판단되는 보안부문과 세부보안 진단항목을 도출하였다. 도출한 보안부문의 세부보안 진단항목을 보안역량 속성으로서 기술보호대응책에 어떠한 영향을 주는지 분석하고 보안성과에 미치는 영향을 분석해보고 시사점을 도출하고자 한다. [그림 1]은 본 연구의 모형이다.

[그림 1] 연구의 모형

3.2 연구의 가설

3.2.1 보안역량진단이 기술보호대응책에 관한 가설

H1a. 보안정책은 기술보호대응책에 유의한 정(+)의 영향을 미칠 것이다.

H1b. 인적자원관리는 기술보호대응책에 유의한 정(+)의 영향을 미칠 것이다.

H1c. IT 설비관리는 기술보호대응책에 유의한 정(+)의 영향을 미칠 것이다.

H1d. IT 장애관리는 기술보호대응책에 유의한 정(+)의 영향을 미칠 것이다.

H1e. IT 기술적용은 기술보호대응책에 유의한 정(+)의 영향을 미칠 것이다.

3.2.2 기술보호대응책이 보안성과에 관한 가설

H2. 기술보호대응책은 보안성과에 유의한 정(+)의 영향을 미칠 것이다.

3.3 변수의 조작적 정의

연구의 조작적 정의는 아래 <표12>와 같다.

<표 12> 변수별 조작적 정의

변수명	문항수	조작적 정의	참고문헌
기업보안정책	5	기업이 보안정책 관련 사항에 대하여 보유 및 이행을 통하여 발생하는 기대	대·중소기업·농어업 협력재단 중소·중견기업 보안역량진단표
인적자원관리	6	기업이 보유하고 있는 인적자원이 수행하여야 할 보안활동들에 대한 대응 수준	대·중소기업·농어업 협력재단 중소·중견기업 보안역량진단표
IT 설비관리	4	IT 보안관리를 위한 IT 설비관리 분야의 대응 수준	대·중소기업·농어업 협력재단 중소·중견기업 보안역량진단표
IT 장애관리	2	IT 보안관리를 위한 IT 장애관리 분야의 대응 수준	대·중소기업·농어업 협력재단 중소·중견기업 보안역량진단표
IT 기술적용	6	IT 보안관리를 위한 IT 기술적용 분야의 대응 수준	대·중소기업·농어업 협력재단 중소·중견기업 보안역량진단표
기술보호 대응책	5	보안역량진단을 통해 발견되는 문제점을 조치하기 위한 대응방안의 필요성	대·중소기업·농어업 협력재단 중소기업 기술보호 지원제도
보안성과	3	보안역량진단을 통해 마련된 기술보호대응책으로부터 기대하는 보안성과 수준	한국산업기술보호협회 기업의 기술보호투자 및 위험수준에 따른 대응방안

3.4 연구 설계

3.4.1 자료의 수집 방법

본 연구는 보안역량진단이 보안성과에 미치는 영향을 설명하기 위하여 설문조사를 수행하였다. 설문조사는 2017년 9월 28일부터 2017년 10월 17일까지 E-mail과 직접방문에 의한 면접조사 방법을 실시하였다. 분석단위(unit of analysis)는 개인이며, Likert 7점 척도를 사용하여 측정하였다.

다른 조건이 동일하다면 척도항목 수가 많을수록 측정의 정확성이 높아지기 때문에 5점 보다는 7점 Likert를 사용하였으며, 표본의 수가 적은 경우에는 7점 척도를 적용하는 것이 적절하다.

본 연구에 사용된 변수들은 대·중소기업·농어업협력재단에서 보안역량진단표의 측정문항을 일부 활용하였으나 목적에 따라 일부 표현을 수정하거나 새로운 항목을 추가하였다.

3.4.2 설문지의 구성

본 연구의 설문 구성은 <표 13>과 같이 독립변수를 측정하기 위한 23개 문항과 기술보호대응책을 측정하기 위한 5개 문항, 보안성과 측정을 위한 3개 문항으로 Likert 7점 척도로 구성하였다. 설문 응답자의 특성 파악을 위해 일반적인 인구통계학적 특성 문항을 함께 질문하였다.

<표 13> 설문지의 구성

변 수	측 정 항 목
기업보안정책	• 보안규정을 보유 • 보안전담조직이 존재 • 회사의 주요 정보(기술, 영업 등)의 공유(업무담당자와 관계자만 공유, 전 직원이 공유 등) • 정기적으로 보안감사를 실시 • 회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용수준
인적자원관리	• 기존 임직원을 대상으로 보안교육 실시 • 임직원 퇴근 및 자리이탈 시에 보안활동 수행(PC전원 Off, 화면보호기 설정, 출입문과 캐비넷 시건 확인, 문서와 도면 방치 확인) • 신규 입사자와 주요 R&D 프로젝트 참가자에 대해 보안서약서를 징구 • 종업원이 보안정책, 지침, 절차 등을 위반하는 경우 직원에 대한 공식적인 징계 절차 마련과 징계조치 실시 • 제3자(협력업체, 외국인 등)에 대한 관리(관리방안 마련 및 보안서약서 징구)
IT 설비관리	• 정보처리 설비의 운영절차를 문서화하여 규정(컴퓨터의 가동과 종료절차, 백업절차, 유지 보수절차) • 서버, DB 현황, 통신망에 대한 보안점검을 실시 • 내부 통신망과 외부 통신망(인터넷, 협력회사 등)을 분리하여 운영 • 정보시스템의 사용 내용에 대한 로그의 기록과 유지
IT 장애관리	• 주요 장애 발생 시 장애내용이 보고되어 신속하게 시정조치 실시 • 정보시스템에 대한 유지보수를 실시
IT 기술적용	• PC와 주요 시스템 사용자에 대한 패스워드 관리(정례

	적으로 패스워드 변경, 변경점검 등) • 바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구(보안솔루션 도입 사용) • 내부에서 생성된 주요 정보 및 소프트웨어의 백업과 관리 • 지식관리시스템(KMS), 전자결재시스템 등 회사 내 주요 정보에 대한 관리시스템을 사용 • CD, USB 등 정보의 저장이 가능한 저장매체에 대한 관리절차를 마련(저장매체 사용통제, 회사 지정 저장매체 사용) • 외부로의 전자문서 발송에 대한 통제시스템의 마련(E-Mail 등 통제)
기술보호 대응책	• 기술유출 관련 애로사항을 해결하기 위해 보안정책, 보안시스템, 법률자문분야에 대해 최대 3일간 코칭서비스를 제공(사전진단/무료) • 사전진단 결과, 기술유출 위험에 직면하거나 피해를 입은 기업에 대해 최대 7일간 심화자문 코칭서비스를 제공 • 기술자료 임치제도 지원 - 기술자료를 임치금고에 보관하며, 기술유출 발생 시 해당기술의 개발과 보유사실 입증 • 기술지킴(보안관제) 서비스 지원(무료) - 365일 실시간 유출과 비정상 행위의 모니터링, 사용자 통계보고, 상담 운영 • 기술유출방지시스템 구축 지원 - 보안인프라 환경 진단 및 기술유출방지를 위한 보안시스템 구축 비용 지원
보안성과	• 외부협력기관과의 관계 및 신뢰도 제고로 대외적 성과 향상 • 기술유출 위험 감소와 임직원 보안의식 고취로 전반적인 보안역량 향상 • 보유기술의 가치 극대화로 기술경쟁력 유지 향상

3.4.3 자료 분석 방법

설문 분석을 위해 통계 패키지인 Smart PLS 2.0을 사용하였다. 자료분석 방법으로는 설문 응답자의 인구통계적 특성을 파악하기 위하여 빈도분석(frequency analysis)을 수행하였고 설문지의 신뢰도를 측정하기 위하여 설문의 내적 일관성을 나타내는 크론바하 알파(Cronbach Alpha)를 통한 신뢰성 분석과 타당성 분석을 위해 요인분석(factor analysis)을 실시하였다. 그리고 가설 검증을 위해 구조방정식(structural equation) 접근방법인 부분최소제곱법(PLS)과 조절효과 분석을 위해 조절회귀분석을 사용하였다.

PLS란 Partial Least Squares 라는 말의 약자로 부분최소자승법을 이용해 구조방정식모델을 추종하는 기법을 사용하는 방법론을 의미한다. 주성분분석(principle component testimation)을 기반으로 계수를 측정하는 성분기반 접근방식(component-based approach)을 사용하는 구조방정식모델이다(구동모, 2013, p329).

PLS는 LISREL과 달리 측정오차에 대한 통제가 불가능하다는 단점이 있지만 구조방정식 모형을 분석하기 위한 다른 방법들에 비해 작은 표본 크기에도 분석이 가능하고 잔차 분포의 영향도 적게 받는다는 장점을 갖고 있다(Chin, 1988).

Ⅳ. 실증 분석

4.1 기초 자료 분석

본 연구의 실증적 분석을 위하여 설문지를 E-mail 140부, 직접 21부를 배부하였고 이 중 E-mail 76 부와 직접 설문 응답한 21부가 회수되었으며, 총 97부의 설문을 이용하여 분석하였다.

<표 14>는 연구에 사용된 응답자의 인구통계학적 특성이다. 응답자의 남·여 비율은 각각 81.25%와 18.75%로 차이가 많으며, 연령대의 경우는 30대가 전체 응답자의 35.41%를 차지하여 다소 젊은 층에 편중 되어 있고 학력의 경우는 대학졸업(재학포함)이 44.79%로 가장 많이 차지하고 있다. 또한 직위의 경우는 차·과장이 28.12%로 가장 많으나 전반적으로 나누어져 있고 근무부서의 경우는 기술개발(연구소)가 46.87%로 거의 절반을 차지하고 있으며, 주력업종은 SW·정보처리 58.33%로 편중되었다.

<표 14> 인구통계학적 특성(n=97)

항목		빈도수	비율(%)
성별	남	78	81.25
	여	18	18.75
연령	20대	16	16.66
	30대	34	35.41
	40대	23	23.95
	50대	18	18.75
	60대 이상	5	5.20
학력	고졸	6	6.25
	전문대 졸업(재학포함)	26	27.08
	대학 졸업(재학 포함)	43	44.79
	대학원 졸업(재학포함) 이상	21	21.87
직위	사원	16	16.66
	대리	18	18.75
	차·과장	27	28.12
	부장	13	13.45
	임원	22	22.91
근무부서	관리	24	25
	영업	12	12.5
	기술개발(연구소)	45	46.87
	생산	6	6.25
	품질	9	9.37
주력업종	전기/전자	10	10.41
	기계	9	9.37
	금속가공	0	0
	SW·정보처리	56	58.33
	통신	4	4.16
	화학(플라스틱)	6	6.25
	광학기기	2	2.08
	기타	9	9.37

4.2 신뢰도 및 타당성 분석

4.2.1 신뢰성 분석

신뢰성(reliability)이란 넓은 의미에서 측정상의 오류가 발생되지 않을 정도로 연구대상인 응답자에게 반복적인 측정을 했을 경우에 응답결과가 얼마나 일관성 있게 나타났느냐를 판단하는 개념이다.

본 연구에서도 신뢰성 측정을 위하여 측정항목간의 내적 일관성을 검증하는 Cronbach's α계수, 합성 신뢰성(CR; composite reliability) 그리고 평균분산 추출(AVE; average variance extracted) 값을 통해 확인하였다. Cronbach's α계수는 일반적으로 0.7이상이면 신뢰성이 인증된다고 보며, CR 값은 보통 0.7 이상일 때, AVE 값은 0.5이상이면 측정변수들의 신뢰성이 확보된 것으로 본다.

<표 15>에 제시된 바와 같이, 본 연구에서 고려된 모든 변수들의 크론바 알파 값은 0.523~0.914 사이의 값을 나타내고 있어, 임계값인 0.7을 모두 상회하고 있으며, CR 값도 모두 0.781 이상으로 임계값 0.7을 상회하고 있음을 확인 할 수 있다. AVE 값도 모두 0.632를 상회하고 있어 임계값인 0.5를 상회하고 있음을 알 수 있다. 이러한 결과들을 토대로 본 연구에서 고려하고 있는 변수들의 신뢰성이 확보되고 있음을 알 수 있다.

4.2.2 타당성 분석

타당성(validity)이란 최대한 상이한 방법을 사용하여 동일한 속성을 두시도 간

결과의 일치 정도로써 연구자가 측정하고자 하는 개념을 얼마나 정확하게 측정하였는가의 문제라고 할 수 있다. 본 연구에서 설정한 전체 모형에 대한 집중 타당성의 경우, <표 15>에 제시된 바와 같이, 요인적재 값이 모두 모두 0.6보다 큰 값을 보이고 있어 집중 타당성도 확보된 것으로 판단된다.

이와 같이 측정도구의 신뢰성 및 타당성이 검정되어 최종적 문항들을 기반으로 가설검정을 실시하였다.

<표 15> 연구모형의 확인적 요인분석 수행결과

변수명		요인적재량	C.R	AVE	Cronbach's α
기업 보안정책	A1	0.732	0.878	0.645	0.818
	A2	0.881			
	A3	0.734			
	A4	0.854			
인적자원 관리	B1	0.788	0.895	0.632	0.856
	B2	0.761			
	B3	0.858			
	B5	0.816			
	B6	0.746			
IT 설비관리	C1	0.926	0.909	0.834	0.803
	C2	0.900			
IT 장애관리	D1	0.937	0.950	0.905	0.897
	D2	0.965			
IT 기술적용	E1	0.632	0.781	0.649	0.723
	E5	0.948			

기술보호 대응책	Y1	0.904	0.935	0.745	0.914
	Y2	0.883			
	Y3	0.807			
	Y4	0.853			
	Y5	0.864			
보안성과	Z1	0.908	0.944	0.850	0.912
	Z2	0.942			
	Z3	0.916			

4.2.3 상관관계분석

본 연구에서 설정한 가설검증을 실시하기에 앞서 모든 연구가설에 사용되는 측정변수들 간의 관련성을 분석하고 만약 관련성이 있다면 어느 정도 관련이 있는지 파악하기 위하여 상관관계 분석을 실시하였다.

상관관계 분석에 의한 상관계수(correlation coefficient)는 0에서 ±1사이로 나타나며, ±1에 가까울수록 상관관계는 높아지고 0에 가까울수록 상관관계는 낮아진다. 즉, 변화의 강도는 절대값 1에 가까울수록 높고 변화의 방향은 (+)는 정의 방향, (-)는 음의 방향이라고 한다. 상관관계 분석에서 변수들 간의 관련성 정도를 판단하는 기준은 ±0.9이상은 매우 높은 상관관계, ±0.7~0.9미만은 높은 상관관계, ±0.4~0.7미만은 다소 낮은 상관관계, ±0.2~±0.4미만은 낮은 상관관계, ±0.2미만은 상관관계가 거의 없는 것으로 판단한다.(송지준, 2013, p121).

일반적으로 Pearson 상관계수가 0.6이상이 나타나면 다중공선상이 존재한다

고 하지만, 판별타당성을 통해 다중공선성을 확인 할 수 있다. 판별타당성 검증은 평균분산추출량(AVE)과 요인들 간 상관계수 값을 이용하여 분석할 수 있으며, AVE 제곱근의 값이 다른 구성개념간의 상관관계 값보다 클 경우, 판별타당성이 있다고 판단한다.

판별타당성 검증을 위해 <표 16>과 같이 상관계수와 분산추출지수(AVE)를 비교해 본 결과 모든 구성 개념간의 상관계수가 대각선으로 표시된 분산 추출지수가 각 요인의 상관계수의 제곱, 결정계수보다 크게 나타나 연구 요인들 사이에 존재하는 판별타당성이 확보되었으며, 다중공선성에는 문제가 없는 것으로 판단된다.

<표 16> 상관관계 및 판별타당성 분석 결과

변수명	AVE	기술보호대응책	IT 기술적용	기업보안정책	보안성과	IT 설비관리	인적자원관리	IT 장애관리
기술보호대응책	0.745	**0.863**						
IT 기술적용	0.649	0.448	**0.805**					
기업보안정책	0.645	0.506	0.483	**0.803**				
보안성과	0.850	0.713	0.572	0.537	**0.921**			
IT 설비관리	0.834	0.286	0.445	0.635	0.381	**0.913**		
인적자원관리	0.632	0.593	0.399	0.588	0.602	0.629	**0.794**	
IT 장애관리	0.905	0.141	0.403	0.448	0.248	0.584	0.468	**0.951**

* 대각선의 값은 AVE의 제곱근 값을 나타냄

4.3 가설 검증

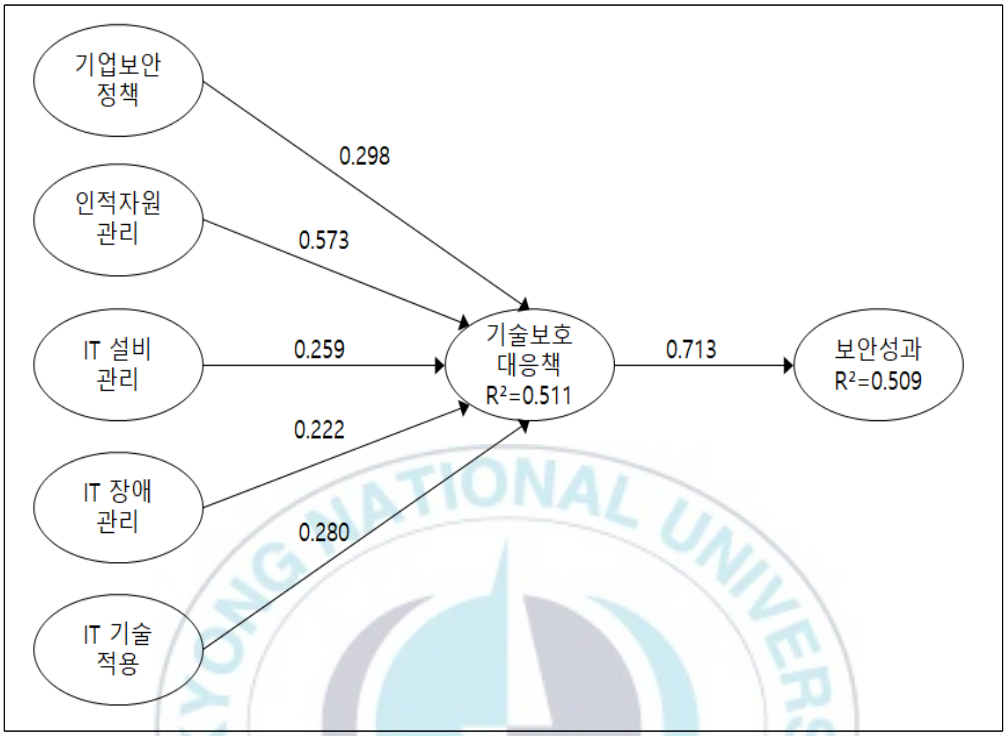
4.3.1 연구모형의 적합도 분석

구조모형 분석은 Smart PLS 2.0을 사용하였으며, 구조모형 분석을 통하여 경로계수와 내생변수에 대한 결정계수(R^2)값을 도출하였다. 내생변수에 대한 결정계수(R^2)의 결과 값은 예측변수가 갖는 총 변동 중에서 회귀선, 독립변수에 의해 설명되는 비율을 의미한다. R^2값이 0.26이상인 경우는 적합도를 '상', 0.26~0.13인 경우는 적합도를 '중', 0.13이하인 경우는 적합도를 '하'로 표시할 수 있다(Cohen, 1988). 구성요소 값이 기술보호대응책과 보안성과 각각에 대하여 '상'으로 평가 할 수 있다.

4.3.2 가설의 검정

본 연구 모형에서 타당성과 신뢰성 검증 과정에서 제외한 8개의 문항인 기업보안정책의 A4, 인적자원관리의 B4, IT 설비관리의 C3, C4, IT 기술적용의 E2, E3, E4, E6를 제거하고 구조모형 분석을 통해 각 가설을 검증하였다.

가설을 검증한 결과는 다음의 [그림 2]에 제시하였으며, 본 연구에서 제안한 가설들은 모두 채택되었다.



[그림 2] 구조모형 분석 결과

<가설 1>의 기업보안정책이 기술보호대응책에 미치는 영향을 검정한 결과 긍정적인 영향을 미치는 것으로 나타나 가설 1은 채택되었다.

<가설 2>의 인적자원관리가 기술보호대응책에 미치는 영향을 검정한 결과 긍정적인 영향을 미치는 것으로 나타나 가설 2는 채택되었다.

<가설 3>의 IT 설비관리가 기술보호대응책에 미치는 영향을 검정한 결과 긍정적인 영향을 미치는 것으로 나타나 가설 3은 채택되었다.

<가설 4>의 IT 장애관리가 기술보호대응책에 미치는 영향을 검정한 결과 긍정적인 영향을 미치는 것으로 나타나 가설 4는 채택되었다.

<가설 5>의 IT 기술적용이 기술보호대응책에 미치는 영향을 검정한 결과 긍정

적인 영향을 미치는 것으로 나타나 가설 5는 채택되었다.

<가설 6>의 기술보호대응책이 보안성과에 미치는 영향을 검정한 결과 긍정적인 영향을 미치는 것으로 나타나 가설 6은 채택되었다.

채택된 모든 가설들은 선행연구와 기업의 보안역량진단에서 각각의 원인변수와 결과변수 간에 유의한 영향을 미치는 것으로 규명한 연구와 일치한 결과이다.

<표17>은 본 연구에서 설정한 가설들에 대한 검증 결과를 종합적으로 정리하여 제시하고 있다.

<표 17> 연구모형의 가설 검증 결과

가설	원인변수	결과변수	경로계수	t-값	결과
H1	기업보안정책	기술보호대응책	0.298	2.135	채택
H2	인적자원관리	기술보호대응책	0.573	4.040	채택
H3	IT 설비관리	기술보호대응책	0.259	2.013	채택
H4	IT 장애관리	기술보호대응책	0.222	2.361	채택
H5	IT 기술적용	기술보호대응책	0.280	2.096	채택
H6	기술보호대응책	보안성과	0.713	9.249	채택

t=1.645'' (p<0.05) t=3.30''' (p<0.001)

Ⅴ. 결 론

5.1 연구 결과 요약 및 시사점

본 연구에서는 보안성과에 영향을 미치는 보안역량진단요인과 기술보호대응책을 매개로 실증분석을 실시하였다. 중소·중견기업의 기술보호를 위하여 지원하는 기술보호상담 및 기술보호컨설팅 체계를 바탕으로 연구모형을 설정하였고 가설을 검증하기 위하여 편미분 구조방정식인 Smart PLS 2.0을 사용하여 실증연구를 하였다.

본 논문의 연구결과를 요약하면 다음과 같다.

첫째, 보안정책은 기술보호대응책에 유의한 정(+)의 영향을 미치는 것으로 나타났다.

둘째, 인적자원관리는 기술보호대응책에 유의한 정(+)의 영향을 미치는 것으로 나타났다.

셋째, IT 설비관리는 기술보호대응책에 유의한 정(+)의 영향을 미치는 것으로 나타났다.

넷째, IT 장애관리는 기술보호대응책에 유의한 정(+)의 영향을 미치는 것으로 나타났다.

다섯째, IT 기술적용은 기술보호대응책에 유의한 정(+)의 영향을 미치는 것으로 나타났다.

여섯째, 기술보호대응책은 보안성과에 유의한 정(+)의 영향을 미치는 것으로

나타났다.

본 연구의 분석결과를 통한 시사점은 중소·중견기업의 기술보호대응책에 영향을 미치는 보안역량진단의 요인으로서 IT 설비관리와 IT 장애관리 보다는 IT 기술적용과 기업보안정책 및 인적자원관리를 중요한 요인으로 인식하고 있는 것으로 나타났으며, 기술보호대응책은 보안성과에 중요한 요인으로 인식하고 있는 것으로 나타났다.

5.2 연구 한계점 및 향후 연구 방향

본 연구의 한계점과 향후 연구 방향은 아래와 같다.

첫째, 본 연구의 분석 대상이 30대 연령에 편중되었고 근무부서가 기술개발(연구소)가 절반 가까이를 차지하고 있으며, 주력업종은 SW·정보처리에 58.33%로 절반이상이 치중되어 있는 현상이 나타났다. 향후 연구에서는 조사대상의 표본을 사전에 잘 추출하여 편향성을 감소시키고 연구의 일반화를 기하고자 한다.

둘째, 본 연구모형의 기술보호정책과 보안성과에 영향을 미치는 보안역량진단 변수에 대한 추가적인 고찰을 통한 연구의 정교화가 필요할 것이다.

셋째, 중소·중견기업 보안역량진단표의 진단항목이 현 시점의 중소·중견기업의 보안환경에 적합한가에 대한 검토를 통해 재정립이 필요하며, 이를 위한 기초자료로 활용할 수 있는 근거 제공을 위한 연구가 필요하다.

참고 문헌

<국내문헌>

강다연, 장명희(2012), “해양항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인”, 한국항만경제학회지, 28(1), 1-23.

강푸름(2013), “중소기업 기술유출 방지를 위한 핵심인력 관리 방안에 관한 연구”, 경기대학교 대학원 석사학위논문.

강헌(2014), “중소기업기술 보호방안”, 아주법학, 8(3), 55-74.

구동모(2013), “SPSS, LISREL, PLS 및 PROCESS를 활용한 기초, 조절 매개효과 분석을 위한 연구방법론”, 서울: 학현사, 329.

김경규(2009), “정보자산보호 성과가 정보보호 성과에 미치는 영향에 관한 연구“, 정보관리연구, 40(3).

김범석, 강맹수, 민재형(2013), “원청-하청 기업 간 거래 건전성 평가를 위한 동반성장지수 개발”, Korea Business Review, (17)1, 225-242.

김병근, 박성근(2014), “중소기업에서 기술협력, 전유수단과 지식일출이 기술혁신성과에 미치는 영향”, 경영학연구, 43(1), 95-120.

김용찬(2013), “시스템다이내믹스를 통한 산업기술유출방지정책연구”, 서울과학종합대학교대학원 석사학위논문.

김재수(2014), “산업보안발전 및 산학연계를 위한 기업문화와 산업보안의 현재와 미래과제”, 2014년 한국산업보안연구학회 상반기 제9회 학술세미나.

김종기, 강다연(2008), “보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향”, 정보보호학회 논문지, 18(4), 123-133.

김학준(2014), “산업기술 유출사례를 통한 기업조직의 관리적 보안 개선방안에 관한 연구”, 서울과학종합대학교대학원 석사학위논문.

노민선, 이삼열(2010), “중소기업의 산업보안 역량에 대한 영향요인 평가”, 한국행정학보, 44(3), 239-259.

노주하(2011), “기술유출 방지를 위한 보안시스템 구축 방안에 관한 연구 : 기술적 보안을 중심으로”, 서울과학종합대학교대학원 석사학위논문.

박찬수, 황정하(2013), “기술유출에 대한 범국가적 대응 방안”, 과학기술정책연구원.

서동진(2016), “국내기업의 기술보호수준에 영향을 주는 요인에 관한 연구”, 충북대학교대학원 석사학위논문.

선한길(2005), “국내 기업의 정보보호 정책 및 조직 요인이 정보보호 성과에 미치는 영향”, 경영정보학회 춘계학술대회.

손태현(2015), “기업의 정보보호활동이 정보보안과 정보경영 성과에 미치는 영향”, 명지대학교 대학원 박사학위논문.

송지준(2013), “논문작성에 필요한 SPSS/AMOS 통계분석방법”, 파주시, 21세기사.

신현구(2014), “산업보안정책 준수의지의 영향요인에 관한 연구 : 조직요인과 개인요인을 중심으로”, 경기대학교대학원 박사학위논문.

연희모(2013), “내부자에 의한 산업기밀 유출방지 방안”, 성균관대학교 국가전략대학원 석사학위논문.

오창규, 김종기(2003), “효과적인 정보보호 교육 및 훈련을 위한 프레임워크 개발”, 정보보호학회 논문지, 13(2), 59-69.

이근(2002), “지적재산권과 기업의 특허전략”, 과학기술정책, (138), 24-31.

이근주(2014), “산업기술 유출방지를 위한 보안 감사 시스템 개발”, 남서울대학교대학원 석사학위논문

이장우(2011), “한국형 동반성장 정책의 방향과 과제”, 중소기업연구, 33(4), 77-93.

이정수(2011), “산업보안을 위한 직무발명보상 형태에 관한 연구 : 금전보상과 결합보상을 중심으로”, 서울과학종합대학교대학원 석사학위논문.

이태규(2011), “산업정보유출 방지와 인적 보안관리”, 성균관대학교 국가전략대학원 석사학위논문.

전승준(2013), “산업기술 보호를 위한 기업의 보안 수준 강화 연구”, 한국산업기술대학교 산업기술경영대학원 석사학위논문.

정병수, 류상일, 김화수(2012), “산업보안의 연구경향분석-학술연구정보서비스 (2000년~2011년)를 중심으로”, 한국행정논집, 9(2), 195-215.

채정우(2013), “산업보안관리체계의 전략적우선순위결정에 대한 연구”, 서울과학종합대학교대학원 박사학위논문.

허재영(2009), “중소기업의 산업보안을 위한 실증적 연구”, 한양대학교대학원 석사학위논문.

홍기향(2004), “정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구”, 국민대학교대학원 박사학위논문.

<국외문헌>

Arundel, A. (2001). "The relative effectiveness of patents and secrecy for appropriation", Research policy, 30(4), 611-624.

Baker, W. H., &Wallace, L. (2007). "Is information security under control: Investigating quality in information security management", Security &Privacy, IEEE, 5(1), 36-44.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS quarterly, 34(3), 523-548.

Chin, W. W. (1988). "The Partial Least Squares Approach to Structural Equation Modeling", in G. A. Marcoulides(ed.), Modern Methods for Business Research, 22(1), 7-16.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). "Knowing is doing: Anempirical validation of the relationship between managerial information security awareness and action", Information Management & Computer Security, 16(5), 484-501.

Cohen, J. O. (1988). Statistical power analysis for the behavioral science(2nd) hillsdale, new jersey: lawrence erlbaum associates, 90-200.

Hone, K., & Eloff, J. H. P. (2002). "Information security policy—what do international information security standards say?", Computers & Security, 21(5), 402-409.

Hong, S. C., “Recent SMEs main phase indicator changes cause and implications,” Focus for Korea Small Business Institute, 2014. 8. 13.

Ives, B., & Learmonth, G. P. (1984). "The information system as a competitive weapon", Communications of the ACM, 27(12), 1193-1201.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). "An integrative study of information systems security effectiveness", International journal of information management, 23(2), 139-154.

Mun, B. K., “The competitiveness in world export markets the number one item,” Trade Focus for Institute for International Trade, Vol. 14, No. 2, 2015.

National Industrial Security Center, “Technology Leakage Statistics,” 2014.

OECD, “2013 OECD Science, Technolog and Industry Scoreboard 2013,” 2013. 10.23.

Post, G., & Kagan, A. (2000). "Management tradeoffs in anti-virus strategies", Information & Management, 37(1), 13-24.

Siponen, M. T. (2000). "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice", Information Management & Computer Security, 8(5), 197-209.

Small and Medium Business Administration, “2013 Technology Protection Capabilitiy & Sueftyrvey on the level of Small &

Medium Business," 2014.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). "An integrated view of human, organizational, and technological challenges of IT security management", Information Management & Computer Security, 17(1), 4-19.

<설문지>

연구제목	**보안역량진단이 보안성과에 미치는 영향**

본 설문지는 중소·중견기업의 기술보호를 위한 보안역량에 대한 정보를 얻어 보안역량 속성이 기술보호대응책에 미치는 영향과 보안역량 속성이 보안성과 만족도에 미치는 영향을 연구하여 기술보호체계 향상 방안을 강구하고자 실시하고 있습니다.

기술보호를 위한 보안역량에 대한 귀하의 의견과 느끼신 생각을 알아보기 위한 것으로 모든 질문에 대하여 평소의 생각을 진솔하게 응답해 주시면 감사 하겠습니다.

본 조사는 무기명으로 실시되고, 그 결과는 익명성을 보장하며, 수집된 자료는 반드시 학위논문작성을 위한 학문적 목적에만 활용할 것을 약속드립니다. 본 설문지는 모두 익명으로 처리되며, 귀하의 응답내용은 통계법 제 8조에 따라 보호됨을 알려 드립니다.

바쁘신 와중에도 본 연구의 설문에 응답해 주셔서 깊은 감사드립니다.

귀하의 평안하심을 기원합니다.

2017년 9월 27일

지도교수 : 김 하 균
연 구 자 : 김 종 원
연 락 처 : 010-2447-9339
E-mail : atomkjw@naver.com

다음은 귀하의 일반적인 사항에 대한 질문입니다. 해당하는 번호에 체크 (∨) 해주십시오.

1. 귀하의 성별은?

①남자 ②여자

2. 귀하의 연령대는?

①20대 ②30대 ③40대 ④50대 ⑤60대 이상

3. 귀하의 학력은?

①고졸 ②전문대 졸업(재학 포함) ③대학 졸업(재학 포함)
④대학원 졸업(재학 포함)이상

4. 귀하의 직위는?

①사원 ②대리 ③차·과장 ④부장 ⑤임원

5. 귀하의 근무부서는?

①관리 ②영업 ③기술·개발(연구소) ④생산 ⑤품질

6. 귀사의 주력업종은?

①전기/전자 ②기계 ③금속가공 ④SW·정보처리 ⑤통신
⑥화학(플라스틱) ⑦광학기기 ⑧기타

다음의 설문을 읽으시고 귀하의 생각과 가장 가까운 번호에 체크(v) 해주십시오.

Ⅰ. 기업의 보안정책에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
보안규정을 보유	①	②	③	④	⑤	⑥	⑦
보안전담조직이 존재	①	②	③	④	⑤	⑥	⑦
회사의 주요 정보(기술, 영업 등)의 공유(업무담당자와 관계자만 공유, 전 직원이 공유 등)	①	②	③	④	⑤	⑥	⑦
정기적으로 보안감사를 실시	①	②	③	④	⑤	⑥	⑦
회사가 보유한 주요 정보 및 자산을 보호하기 위해 투자하는 비용수준	①	②	③	④	⑤	⑥	⑦

Ⅱ. 기업의 인적자원관리에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
기존 임직원을 대상으로 보안 교육 실시	①	②	③	④	⑤	⑥	⑦
임직원 퇴근 및 자리이탈 시에 보안활동 수행(PC전원 Off, 화면보호기 설정, 출입문과 캐비넷 시건 확인, 문서와 도면 방치 확인)	①	②	③	④	⑤	⑥	⑦
신규 입사자와 주요 R&D 프로젝트 참가자에 대해 보안서약서를 징구	①	②	③	④	⑤	⑥	⑦
종업원이 보안정책, 지침, 절차 등을 위반하는 경우 직원에 대한 공식적인 징계 절차 마련과 징계조치 실시	①	②	③	④	⑤	⑥	⑦
제3자(협력업체, 외국인 등)에 대한 관리(관리방안 마련 및 보안서약서 징구)	①	②	③	④	⑤	⑥	⑦
회사의 정보자산에 대한 사용자(임직원, 계약자, 제3의 사용자 등)들의 접근 권한은 퇴사, 계약종료, 역할 조정 등의 사유 발생 시 조정	①	②	③	④	⑤	⑥	⑦

Ⅲ. 기업의 IT보안관리에 대한 측정문항입니다.

3.1 IT 설비관리에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
정보처리 설비의 운영절차를 문서화하여 규정(컴퓨터의 가동과 종료절차, 백업절차, 유지 보수절차)	①	②	③	④	⑤	⑥	⑦
서버, DB 현황, 통신망에 대한 보안점검을 실시	①	②	③	④	⑤	⑥	⑦
내부 통신망과 외부 통신망(인터넷, 협력회사 등)을 분리하여 운영	①	②	③	④	⑤	⑥	⑦
정보시스템의 사용 내용에 대한 로그의 기록과 유지	①	②	③	④	⑤	⑥	⑦

3.2 IT 장애관리에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
주요 장애 발생 시 장애내용이 보고되어 신속하게 시정조치 실시	①	②	③	④	⑤	⑥	⑦
정보시스템에 대한 유지보수를 실시	①	②	③	④	⑤	⑥	⑦

3.3 IT 기술 적용에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
PC와 주요 시스템 사용자에 대한 패스워드 관리(정례적으로 패스워드 변경, 변경점검 등)	①	②	③	④	⑤	⑥	⑦
바이러스 침입, 해킹, 내부로부터의 정보유출을 방지하기 위한 대책을 강구(보안솔루션 도입 사용)	①	②	③	④	⑤	⑥	⑦
내부에서 생성된 주요 정보 및 소프트웨어의 백업과 관리	①	②	③	④	⑤	⑥	⑦
지식관리시스템(KMS), 전자결재시스템 등 회사 내 주요 정보에 대한 관리시스템을 사용	①	②	③	④	⑤	⑥	⑦
CD, USB 등 정보의 저장이 가능한 저장매체에 대한 관리절차를 마련(저장매체 사용통제, 회사 지정 저장매체 사용)	①	②	③	④	⑤	⑥	⑦
외부로의 전자문서 발송에 대한 통제시스템의 마련(E-Mail 등 통제)	①	②	③	④	⑤	⑥	⑦

Ⅳ. 기술보호 대응책에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
기술유출 관련 애로사항을 해결하기 위해 보안정책, 보안시스템, 법률자문분야에 대해 최대 3일간 코칭서비스를 제공(사전진단/무료)	①	②	③	④	⑤	⑥	⑦
사전진단 결과, 기술유출 위험에 직면하거나 피해를 입은 기업에 대해 최대 7일간 심화 자문 코칭서비스를 제공	①	②	③	④	⑤	⑥	⑦
기술자료 임치제도 지원 - 기술자료를 임치금고에 보관하며, 기술유출 발생 시 해당기술의 개발과 보유사실 입증	①	②	③	④	⑤	⑥	⑦
기술지킴(보안관제) 서비스 지원(무료) - 365일 실시간 유출과 비정상 행위의 모니터링, 사용자 통계보고, 상담 운영	①	②	③	④	⑤	⑥	⑦
기술유출방지시스템 구축 지원 - 보안인프라 환경 진단 및 기술유출방지를 위한 보안시스템 구축 비용 지원	①	②	③	④	⑤	⑥	⑦

Ⅴ. 보안성과에 대한 측정문항입니다.

설문내용	전혀 중요하지 않다	중요하지 않다	중요하지 않은 편이다	보통이다	중요한 편이다	중요하다	매우중요하다
외부협력기관과의 관계 및 신뢰도 제고로 대외적 성과 향상	①	②	③	④	⑤	⑥	⑦
기술유출 위험 감소와 임직원 보안의식 고취로 전반적인 보안 역량 향상	①	②	③	④	⑤	⑥	⑦
보유기술의 가치 극대화로 기술경쟁력 유지 향상	①	②	③	④	⑤	⑥	⑦

귀중한 시간을 할애하여 본 설문에 끝까지 응답해 주신 것에 대해 진심으로 감사드리며, 정성껏 작성해 주신 설문은 소중히 활용하겠습니다.