Journal of Convergence for Information Technology
Vol. 10. No. 11, pp. 332-339, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.11.332

국내 중소기업 정보보호 지원 정책 개선 방안에 관한 연구

장상수
한국인터넷진흥원 연구위원

A Study on Improvement Plans of SMEs Support Policy for Information Security in Korea

Sang-Soo Jang
Researcher, ICT Future Research Lab, Korea Internet & Security Agency

요 약 본 연구는 4차산업 혁명을 뒷받침하고 국가 경제의 중추적 역할을 하는 중소기업들이 해킹이나 기술유출 등으로 경제 활동을 할 수 없다면, 이는 국가 사회적, 경제적으로 엄청난 손실을 초래할 수 있다. 이러한 국내 중소기업에 대한 정부의 정보보호 지원 정책에 대해 형황 및 문제점 분석과 개선 방안을 도출하여 제시하는데 목적이 있다. 이를 위해 선행연구 검토 분석, 중소기업의 정보보호 실태 현황과 주요국의 중소기업 정보보호 지원 정책에 현황과 문제점을 분석해보고 분석결과를 토대로 실수요자인 중소기업들의 정보보호 지원 정책의 우선순위 등을 실태조사를 통해 검증하고자 한다. 연구결과 향상된 지원 정책으로 정보보호 인식제고 강화, 법적 근거 마련, 자발적 역량강화, 공동 대응체계 구축, 전문인력 및 예산 지원 강화, 지역 안전망 구축, 언택트 시대 지원 강화, 지역 전략산업 보안 내재화 등이 도출되었다. 이는 향후 포스트 코로나19 대비 중소기업의 정보보호 수준 제고를 위한 정부의 중소기업에 대한 정보보호 지원 정책으로 활용이 가능하다.

주제어 : 해킹, 기술유출, 중소기업, 정보보호 지원 정책, 인식제고, 보안 내재화, 사이버 안전망, 전략산업

Abstract This study aims to analyze problems and deduce improvement plans for information security support policies for SMEs in Korea. To this end, an effective support policy necessary for reinforcing cyber safety nets to enhance the level of information security of domestic SMEs based on the analysis results by analyzing the status and problems of the previous research review and analysis, the current status of information security of SMEs and the information security support policies of major SMEs at home and abroad. I would like to suggest improvement measures. Reinforcement of awareness, legal basis, voluntary capacity building, joint response system, professional manpower and budget support, cyber security construction, untact era support, and regional strategic industry security internalization were suggested. This can be used as the government's information security support policy to raise the level of information security of SMEs in preparation for the post Covid19.

Key Words : Hacking, Technology leak, SMEs, Information Security Support Policy, Raising awareness, Serity by Design, Cyber Security, Strategic industry.

1. 서론

1.1 연구의 필요성

지금의 언택트(untact) 시대, 4차 산업혁명과 지능정보화사회를 바라보는 시각에는 기대감와 두려움이 함께 공존하는 것이 사실이다. 비대면, 초연결사회가 본격화될수록 사이버 위협 또한 가속화될 것이기 때문이다. 이렇게 언택트 시대, 4차산업혁명 시대를 뒷받침하

*Corresponding Author : Sang-Soo Jang(ssjang0116@gmail.com)
Received March 6, 2020
Revised November 4, 2020
Accepted November 20, 2020
Published November 28, 2020

고 우리 경제의 중추적 역할을 맡고 있는 중소기업의 경우 현실적으로 정보보호를 논하기에는 어려움이 많다. 인력 및 예산 등 정보보호에 투자할 경영 여건이 여의치 않다는 것이다. 중소기업의 경우 정보보호 정책, 조직 구성 등 미흡으로 사이버 위협에 항상 노출되어 있어 매우 취약한 것이 현실이다. 더욱이 지역 간 정보보호 수준 격차 해소를 위해 지방의 중소기업 정보보호 수준 제고 및 정보보호 문화 확산 · 정착이 시급한 실정이다.

이렇게 중소기업의 사이버 안전망 취약 문제는 침해사고나 개인정보 및 기술유출 사고 발생 시 사회 안전에 직접적 위협이 될 수 있으므로, 정부 차원에서 정책적 지원, 제도적 연구 등 향상된 지원 정책 방향을 제언하고자 한다.

1.2 연구의 목적

포스트 코로나로 가속화된 4차산업혁명의 디지털 전환(digital transformation)과 코로나19 팬데믹이후 비대면 경영 환경 구축이 요구되고 있다. 이러한 시대에 중추 역할을 담당하고 있는 중소기업들에게 사이버 위협이나 데이터 위변조 위협은 중소기업이라고 예외는 없다. 그러나 현재 국내 중소기업의 정보보호 활동에 대한 어려움을 해소하고 지원할 수 있는 정부의 지원 정책은 제도적, 기술적으로나 아직 미흡한 실정이다. 이에 본 연구에서는 정부 차원에서 중소기업 정보보호 지원 정책 문제점을 분석하고 효과적인 중소기업 정보보호 지원 제도 개선, 정책 개발 제안, 정책 참조를 목적으로 수행되었다.

1.3 연구의 범위

이를 위해 선행연구 검토 분석, 국내 중소기업의 정보보호 실태 현황과 정책 개선을 위한 우선 순위 수요조사 분석 및 국내외 주요 국가의 중소기업 정보보호 지원 정책에 대하여 분석하여 실효적 지원 정책 개선 방안을 도출하고자 하였다. 제1장에서는 연구의 필요성, 연구 목적, 연구범위 등을 다루었다. 제2장에서는 선행연구와 이론적 배경을 살펴보고 제3장에서는 국내 중소기업 정보보호 지원 정책 개선 방안에 대해 제시하였다. 마지막 제4장에서는 지금까지의 연구결과를 요약하고, 결론과 정책적 제언을 하였다.

2. 관련연구 및 배경이론 검토

2.1 선행연구

노민선 외 1명(2010)은 “중소기업의 산업보안 역량에 대한 영향요인 평가”연구에서 정부 차원에서 우선적으로 추진해야할 사항으로 중소기업 지원 범위의 구체화, 기술유출 경험이 있는 중소기업에 대한 컨설팅 기능 강화, 혁신형 중소기업 인증시 보안관리 항목을 평가지표에 반영, 기술을 해외로 이전하거나 진출하고자 하는 중소기업에 대한 보안 정책 강화 등을 제시하였다[1].

김양훈 외 1명(2013)은 “적정 수준의 중소기업 정보보호 추진방향”연구에서 정보보호 지원 환경 측면에서는 경영진에 대한 인식을 제고, 적합한 정보보호 정책 수립을 하여야 한다. 정보보호 기반 구축에 있어서는 퇴직자에 대한 보안관리와 정보보호 운영 관리 측면에서는 정보보호에 대한 전문 지식 및 유관 기관과의 유기적 협조가 요구된다라고 제시하였다[2].

이장훈 외 2인(2014)은 “중소기업 기술보호 개선방안에 대한 연구”에서 기술보호 전문가를 양성하고 보안 리더십, 법적 제도적 개선, 예산을 확대하고 지원 방식을 개선 등을 제안하였다[3].

김태성 외 4인(2019)은 “중소기업 정보보호 성과측정 모델 및 방법 개발” 연구에서 한국인터넷진흥원 지역정보보호지원센터의 확대 및 강화, 정보보호 컨설팅 등 서비스 및 제품 구매 지원 강화, 인식제고 및 교육 강화 등을 언급하였다[4].

정은한 외 1인(2020)은 “클라우드 컴퓨팅 서비스의 정보보호 실효성 증진을 위한 정보보호 정책의 언어적 특성 분석” 연구에서 정보보호 정책은 사용자가 서비스 이용 전에 반드시 동의해야만 하는 서비스라는 용어로 정의하고 포괄적인 용어와 불확실한 언어의 구사는 소송 위험에 대한 우려를 공급자가 안고 있음을 시사한다 하였다[5].

2.2 이론적 배경

2.2.1 국내 중소기업 정보보호 실태 현황

통계청에 따르면 국내 중소기업 비중이 99%, 종사자 수도 88%를 넘고 있다. 침해사고 기업 가운데 97%가 중소기업이다. 또한 전체 중소기업의 78%가 지역에 위치하고 있어 지역의 정보보호 기반은 매우 취약하다.

정보보호 사각지대, 지역 보안수준 격차 등 지역의 경우 정보보호 생태계는 매우 열악하다. 과학기술정보통신부(한국정보보호산업협회)의 '2019년 정보보호 실태조사'에 따르면 정보보호(개인정보보호) 예산을 보유하고 있는 사업체는 32.2%(전년대비 3.9%p↓)감소하였으며, 정보보호 중요성에 대한 인식은 87.0%로(전년대비 1.4%↓)했으며, 정보보호정책 수립은 23.1%로 7.1% 증가하였으나 5인 미만의 기업에서는 5.1% 소폭 증가하였다. 정보보호 서비스 이용에서는 42.5%로(전년대비 16.9%↓)로 크게 감소한 것으로 조사됐다[6].

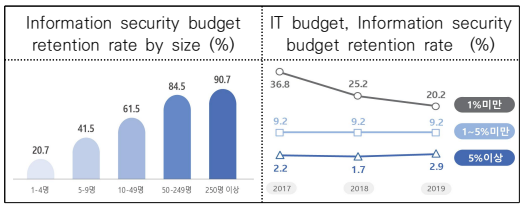

Fig. 1. Information security(personal information) budget retention rate

중소벤처기업부 '2017 중소기업 기술보호 실태조사'에 의하면 기술유출의 피해 금액은 1,022억 원으로 전년도 1,097억 대비하여 75억 원 정도 감소한 것으로 조사되었다. 평균 피해 금액 역시 전년도 (18.9억 원) 대비 5.8억 원 감소한 13.1억으로 나타났다. 비 수혜기업은 총 22건의 기술유출이 발생하였으며, 총 피해금액은 98억 원, 건당 평균 피해금액은 4.5억의 기술유출 피해가 발생한 것으로 조사되었다. 수혜기업은 총 56건의 기술유출이 발생하였으며, 총 피해금액은 924억 원, 건당 평균 피해금액은 16.5억의 기술유출 피해가 발생한 것으로 나타났다[7].

Table 1. Number of technology leaks and damages

Division	Total (number)	Average (number)	Total damage amount (KRW 100 million)
SME	78	1.5	1,022
Beneficiary Company	56	1.37	924
Non-beneficiary company	22	2.0	98

개인정보보호위원회의 '개인정보 유출 현황'를 분석한 결과(Table 2) 2016년부터 2020년 9월까지 공공·민간·온라인 부문에서 376회, 6천 414만 건의 개인정보가 유출된 것으로 나타났다. 실제 2017년 610만 건이던 개인정보 유출 건수는 2019년 1천 839만 건으로 3배 이상 증가했고, 올해 9월까지 994만 건의 개인정보가 유출됐다[8].

Table 2. Personal information leakage in the last 5 years

Year	Number of cases	Administrative disposition	Fine (10,000 won)	Amount of penalty imposed per case(won)
2016	21,172,191	21,172,191	479,336	226.4
2017	6,099,528	6,070,561	174,805	288.0
2018	8,540,090	8,211,834	375,015	456.7
2019	18,385,748	15,361,310	282,337	183.8
2020.9	9,941,735	53,345	2,127	398.7
Total	64,139,292	50,869,241	1,313,620	258.2

또한 한국인터넷진흥원이 수행한 '2019년 중소기업 컨설팅 서비스 결과보고서'에 따르면 컨설팅 지원 신청 업체(179건)의 신청 사유에 대하여 분석한 결과 Table 3과 같이 어느 정도 정보보호 필요성은 인식하고 있으나(43%), 외부로 부터의 침해사고 경험이나 정보보호 관리의 어려움을 호소하고 있다[9].

Table 3. Reasons for requesting information protection consulting service

Items	Answer(%)
Insider leak experience	11(6.1)
Security accident From outside	44(24.6)
Awareness of information security	77(43.0)
Difficult to manage information security	25(14.0)
Strengthening the level of information security	22(12.3)
Total	179(100.0)

또한 정보보호 활동의 어려움을 조사 분석한 결과 Table 4에서 전체 기업 중 정보보호에 대하여 어떻게 보호해야하는지 모른다는 기업이 가장 많았으며(17.1%), 산업별로 정보통신 관련 중소기업은 전담 인력 채용의 어려움이 가장 크며, 정보보호 투자에 대한 여력이 없는 것으로 나타났다[9].

Table 4. Difficulties in SME information security activities

Items	Answer(%)
Not sure how to protect	47(17.1)
Difficult maintenance	22(8.0)
Difficult to manage information protection	33(12.0)
Difficulties in establishing and operating information protection policies	26(9.5)
Poor response to internal and external intrusion	43(15.7)
Difficulty in hiring dedicated personnel and maintaining work	39(14.2)
Absence of professional service and burden on price	13(4.7)
Difficulties in cognitive and professional education	15(5.5)
No room for information security investment	36(13.3)
Total	179(100)

2.2.2 국내 중소기업 정보보호 지원 정책 현황

가. 부처별 중소기업 지원 정책 현황

국내의 중소기업 정보보호 주요 지원 정책으로는 먼저 과학기술정보통신부 및 한국인터넷진흥원에서 2014년부터 본격적으로 지역 중소기업의 정보보호 수준 제고 및 침해사고 예방・대응 역량 강화, 정보보호 산업 활성화를 위하여 '지역 중소기업 정보보호 지원' 사업을 추진하고 있다. 이를 위하여 지자체 및 지역 유관기관과 협력하여 "지역정보보호지원센터"를 구축·운영 중에 있다[10].

또한, 중소벤처기업부와 대・중소기업・농어업협력재단에서 시행하는 '기술보호 전문가 상담·자문', '중소기업 기술분쟁 조정·중재', '기술자료 임치제도', '기술유출방지시스템구축 지원' 사업 등이 있다[11].

나. 중소기업 지원 관련 근거 법률 현황

국내 중소기업 대상 정보보호 지원 관련 법률 현황으로는 과학기술정보통신부 소관 법률로는「정보보호산업의 진흥에 관한 법률」)과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」등이 있으나 중소기업에 대한 정보보호 지원 사업의 법적 근거를 구체적으로 명시하지 않고 있다. 또한 산업통상자원부 소관 법률인「산업기술의 유출방지 및 보호에 관한 법률」과 중소벤처기업부 소관 법률인「중소기업기술 보호 지원에 관한 법률」, 「중소기업기술 촉진법」이 있으나 산업기술 보호 위주로 되어있다.

2.2.3 해외 중소기업 정보보호 지원 정책 현황

가. EU(European Union)

유럽집행위원회(EU)의 "Horizon 2020"은 중소기업 사이버 보안 강화 관련 프로그램으로 중소기업・영세기업이 개인정보보호, 보안 위협을 능동적으로 모니터링하고 예측, 접근하기 위한 효율적인 솔루션 개발・연구하는 프로그램이다. EU의 사이버 보안법(Cybersecurity Act) 발효로 ENISA(European Union Agency for Cybersecurity)가 EU 내 중소기업의 사이버 보안 문화 구축을 위한 사이버 보안 교육 실시, 기업 관련 보안 지침 및 권장사항, 모범사례 등을 연구하고 중소기업 간 협력 네트워크를 지원 하고 있다[12].

나. 미국

미국은 NIST와 SBA(Small Business Administration, 중소기업청)를 중심으로 중소기업의 사이버 보안 역량 강화를 위한 법 제정(NIST Small Business Cybersecurity Act, 2018)하여 운영중에 있다. 중소기업에 대한 사이버 보안 예산 지원, 자원을 지원할 수 있는 근거 법률로 정보보호 지침, 도구, 모범사례, 표준, 방법론 등을 제공하고 있다. 중소기업청 산하기관인 SBDC(Small Business Development Center)가 중소기업에 대해 사이버 보안 관련 정보와 교육, 컨설팅을 지원하고 있으며, 소규모기업에 대한 사이버 보안 교육 지원으로 중소규모 기업이 사이버 공격으로부터 시스템을 보호할 수 있도록 돕는 것을 목적으로 하고 있다[13].

다. 영국

영국은 중소기업 정보보호 수준 제고를 위해 Cyber Essentials Scheme(CES)인 정보보호 인증 제도를 도입 운영하고 있다. 또한 국가사이버 보안센터(NCSC)는 공공기관 뿐만 아니라 민간기업의 중소기업, 자영업자 등이 사이버 보안을 이해하고 활용할 수 있도록 사이버 공격에 대한 자체 시스템 보호 지침, 중소기업 사이버 보안 가이드 등을 제공하고 있다[14].

라. 일본

일본은 경제산업성 및 IPA(Information technology Promotion Agency)는 중소기업이 지켜야 할 정보보호 대책을 단계적으로 추진할 수 있도록 중소기업 정보보호대책 가이드라인을 개발하여 제공하고 있으며, 중

소기업이 스스로 정보보호 수준을 평가해볼 수 있는 정보보호 벤치마크시스템(ISM-Benchmark)도 운영중에 있다. 또한 중소기업 스스로가 정보보호 대책을 적용 및 시행하는 것을 선언하는 제도인 Security Action을 수행하고 있다[15].

3. 국내 중소기업 정보보호 지원 정책 개선 방안

3.1 연구 방법

3.1.1 연구 설계 및 조사

이 연구는 중소기업의 정보보호 수준 제고를 위한 정보보호 지원 정책 개선 방안에 대한 연구로서, 정보보호 지원 정책 관련 선행연구와 이론적 배경을 중심으로 하되 정부의 정보보호 정책 수혜자인 중소기업 담당자의 의견과 정보보호 실태 현황을 가미하여 연구방향을 설정하였다. 연구 내용을 보다 객관성 확보를 위해 설문조사 대상자인 과학기술정보통신부에서 수행한 2019년 정보보호 컨설팅 지원 서비스 중소기업 담당자를 대상으로 우선적으로 '중소기업 정보보호를 위한 개선사항이 무엇인가'라는 질문에 국내 중소기업의 정보보호 정책의 실태 및 문제점을 체계적으로 밝혀내기 위하여 설문 조사를 실시하였다.

3.1.2 자료 수집 및 분석

이 연구는 질적 연구의 설계 방법 중 반구조화 된 심층 설문기법으로 실시하였다. 중소기업 담당자, 임원, CEO 등 중소기업 정보보호 관련 전문가들의 설문 인터뷰를 바탕으로 실시하여 분석하였으며, 자료 분석은 현장에서의 설문지와 수집된 자료를 바탕으로 분석하였다. 수집된 자료를 통해 중소기업 정보보호의 현황 및 문제점, 개선방안에 대한 공통점, 특수성, 객관성, 타당성을 고려하여 분석하였다.

3.1.3 연구의 타당성 및 신뢰도

자료수집과 분석단계에서 질적 연구의 경험이 있는 연구자가 직접 설명을 하여 참여자들에 대한 신뢰도와 객관성, 타당성을 수집하고 분석하는 데 서로 자료를 공유하고 정확한 내용을 점검하였다. 이를 통해 연구자의 주관적인 편견과 해석을 최소화하여 정확성과 진실성, 신뢰성을 확보하였다.

3.2 정보보호 지원 정책의 문제점 분석 결과

3.2.1 중소기업 침해사고 및 정보유출 주요 원인

가. 정보보호에 대한 인식 부족

과학기술정보통신부의 2019년 정보보호 실태조사 결과에서 정보보호 중요성에 대한 인식은 87.0%로(전년대비 1.4%↓)했으며, 정보보호정책 수립은 23.1%, 정보보호 서비스 이용 42.5%로(전년대비 16.9%↓)로 크게 감소한 것으로 조사됐다. 이렇게 중소기업 정보보호와 관련이 있는 부처나 지자체, 관계기관 뿐만 아니라 해당 중소기업의 CEO와 담당자들의 정보보호 인식 제고 문제는 매우 심각하다 할 수 있다[6].

나. 중소기업의 자체 역량 강화 및 인센티브 부족

중소기업 스스로 정보보호 필요성을 인식하여 자율적으로 정보보호 역량을 강화할 수 있도록 정부의 적극적인 지원 및 중소기업에 적합한 맞춤형 동기부여가 가능한 인센티브가 현재로는 부재한 것으로 나타났다[10].

다. 정보보호 전담인력 및 예산 부족

과학기술정보통신부 '2019년 정보보호 실태조사 '에서도 정보보호 조직운영(12.3%, 6.8%p↑), 정보통신(IT) 예산 중 정보보호 예산을 1% 미만으로 편성한 기업은 감소(20.2%, 5.0%p↓)하고, 5% 이상 편성한 기업은 증가(2.9%, 1.2%p↑)로 나타났다. 이와 같이 대부분 중소기업이 전담 인력과 예산 부족의 어려움을 호소하고 있다[16].

3.2.2 중소기업 정보보호 지원의 산발적 지원

가. 중소기업 정보보호 공동 대응 체계 구축 미흡

중소기업들이 정보보호 위협에 대응할 수 있도록 기술적 방법, 정보보호 서비스나 제품 정보, 정부 지원 정책 등을 공유하며 공동 대응해 나갈 수 있는 체계 구축이 미흡한 실정으로 나타났다.

나. 관련 부처간 협업 체계 부족

중소기업의 정보보호 주무부처인 과학기술정보통신부, 중소벤처기업부, 산업통산자원부, 유관 기관 등이 협력 체제를 유지하고 있지만, 중소기업의 침해사고나 기술유출에 대해 초기 단계부터 효율적으로 대응할 수 있는 정보공유, 효율적 협업체계 또한 미흡한 실정이다.

3.2.3 체계적 지원 근거 법제도 미흡

앞에서 살펴본 중소기업 정보보호 지원 근거 법률은 기능적으로 분리되어 있고 구체적인 지원 근거나 지원 제도, 컨트럴 타워 부재, 부처간 역할 등이 명확하지 않거나 중복과 이원화로 이해당사자들에게 혼선을 야기하고 있다.

3.2.4 지역 전략산업과의 연계 부족

지자체별로 4차산업 혁명 핵심 기술인 인공지능, 클라우드, 빅데이터, 사물인터넷, 모바일 등 사업들이 우리 국민생활에 막대한 영향을 미치는데도 불구하고 정보보호 예산은 반영이 안되다보니 지자체별 추진 사업이 정보보호 사업과 연계나 협력이 부족한 실정이다.

3.2.5 지역 사이버 안전망 구축 미흡 및 컨설팅 방법 부재

한국인터넷진흥원은 전국 10개의 “지역정보보호지원센터”을 구축 운영중에 있으나, 2020년 10개의 센터로는 물리적 한계로 전국적인 사이버 방역체계를 구축하기에는 한계가 있다. 또한 Table 5와 같이 정보보호 지원 정책의 하나인 무료 정보보호 컨설팅 서비스의 경우 매년 보안 컨설팅 전문기업을 선정하다 보니 컨설팅 방법이나 절차가 상이하고 수준의 차이로 컨설팅 결과에 대한 실효성에 의문를 제기하고 있다[10].

Table 5. Comparison of information security consulting checklists for 2018~2019

Check list	CIIP	ISMS	SME security consulting	
			A (2018)	B (2019)
Managerial	46	16	95	63
Technical	159	64	251	115
Web	28		14	14
Privacy	-	22	27	27
Total	233	102	387	219

3.2.6 언택트 시대 대비한 지원 정책 미흡

코로나19 영향으로 재택근무, 원격화상회의, 온라인 교육 등과 같은 비대면(untact) 환경에서 보안 위협에 취약한 중소기업의 보안 문제 해결이 시급한 실정이다. 그러나 현재 지원방식이 현장 방문 위주의 서비스로 비대면 시대에 적합하지 않다. 또한 지원 대상에서도 예산상의 제한으로 많은 중소기업이 혜택을 받기에는 한계가 있다[16].

3.3 향상된 중소기업 정보보호 지원 정책

지금까지 중소기업의 수요에 적합한 정보보호 지원 정책을 도출하기 위해서, 선행연구와 국내외 중소기업 정보보호 지원정책 분석을 통해 지원 정책을 선정하였다. 이를 검증하기 위하여 한국인터넷진흥원에서 수행한 2019년 정보보호 컨설팅 수혜대상 중소기업을 상대로 지원 정책에 대한 문제점과 개선 방안 의견수렴을 하고자 개선 사항이나 시급한 지원 정책 우선 순위를 조사하였다. Table 6과 같이 지역별 중소기업 80개를 선정하여 응답 업체 62개에 대하여 분석하였다.

Table 6. SME information protection support policy priority demand survey

NO	Questions	answer(%)
1	Raising awareness of information security	62(100)
2	SMEs' own capacity building and incentives	56(90)
3	Reinforcement of information security personnel and budget support	54(87)
4	Establishment of a joint response system for small and medium business information protection	45(72)
5	Establishment of cooperation system between ministries	35(56)
6	Improvement of legal system based on systematic support	28(45)
7	Insufficient establishment of regional cyber safety net and improvement of consulting method	25((40)
8	Preparing a support policy for the untact era	20(32)
9	Strengthening linkage with regional strategic industries	18(29)
10	Other	5(8)

정책 수요 조사 결과 우선순위에서 가장 많은 정보보호 인식제고 추진(100%), 중소기업의 자체 역량 강화 및 인센티브 마련(90%), 정보보호 전담인력 및 예산 지원 강화(87%), 중소기업 정보보호 공동 대응 체계 구축(72%)로 나타났다. 향상된 중소기업 정보보호 지원 정책으로는 다음과 같이 9개의 향상된 개선 과제를 도출하였다.

3.3.1 정보보호에 대한 인식 강화

첫째, 지자체, 산업단지 등을 대상으로 정보보호 인식제고 및 홍보 캠페인 진행 등 다양한 방안 모색이 필

요하다. 둘째, 중소기업들의 IT 자산 보유 수준 및 정보보호 실태 파악을 하여 최소 정보보호가 시급한 중소기업을 선정하여 최소한의 정보보호 가이드라인과 기초 보안교육을 제공이 필요하다.

3.3.2 중소기업의 자체 역량 강화 및 인센티브 마련

첫째, 중소기업이 사이버 보험을 적극 가입 할 수 있도록 보험료의 비용 일부를 지원하는 정책이 필요하다.

둘째, 중소기업이 자발적으로 자사의 정보보호 활동과 그에 대한 성과를 평가하여 마일리지를 부여하는 방식을 고려할 필요가 있다.

셋째, 정보보호 활동에 적극적인 중소기업에게는 국가기관이나 지자체, 공공영역에서 입찰 참여시 가산점 부여, 법인세 인하 정책과 4차산업혁명의 핵심기술을 개발하고 적용하는 중소기업에 대해서는 의무적으로 정보보호 대책을 수립하도록 할 필요가 있다.

3.3.3 정보보호 전담인력 및 예산 지원 강화

포스트 코로나 시대에 보다 금전적 비용 지원을 확대하여 정보보호 제품 및 서비스를 구매하고자 하는 중소기업을 대상으로 기업 현금 부담을 줄이고 보다 많은 실질적 혜택이 갈 수 있도록 지원을 강화해야 한다.

3.3.4 중소기업 정보보호 공동 대응 체계 구축

첫째, 중소기업이 침해사고나 기술유출 사고시 중소기업간 정보공유와 협력체계를 구축해야 한다. 둘째, 지자체별로 지역전략산업이나 특화산업 보안강화를 위해 “중소기업 사이버보안관제센터”(가칭) 구축을 고려해야 한다.

3.3.5 부처간 협업 체계 마련

첫째, 중소기업의 정보호 지원을 체계적이고 효율적으로 지원하기 위해서는 부처간 협업 체계 마련을 위해 “중소기업정책협의회(가칭)”를 구축해야 한다. 둘째, 정보보호 활동 지원을 위해 수행 주체들이 체계적이고 지속적이고 안정적인 지원 활동 기반 마련을 위한 다양한 법적, 제도적 도입 방안도 검토할 필요가 있다.

3.3.6 체계적 지원 근거 법제도 개선

첫째, 과학기술정보통신부에서 수행하는 중소기업 정보보호 지원 사업의 연속성이나 당위성면에서 보다 전문적이고 체계적인 중소기업의 사이버위협에 대응하기 위한 법·제도적 근거 마련이 필요하다. 정보보호 기본법인「중소기업 정보보호 지원에 관한 법률」(가칭) 제정하여 중소기업 정보보호 컨트롤 타워를 명확히 하고 일원화할 필요가 있다. 둘째, 정부 주무 부처나 지자체 등 중소기업의 정보보호 관련 규정 제정을 통해 수행 주체의 역할을 명확화하고 중소기업이 정보보호 정책 추진에 협력할 수 있도록 제도적 근거 마련이 필요하다.

3.3.7 지역 사이버 안전망 구축 및 컨설팅 방법 개선

첫째, “지역정보보호지원센터”를 현재 10개 센터를 전국 17개 광역시도 모두 “지역정보보호지원센터”를 구축해야 한다. 둘째, 지역 거점 단지 조성, 지역 영세기업의 사이버 안전망 구축을 지원할 지엽별 “정보보호 기업 육성센터”도 함께 건립이 필요하다. 셋째, 현재의 중소기업 정보보호 컨설팅 방법인 단순 체크리스트 기반에서 데이터 중요도, 위험관리 기반의 실효성 있는 보안 컨설팅 방법을 적용해야 한다.

3.3.8 언택트 시대 대비한 지원 정책 마련

첫째, 현장 방문 위주의 서비스 형태에서 클라우드 형태로 제공되는 보안 서비스(SECaaS : Security as a Service)지원 사업 등 다양한 비대면 서비스 개발이 필요하다. 둘째, 비대면 서비스 강화와 함께 비대면 정보보호 컨설팅 방법론 개발도 필요하다[16].

3.3.9 지역 전략산업과의 연계 강화

첫째, 4차산업 혁명 핵심 기술을 지역 전략산업이나 특화산업을 뒷받침하기 위해서는 제품개발이나 서비스 개발 단계부터 정보보호를 고려한 내재화가 필요하다. 둘째, 중소기업 지원 방식을 4차산업혁명에 참여하는 혁신적 중소기업을 대상으로 우선적으로 지원 대상을 명확하게 선택과 집중을 할 필요가 있다. 셋째, 스마트 공장, 스마트 시티, 인공지능 등 4차산업 혁명 핵심 기술 개발 사업의 주체는 정보보호 예산을 반영하도록 의무화 해야 한다.

4. 결론 및 제언

본 연구결과에서 나타난 시사점은 다음과 같다. 첫째, 국내 중소기업의 사이버 위협에 대응할 수 있는 안

전한 경영 활동을 지원할 필요가 있다는 것이다. 둘째, 지역균형발전, 지역 간 정보보호 격차 문제와 중소기업 정보보호 문제를 국가적 당면과제로 인식이 필요하다. 셋째, 보안 취약 부문에 대한 지원과 점검을 확대해 보안 사각 지대가 없는 촘촘한 지역 사이버 안전망을 구축해야 한다. 넷째, 정부의 적극적인 지원과 지자체, 지역 유관기관, 학계의 능동적인 참여와 지역 중소기업 자체의 개선 노력과 보안업계의 시장 확대를 위한 노력 등이 함께 이뤄져야 한다는 것이 검증되었다는 것이다.

본 연구결과를 토대로 다음과 같이 정책적 제언을 하고자 한다. 첫째, 기존 중소기업에 대한 침해사고 및 기술유출 방지 지원 정책에 대한 실효적이며 중소기업의 자발적 참여 유도 정책이 필요하다. 둘째, 부처간 중소기업 정보보호 지원 업무에 대한 재 검토를 통해 부처간 협업 체계 마련 방안해야 한다. 셋째, 각 부처별 산재해 있는 중소기업 정보보호 지원에 대한 법제도적 지원을 체계적이고 종합적이고 일관성 있도록 지원하기 위한 컨트롤 타워 기능이 필요하다. 넷째, 코로나19 대응, 언택트 시대 대비한 중소기업 효율적 지원 방안 마련이 필요하다. 다섯째, 지역 균형발전과 지역의 정보보호 격차 해소를 위한 지역 사이버 안전망 강화 방안이 필하다. 마지막으로 기존 중소기업 정보보호 지원 정책을 보완하고 제안된 지원 정책 방향을 적용이 필요하다.

향후 중소기업 정보보호 정책 기관인 과학기술정보통신부, 중소벤처기업부 등과의 협력을 통해 4차 산업혁명에 필요한 다양한 중소기업 정보보호 지원 정책의 밑거름이 될 수 있을 것으로 기대한다.

REFERENCES

[1] M. S. Noh & S. Y. Lee, (2010), Explaining Industrial Security of SMEs in Korea:An Ordered Logit Analysis, *Korean Public Administration Review, 44(3),* 239-259.

[2] Y. H. Kim & H. B. Chang. (2013). SME Information Protection Promotion Direction, *Korea Institute of Information Security And Cryptology, 23(4),* 41-46.

[3] J. H. Lee & W. S. Shin & H. J. Park, (2014), A Study on Improvement Plans for Technology Protection of SMEs in Korea, *Society of Korea Industrial and Systems Engineering, 37,* 77-84.

[4] T. S. Kim. (2019). *SME information protection performance measurement model and method development.* Naju : KISA.

[5] E. H. Jeong & K. I. Kim. (2020). An Analysis of Linguistic Characteristics of Information Protection Policies to Improve the Effectiveness of Information Protection in Cloud Computing Services. *Journal of Convergence for Information Technology, 10(10),* 15-23.
DOI : 10.22156/CS4SMB.2020.10.10.015

[6] Ministry of Science and ICT. (2020). *Information Security Survey 2019.*

[7] Ministry of SMEs and Startups. (2018). *2017 SMEs Technology Protection Survey.*

[8] Personal Information Protection Commission, (2020), *Information Security Survey 2020.*

[9] Korea Internet and Security Agency. (2020). *2019 SME Information Protection Consulting Result Report.* Naju : KISA.

[10] Korea Internet and Security Agency. (2020). *Local SME Information Security Support,* (Online). https://www.kisa.or.kr.

[11] Ministry of SMEs and Startups. (2020). *SMEs Technology Protection Ultari,* (Online). https://www.ultari.go.kr

[12] European Commission. (2020). *Horizon. EC.* (Online). https://ec.european.eu.

[13] USA Congress. (2020). *NIST Small Business Cybersecurity Act.* (Online). https://congress.gov.

[14] National Cyber Security Center. (2020). *Cyber Essentials.* (Online). www.cyberessentials.ncsc.gov.uk.

[15] IPA, Benchmark System. (2020). *Security Action.* (Online). https://www.ipa.go.jp.

[16] Korea Internet and Security Agency. (2020). *Security survey when working from home.* Naju : KISA.

장 상 수(Sang-Soo Jang) [정회원]

· 1989년 2월 : 한국항공대학교 항공통신정보공학과(이학사)
· 2010년 8월 : 전남대학교 정보보호대학원(이학박사)
· 1989년 2월 ~ 2000년 5월 : 대한항공 정보시스템실
· 2000년 5월 ~ 현재 : 한국인터넷진흥원 연구위원
· 관심분야 : 정보보호, 융합보안, ISMS, 개인정보보호
· E-Mail : ssjang0116@gmail.com