韓國IT서비스學會誌
第21卷 第1號
2022年 2月, pp.81-102

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2022.21.1.081

중소기업의 특성을 고려한 정보보호 관리체계 평가 모델 개선*

김이헌** · 김태성***

Improvement of Information Security Management System Evaluation Model Considering the Characteristics of Small and Medium-Sized Enterprises*

Yi Heon Kim** · Tae-Sung Kim***

■ Abstract ■

Although more than 99% of all Korean companies are small and medium-sized enterprises (SMEs), which accounts for a large part of the national economy, they are having difficulties in securing information protection capabilities due to problems such as budget and manpower. On the other hand, as 97% of cyber incidents are concentrated in SMEs, it is urgent to strengthen the information protection management and response capabilities of SMEs. Although the government is promoting company-wide information security consulting for SMEs, the need for supplementing it's procedures and consulting items is being raised. Based on the results of information security consulting supported by the government in 2020, this study attempted to derive improvement plans by interviewing SME workers, information security consultants, and system operators. Through the research results, it is expected to create a basis for SMEs to autonomously check the information security management system and contribute to the reference of related policies.

Keyword : Information Security Management System, Information Security Consulting, Information Security of SMEs

Submitted : December 6, 2021 Accepted : December 30, 2021

* 본 논문은 충북대학교 국립대학육성사업(2021)지원을 받아 작성되었음. 본 논문의 일부 내용이 2021년 한국IT서비스학회 추계학술대회에서 발표되었고, 우수논문상을 수상하였음.

** 충북과학기술혁신원 선임연구원

*** 충북대학교 경영정보학과 교수/보안경제연구소 소장, 교신저자

1. 서 론

통계청에 의하면 우리나라 전체 기업의 99% 이상이 중소기업으로 이루어져 있는데, 중소기업의 경우 인력과 예산의 측면에서 정보보호 역량 확보에 어려움을 겪고 있는 실정이다. 실제로 한국정보보호산업협회의 2020년 정보보호 실태조사 결과를 보았을 때 재직자 50인 미만의 기업이 50인 이상 기업에 비해 보안정책 수립, 정보보호 책임자 임명, 정보보호 전담조직 운영 등 보안에 대한 역량과 환경이 열악한 것으로 나타났다(한국정보보호산업협회, 2021). 반면 한국인터넷진흥원 보도자료에 따르면 사이버 침해사고의 98%가 중소기업에 집중되어 있어 예산과 인력, 인식이 부족한 중소기업의 정보보호 관리·대응 역량 강화가 시급하다(연합뉴스, 2018).

현재 우리나라는 정보보호 관리과정, 보안수준 등의 관리체계(ISMS)와 개인정보의 수집, 이용, 파기 등 개인정보 관리체계(PIMS)를 하나로 통합하여 심사, 인증을 하는 ISMS-P 제도를 운영함으로써 기업의 정보보호 및 개인정보보호 관리 수준 향상을 도모하고 있다(한국인터넷진흥원, 2021). 그러나 이 제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 2항에 따라 ISP, IDC 사업자와 일정 매출액, 이용자 기준 이상의 의료기관과 학교, 대규모의 기업을 의무 대상자로 하고 있으며, 중소기업의 경우 자율적인 정보보호 보호조치가 요구된다.

2014년부터 정부에서는 지자체와 협력하여 예산과 인력 등 경영여건이 어려운 중소기업을 대상으로 정보보호 컨설팅을 지원하고 있다. 컨설팅은 자산과 진단대상 식별 등의 사전준비 단계를 거쳐 체크리스트 기반 정보보호 관리체계 점검과 모의해킹 기술진단 등 전사적 보안 취약점을 점검하는 현장컨설팅의 단계로 이루어져있으며 컨설팅 이후에는 점검 결과를 바탕으로 맞춤형 솔루션의 도입을 지원하고 컨설팅 결과의 이행조치를 지원하는 이행점검이 수행된다.

이와 같은 정부의 중소기업 정보보호 컨설팅 지원사업은 연간 600개사(2021년 목표)를 대상으로 지속지원하고 있으나 절차나 효과성의 측면에서 개선의 필요성이 제기되고 있다. 컨설팅 전문 업체의 위탁용역을 통해 사업이 추진되는데 컨설팅 업체별 기준이 상이하고 중소기업의 규모나 유형을 고려하지 않아 표준적인 정보보호 수준을 측정하는데 한계가 있으며, 중소기업의 입장에서 적용조차 어려운 항목이 대부분인 것으로 확인되기도 하였다(장상수, 2020). 실제로 2018년의 지원결과를 보았을 때 총 지원기업 195개사의 최초진단 시 정보보호 관리체계 보안수준이 52.4%, 컨설팅 이후 점검 시의 수준이 60.2%로 7.8%p에 불과한 개선율을 보였으며, 이는 컨설팅 이후에도 자체적으로 정하고 있는 권고수준인 80%에 미치지 못하는 수치이다(김재남 등, 2019). 이를 통해 정부의 중소기업 정보보호 지원사업 역시 실효성에 대한 문제의식과 검증이 필요할 것으로 판단된다.

본 연구에서는 실제 중소기업 대상 정보보호 관리체계 컨설팅 결과를 바탕으로 컨설팅을 받은 중소기업 관계자(담당자), 정보보호 컨설팅 전문가, 정책담당자 등 다양한 이해관계자의 의견수렴을 통해 중소기업 현실에 맞는 맞춤형 정보보호 관리체계의 개선방안을 제시하고자 한다.

2. 선행연구

그간 중소기업의 정보보호를 위한 정보보호 관리체계(ISMS) 중심의 많은 연구들이 이루어졌으며, 기존의 방법론이나 평가 기법이 중소기업에 동일하게 적용하기에 무리가 있다는 문제의식 아래 다양한 정보보호 관리체계 모델과 정책의 개선방안이 제시되었다.

2.1 현황분석을 통한 정책 및 컨설팅 방법론 개선

다수의 연구가 선행연구와 문헌고찰, 현황 분석을 통해 정책과 컨설팅 방법론의 개선방안을 제안하였다. 노민선 등(2010)은 중소기업의 산업보안 역량수준에 미치는 영향에 대하여 문헌연구를 통해 가설을 검증하고 정책의 개선방안을 도출하였다. Barlette

et al.(2010)은 ISO/IEC 27001 및 27002 표준 등 주요 정보보안 관리 방법과 표준을 검토하고 기업에서 표준 준수가 힘든 이유를 분석, 기업에 적용하기 위한 방법을 제안하였다. 김양훈 등(2013)은 중소기업의 정보화 특성에 대한 선행연구를 분석하고 중소기업의 정보화와 정보보호 현황 파악을 통해 적정수준의 중소기업 정보보호 수행방안을 제언하였다. Kurpjuhn(2015)는 중소기업의 네트워크를 외부의 위협으로부터 보호하기 위해 한정된 시간과 자본을 투자하는 비즈니스 사례를 설명하였다. 서동호 등(2017)은 정보보호 관리체계(ISMS)와 유사 인증체계 분석을 통해 인증제도의 운영방향을 제시하였다. Javid et al.(2017)은 다양한 위험관리 프레임워크를 분석・통합하여 소규모 기업이 정보시스템의 운영수준에서 위험관리를 수행하기 위한 모델을 제안하였다. Paul(2017)은 사이버 위협으로부터 중소기업을 강화하는 6가지 방법(로그분석, 동적 디렉토리 관리, 사전감시, 클라우드 보안, 암호관리, 방화벽 분석)을 제안하였다. 김재남(2019)은 한국인터넷진흥원에서 수행한 중소기업 정보보호 컨설팅 결과를 바탕으로 효과를 분석하고 문제점과 한계점 파악을 통해 개선방안을 제시하였다. 이효경(2019)은 국내의 중소기업 대상 정보보호 지원 관련 법제도・정책의 현황과 해외 동향 분석을 통해 시사점과 개선방향을 제시하였다. Ozkan et al.(2019)은 기존의 다양한 보안 표준들이 중소기업을 대상으로 실행이 불가능하거나 유용하지 않는 점 등의 문제를 제기하였으며 중소기업 현실에 맞는 표준 및 요구사항에 대한 향후 과제를 제안하였다. 김신석 등(2020)은 문헌연구를 통해 기업의 규모별 개인정보보호 인식과 환경차이를 분석하고 중소기업에 맞는 개인정보보호의 기술적 보호조치 방안을 제안하였다. 장상수(2020)는 현행 제도의 정보보호 컨설팅 방법론을 비교분석하여 체크리스트 기반의 정보보호 컨설팅에서 위험관리 기반의 개선된 방법론을 제시하였다. Benz et al.(2020)은 NIST(National Institute of Standards and Technology)의 사이버보안 프레임워크를 기반으로 중소기업이 정보보호 성숙도를 자체 평가하기 위한 모델을 제안하였다. Ozkan et al.(2020)은 중소기업의 특성과 정보보호 성숙도 모델을 분석하고 매핑하여 중소기업을 위한 정보보호 성숙도 모델의 설계를 위한 요구사항을 도출하였다.

2.2 재직자 설문을 통한 개선방안 제시

중소기업 관계자 대상 설문을 통해 실제 현황을 분석하고 기존의 연구와 결합하여 개선방안을 제안한 연구들이 이루어졌다. 이정우(2005)는 문헌연구를 통한 중소기업 특성에 맞는 정보보호 관리모델을 구성하고 실증연구를 통해 정보보호 관리모델 구성요소의 중요성 비교분석, PDCA 사이클의 모델을 제시하였다. Yildirima et al.(2011)은 터키의 중소기업 97개사를 대상으로 정보보호 현황을 조사하고 국외의 데이터와 비교 분석하여 운영관리와 보안정책이 개선될 경우 인적보안, 물리보안 등의 다른 보안 변수도 향상되는 것으로 추정하였다. Osborn(2014)은 중소기업의 보안 장벽에 대한 설문조사를 바탕으로 기존의 연구와 결합, 중소기업의 보안 솔루션 개발에 대한 영향에 대해 논하였다. 권장기 등(2017)은 제조업 중소기업 대상 정보보안 실행현황의 조사분석을 통해 자원 제약하의 적용 가능한 보안대책을 제시하였다. 곽재연(2019)은 중소기업 대상 기존 정부지원 방안에 대한 현황과 실태조사를 통해 효율적이고 적절한 지원사업의 방향을 제시하였다. Ključnikov et al.(2019)은 슬로바키아 중소기업 중 정보보호 관리의 성공 요인을 조사하여 보안 통제와 최고 경영진의 지원이 가장 큰 요인임을 제시하였다. Rae et al.(2019)은 중소기업의 정보보호 모범사례에서 보안 행위를 개선시키는 영향요인을 분석하여 중소기업을 대상으로 하는 5×5 매트릭스 기반의 사이버보안 등급 체계를 제안하였다. 장상수(2020)는 중소기업의 정보보호 실태 및 주요국의 정보보호 지원정책 현황과 문제점을 분석하고 중소기업 재직자 대상 설문조사를 통해 지원정책의 우선순위를 검증하였다. Saban et al.(2021)은 중소기업 경영진의 인식에 대한 설문조사를 수행하고 기존의 보안 준비 모델과 비교한 결과

외부의 보안에 대한 영향이 커질수록 중소기업 경영진의 보안 인식이 커지고 보안 구현에 대한 문제가 커질수록 인식과 노력이 감소함을 밝혔다.

선행연구들을 바탕으로 정보보호 관리체계의 개선방안을 제시하고 중소기업을 대상으로 실증분석을 한 연구 또한 이루어졌다. Tawileh et al.(2007)은 중소기업 정보보안 관리의 문제 요인을 제시하고 중소기업의 보안관리 시스템 개발을 위한 전체론적 접근 방식을 제안, 실증연구를 통해 입증하였다. Groner(2012)는 중소기업에 적합한 IT 보안 인프라 설계를 위하여 보안 위협, 요구사항 및 관련 프레임워크 구성요소 간 종속성을 설명하고 독일의 중소기업을 대상으로 실증분석을 하였다. Cholez(2013)는 기업의 정보보안 성숙도에 대한 평가와 프로세스 개선을 통해 중소기업에 적용가능한 방법론을 제안하고 실제 산업에 적용하여 입증하였다. Antunes et al.(2021)은 ISO 27001: 2013을 기반으로 하는 정보보호 및 관리 방법론을 제시하고 포르투갈 중소기업을 대상으로 사례연구를 통해 입증하였다.

2.3 전문가 자문을 통한 개선방안 제시

일부 연구의 경우 정보보호 전문가의 의견을 반영하여 정책과 컨설팅 방법론의 개선을 제안하고자 하였다. 김정덕 등(2006)은 문헌연구와 방문조사를 통한 중소기업 정보보호 특성을 조사하고 중소기업 정보보호 관리체계의 요구사항을 정리, 전문가 실증분석을 통해 정보보호 관리체계를 구성하였다. Valdevit et al.(2009)은 중소기업이 ISO/IEC 27001 인증을 획득하는 과정에 대한 연구를 수행, 전문가 검증을 통해 중소기업의 정보보호 관리체계 이행을 위한 가이드를 제시하였다. 장항배(2010)는 중소기업 산업기술 유출현황 조사결과를 바탕으로 중소기업의 산업기술 유출방지를 위한 정보보호 관리체계를 구성, 전문가 설문을 통해 정보보호 관리체계를 설계하고 문헌연구를 통해 적합성을 검증하였다. Mijnhardt et al.(2016)은 문헌연구와 전문가의 평가를 통해 중소기업의 위험과 우선순위를 식별하고 중소기업을 위한 빠르고 사용하기 쉬운 맞춤형 정보보호 평가도구를 제안하였다.

인력과 예산 측면에서 자체적 정보보호 활동에 어려움을 겪는 중소기업을 대상으로 정보보호 관리체계 모델과 정부의 지원정책 개선에 대한 다양한 연구가 이루어졌으나, 대부분의 연구가 실태조사와 전문가, 중소기업 관계자 설문을 통한 정성적 개선방안을 제시하는데 그쳤으며 실제 컨설팅 사례와 세부 정보보호 관리체계 점검 항목을 기반으로 하는 연구는 부재하였다.

본 연구에서는 실제 사례기반의 연구를 통해 실증적이고 현실에 맞는 정보보호 관리체계 개선방안을 도출하여 중소기업이 자율적으로 정보보호 활동을 할 수 있는 기반을 조성하고 정부의 관련 정책 개선에 기여하고자 한다.

3. 중소기업 컨설팅 지원사업

과학기술정보통신부와 한국인터넷진흥원은 중소기업을 대상으로 정보보호 관리체계 점검을 포함하여 전사적 보안 취약점을 점검하는 현장컨설팅을 수행하고 있다. 기업 당 1,500만 원이 지원되며 2021년 기준 600개사 지원을 목표로 지속 지원하고 있다. 민간 정보보호 전문 컨설팅 업체를 선정하여 총 3~5일의 컨설팅을 수행하고 있으며 컨설턴트가 체크리스트 기반으로 1~2일 정도의 현장 방문 컨설팅을 수행, 모의해킹 등 원격 기술진단 후 컨설팅 결과에 따른 개선방안 도출하고 맞춤형 솔루션 도입을 지원한다(한국인터넷진흥원, 2021). 본 연구에서는 정보보호 관리체계 점검 항목을 분석 대상으로 하여 개선사항을 도출하고자 하였다.

3.1 정보보호 관리체계 항목 분석

2020년 기준 정보보호 관리체계 점검 항목은 ① 정보보호 관리체계, ② 인원보안, ③ 시설보안, ④ IT보안 관리, ⑤ 보안사고 관리, ⑥ 개인정보 관리의 6개 영역과 이에 따른 19개 항목 및 60개의 세부 점

검항목으로 이루어져 있다(<표 1> 참조).

정보보호 관리체계의 영역은 '관리체계 기반마련 및 운영', '위험관리', '관리체계 점검 및 개선'의 세 항목과 9개의 세부항목으로 이루어져 있다. 인원보안의 영역은 '인적보안'과 '외부자 보안'의 2개 항목 및 6개의 세부항목으로 이루어져 있으며 시설보안 영역의 경우 '물리보안'과 '업무환경 보안'의 두 항목과 6개의 세부항목으로 구성되어 있다. 또한 IT보안관리 영역은 '인증 및 권한관리', '접근통제', '시스템 보안관리 및 암호화', '업무용 단말기기/보조 저장매체 관리', '악성코드 및 패치관리', '정보시스템 개발 보안'의 6개 항목과 27개의 세부항목으로 구성되어 정보보호 관리체계 점검항목 중 가장 큰 비중을 차지한다. 보안사고 관리 영역은 '침해사고 예방 및 대응체계 구축'과 '재해복구'의 두 항목으로 되어 있으며 개인정보 관리 영역에서는 '개인정보보호 관리체계 운영', '개인정보의 기술적 보호조치', '개인정보처리 시 보호조치', '정보주체 권리보호'의 4개 항목과 10개 세부항목으로 점검을 하고 있다.

한편 국내에서는 침해사고를 예방하고 기업의 기술적・관리적・물리적 보안수준을 제고하기 위하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 근거, 정보보호 및 개인정보보호 관리체계(ISMS-P)제도를 운영하고 있다(한국인터넷진흥원, 2021). 정보보호 및 개인정보보호 관리체계 인증기준은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항'의 3개 영역과 총 102개의 인증기준으로 구성되어 있다(<표 2> 참조).

정부에서 중소기업을 대상으로 하는 정보보호 관리체계 컨설팅의 6개 영역과 19개 항목은 모두 ISMS-P 인증기준 내에 포함되는 내용이었다. '정보보호 관리체계' 영역은 ISMS-P 인증기준의 '관리체계 수립 및 운영' 영역과 상응 하였으며 '인원보

〈표 1〉 중소기업 지원사업의 정보보호 관리체계 점검항목 구성(한국인터넷진흥원, 2021)

영역	항목	세부항목
1. 정보보호 관리체계	관리체계 기반 마련 및 운영	9개
	위험관리	
	관리체계 점검 및 개선	
2. 인원보안	인적 보안	6개
	외부자 보안	
3. 시설보안	물리보안	6개
	업무환경 보안	
4. IT보안관리	인증 및 권한관리	27개
	접근통제	
	시스템 보안관리 및 암호화	
	업무용 단말기기/보조저장매체관리	
	악성코드 및 패치관리	
	정보시스템 개발 보안	
5. 보안사고관리	침해사고 예방 및 대응체계 구축	2개
	재해복구	
6. 개인정보관리	개인정보보호 관리체계운영	10개
	개인정보의 기술적 보호조치	
	개인정보 처리 시 보호조치	
	정보주체 권리보호	
합계		60개

〈표 2〉 정보보호 및 개인정보보호 관리체계 인증기준 구성(한국인터넷진흥원, 2021)

영역	분야	항목
1. 관리체계 수립 및 운영	1.1. 관리체계 기반 마련	16개
	1.2. 위험 관리	
	1.3. 관리체계 운영	
	1.4. 관리체계 점검 및 개선	
2. 보호대책 요구사항	2.1. 정책, 조직, 자산 관리	64개
	2.2. 인적 보안	
	2.3. 외부자 보안	
	2.4. 물리 보안	
	2.5. 인증 및 권한관리	
	2.6. 접근통제	
	2.7. 암호화 적용	
	2.8. 정보시스템 도입 및 개발	
	2.9. 시스템 및 서비스 운영관리	
	2.10. 시스템 및 서비스 보안관리	
	2.11. 사고 예방 및 대응	
	2.12. 재해복구	
3. 개인정보 처리 단계별 요구사항	3.1. 개인정보 수집 시 보호조치	22개
	3.2. 개인정보 보유 및 이용 시 보호조치	
	3.3. 개인정보 제공 시 보호조치	
	3.4. 개인정보 파기 시 보호조치	
	3.5. 정보주체 권리보호	
합계		102개

안', '시설보안', 'IT보안관리', '보안사고관리'의 4개 영역은 ISMS-P 인증기준의 '보호대책 요구사항'에 포함되는 영역들이다. '개인정보관리' 영역 역시 ISMS-P 인증기준에서 '개인정보 처리 단계별 요구사항' 영역으로 운영 중에 있다(한국인터넷진흥원, 2021)(<표 3> 참조).

중소기업 대상 정보보호 관리체계 컨설팅 항목은 ISMS-P 인증기준에 비해 정보보호 역량이 부족한 기업에서 이해하기 어려운 내용과 준수하기 어려운 내용이 제외되어 있는 등 비교적 간소화되어 운영되고 있다. 정보보호 관리체계 기반마련의 분야에서 ISMS-P 인증기준에서는 정보보호 최고 책임자와 실무조직, 정보보호 위원회 및 담당자 협의체의 구성과 운영을 위한 예산 및 자원의 할당을 요구하지만 중소기업 대상의 컨설팅 기준에서는 정보보호 업무를 전담하거나 겸직하여 보안활동을 수행하고 있는지의 여부만 묻고 있다. 또한 정보보호 관리체계 전 영역에 대한 업무 절차 및 흐름의 문서화, 조직의 대내외 환경 분석을 통한 위험평가와 이에 따른 보호대책 선정 및 이행계획 수립 등의 내용은 제외되어 있다. 최소한의 핵심적인 내용만 담고 있으며 관리체계 운영과 점검, 개선에 대해 지속적이고 주기적인 활동을 요구하고 있지 않다. 이는 최초 심사 이후 보완조치 여부를 확인하고 인증 이후 1년 단위의 사후심사를 거치는 ISMS-P 인증과 달리, 1회성의 전사적 컨설팅을 위하여 항목을 구성한 것으로 판단된다.

중소기업 대상 정보보호 관리체계 컨설팅 항목 중 '인원보안' 영역에서는 임직원 및 관련 외부자의 보안 위반 시 조치에 대한 내용과 외부자 보안에 대한 현황관리 및 관리·감독 등 이행관리에 대한 내용이 빠져있었으며 외부자와 관련하여서는 계약 시의 보

안 준수사항에 대한 내용만 포함되었다.

'시설보안' 영역에서는 정보시스템의 보호에 대한 내용과 보호구역 내의 작업기록, 반출입 기기 통제에 대한 내용이 제외된 한편, 외부 집적정보통신시설(IDC)에 운영 위탁하는 경우 물리적 보안 요구사항을 계약서에 반영하는지 여부가 추가, 포함되어 있다. 정보자산을 외부에 위탁하거나 호스팅 서비스를 주로 이용하는 중소기업의 행태를 반영한 것으로 분석된다.

'IT보안관리' 영역에서는 정보시스템의 사용자 식별에 대한 세부사항과 특수 목적을 위하여 사용하는 계정 및 권한의 별도관리에 대한 내용이 제외되어있다. 또한 정보시스템 도입/개발 시의 보안과 관

〈표 3〉 정보보호 관리체계 점검항목 비교

중소기업 지원사업의 정보보호 관리체계 점검항목		정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증기준	
항목	항목수	분야	항목수
관리체계 기반 마련 및 운영	4	1.1. 관리체계 기반마련	6
		2.1. 정책, 조직, 자산 관리	3
위험관리	2	1.2. 위험 관리	4
관리체계 점검 및 개선	3	1.3. 관리체계 운영	3
		1.4. 관리체계 점검 및 개선	3
인적 보안	4	2.2. 인적 보안	6
외부자 보안	2	2.3. 외부자 보안	4
물리보안	4	2.4. 물리 보안	7
업무환경 보안	2		
인증 및 권한관리	5	2.5. 인증 및 권한관리	6
접근통제	9	2.6. 접근통제	7
시스템 보안관리 및 암호화	4	2.7. 암호화 적용	2
		2.9. 시스템 및 서비스 운영관리	7
		2.10. 시스템 및 서비스 보안관리	-
업무용 단말기기/보조저장매체관리	4	2.10. 시스템 및 서비스 보안관리	9
악성코드 및 패치관리	3	2.10. 시스템 및 서비스 보안관리	-
		2.11. 사고 예방 및 대응	-
정보시스템 개발 보안	2	2.8. 정보시스템 도입 및 개발	6
침해사고 예방 및 대응체계 구축	1	2.11. 사고 예방 및 대응	5
재해복구	1	2.9. 시스템 및 서비스 운영관리	-
개인정보보호 관리체계운영	3	1.1. 관리체계 기반마련	-
		2.2. 인적 보안	-
개인정보의 기술적 보호조치	3	2.5. 인증 및 권한관리	-
		2.7. 암호화 적용	-
		2.9. 시스템 및 서비스 운영관리	-
개인정보 처리 시 보호조치	2	3.1. 개인정보 수집 시 보호조치	7
		3.4. 개인정보 파기 시 보호조치	3
정보주체 권리보호	2	3.5. 정보주체 권리보호	3
미포함	-	2.12. 재해복구	2
		3.2. 개인정보 보유 및 이용 시 보호조치	5
		3.3. 개인정보 제공 시 보호조치	4
합계	60	합계	102

련하여 소스코드 변경이력, 운영환경으로의 이관절차 수립 등 개발보안에 대한 관리여부를 묻고 있으며 소스 프로그램의 접근관리, 시험 데이터에 대한 보관과 파기 등의 세부 내용은 생략되었다. 그 외에도 시스템 및 서비스 운영에 대한 성능과 장애관리 등 가용성과 관련된 부분이 일부 제외되어 있다. 로그와 접속기록에 대한 관리 여부는 확인하고 있으나 그 정확성을 보장하기 위한 점검과 시간 동기화 등의 내용은 생략되어 있으며 정보자산의 재사용 및 폐기절차 역시 제외되어 있다.

'보안사고관리' 영역은 사고 예방 및 대응체계 구축과 백업 · 복구 관리에 대한 내용으로 구성되어 있으며 ISMS-P 항목과 비교하여 세부적인 사고대응 훈련과 개선, 재발방지 대책의 수립 등의 내용은 빠져있다.

ISMS-P의 기준의 '보호대책 요구사항'에 해당하는 내용들은 중소기업 정보보호 컨설팅 항목에 동일한 내용으로 포함되어 있다 하더라도 기술적 세부사항 및 절차와 대책에 대한 계획수립 여부 보다는 관련 솔루션의 활용 여부를 확인하는 항목으로 구성되어 있음을 확인하였다.

'개인정보관리' 영역은 ISMS-P 기준의 개인정보처리단계별 요구사항과는 다소 다르게 구성되어 있다. 개인정보보호 책임자 지정과 교육, 개인정보보호 정책 등 개인정보보호 관리체계 운영에 관한 내용이 포함되어 있으며 개인정보 취급자의 접근권한 관리, 개인정보 암호화 적용 등 개인정보의 기술적 보호조치에 대한 항목으로 구성되어 있다. 개인정보처리 시 보호조치에 관하여서는 적법한 절차에 의해 동의에 따른 개인정보 수집 여부를 묻고 있으나 14세 미만 아동의 개인정보 수집, 민감정보 및 고유식별번호의 별도 동의, 홍보 및 마케팅 목적의 활용 시 조치 등 세부적인 내용은 생략되어 있다. 또한 개인정보 보유 및 이용 시의 보호조치와 제3자 제공 및 업무 위탁 등 개인정보 제공 시의 보호조치에 대한 내용이 제외되어 있다.

정부의 중소기업 대상 정보보호 관리체계 컨설팅 항목을 ISMS-P 기준의 점검항목을 비교 분석한 결과 분야와 항목별 내용이 같다 하더라도 절차나 방식 등 세부적인 사항보다는 주요내용에 대한 준수 여부를 묻고 있는 경우가 대부분 이였으며, ISMS-P 기준에서 세부 분야로 나누어 이행여부를 확인하는 사항들을 하나로 통합하여 포괄적 항목의 이행 여부만을 묻는 점검 항목으로 활용하기도 하였다.

ISMS-P 인증기준의 세부항목 중 필요한 부분만 뽑아 항목으로 재구성하는 등의 형태를 보였으며, 특히 개인정보관리 영역의 경우에는 개인정보 처리단계(수집-보유-제공-파기)에 따른 구성이 아닌 관리적, 기술적 측면의 개인정보 관리에 대한 내용으로 구성되었다. ISMS-P 인증기준에서는 '관리체계 수립 및 운영' 이나 '보호대책 요구사항' 영역에서 정보보호 활동과 함께 묻고 있는 개인정보보호 부분을 분리하여 별도로 점검하고 있는 것이다.

중소기업 대상 현장 방문 컨설팅이 1개 기업 당 1~2일 정도 투입되는 인력과 시간적 여건상 정보보호 관리체계 점검 항목이 관리적, 기술적, 물리적 보안에 대해 주요 내용만으로 구성된 것으로 분석된다.

3.2 2020년 중소기업 지원 결과

2020년 중소기업 정보보호 컨설팅 지원사업의 정보보호 관리체계 점검결과를 한국인터넷진흥원을 대상으로 한 정보공개 청구(정보공개포털, www.open.go.kr)를 통하여 확보하였다(한국인터넷진흥원 정보공개 자료, 2021). 지원기업 중 무작위의 50개사를 대상으로 데이터를 받아, 구성하였으며 재직자 50인 미만의 기업 25개사, 50인 이상 기업 25개사로 구성하였다(2020년 총 400여 개사 지원).

컨설팅 전, 후 정보보호 관리체계 수준을 분석한 결과는 <표 4>와 같다. 컨설팅 전 최초 진단 시 평균 점수(보안율)은 50.38%, 컨설팅 이후 평균 점수는 56%로 5.62%p 상승하였다. 재직자 수 50인 미만/이상 기업의 결과를 분석하였을 때 컨설팅 전 재직자 50인 미만인 기업의 점수는 48.35%, 50인 이상인 기업은 52.40%로 재직자 수 50인 이상인 기업이 4%p 정도 높은 보안수준을 보였다. 컨설팅 이후

재점검 시 보안점수는 재직자 50인 미만의 기업은 54.16%, 50인 이상의 기업은 57.84%로 확인되었다.

〈표 4〉 2020년 중소기업 대상 정보보호 관리체계 컨설팅 결과(한국인터넷진흥원, 2021)

재직자	컨설팅 전	컨설팅 후	개선정도	비 고
50인 미만	48.35%	54.16%	5.81%p	25개사
50인 이상	52.40%	57.84%	5.44%p	25개사
평균	50.38%	56.00%	5.62%p	50개사

4. 연구설계

4.1 연구모형(프로세스)

정부 지원 2020년 중소기업 대상 정보보호 관리체계 컨설팅의 항목별 결과를 바탕으로 컨설팅 전, 후 개선이 미흡하였던 항목을 도출, 중소기업 관계자와 정보보호 컨설턴트, 정책담당자를 대상으로 인터뷰를 실시하여 개선방안을 분석하였다.

정보보호 관리체계 점검항목은 ‘a’, ‘b’, ‘c’ 3개의 척도로 이루어져 있는데, ‘a’는 해당 항목을 잘 이행하고 있는 것, ‘b’는 항목을 준수하고 있으나 일부 운영이 미흡한 것, ‘c’는 해당 항목을 이행하지 않고 있는 것으로 정의되어 있다. 본 연구에서는 컨설팅 전 최초 점검 시 ‘c’ 점수(즉 해당 항목을 이행하고 있지 않은 것)에 대해 컨설팅 이후에도 ‘c’ 점수를 받아 여전히 이행이 되지 않으며 개선이 되지 않은 항목에 대해 연구를 진행하였다.

위와 같이 개선이 되지 않은 항목들은 그 내용이 중소기업이 준수하기에 과도하거나 적합하지 않은 것일 수 있으며 또는 컨설팅의 방법론이 잘못되어 기업의 이해도가 떨어지거나 조치 방법이 잘못되었을 수도 있다. 그 외에도 한 번의 컨설팅만으로는 단기적으로 개선이 어려워 지속적인 지원이 필요한 경우일 수도 있다.

이에 개선이 되지 않은 각 항목에 대해 실제로 컨설팅을 받은 중소기업(4개사)과 중소기업 대상 다수의 컨설팅을 진행한 정보보호 컨설턴트(3명), 중소기업 정보보호 컨설팅 지원사업 관련 정책을 이행하는 담당자(3명)를 대상으로 인터뷰를 실시하였다. 해당 항목이 컨설팅 전, 후 효과가 없었던 이유와 개선방안을 도출하는 것을 목표로 각 항목이 제외되어야 할지, 또는 다른 항목과 대체 또는 통합되어야 할지 등의 결과를 도출하고자 하였다. 또한 정보보호 관리체계 점검 항목에서 빠져있어 추가하여야 할 중요한 내용이나, 전체적인 컨설팅 항목에 대한 정성적인 의견을 반영하고자 하였다.

추가로 기업은 규모와 업종에 따라 정보보호 관리 역량에 큰 차이를 보이고 있는데, 한국정보보호산업협회의 2020 정보보호 실태조사에 따르면 기업 재직자수 50인을 기준으로 정보보호(개인정보보호)의 정책과 조직의 보유율, 교육 실시율 등 정보보호 수준에 큰 격차를 보이고 있다(한국정보보호산업협회, 2021). 이에 본 연구에서는 재직자 기준의 규모별로 필요한 정보보호 관리체계의 준수 수준이 상이할 것으로 판단하여 재직자 수 50인을 기준으로 컨설팅 항목들이 적절한지 등의 연구를 수행하였다. 업종이나 산업별 특성에 따른 기준으로도 정보보호 수준의 격차를 보이고 있으나 업종의 기준이 다양하여 주요 업종별로 별도의 연구가 필요할 것으로 생각된다. 기업 규모의 기준으로 연간 매출액을 선정할 수도 있으나 매출액은 중소기업의 특성상 연도별로 단기적으로 변화가 클 수 있으므로 비교적 단기적으로 변하지 않는 수치인 재직자 수를 기준으로 하는 것이 더 적합할 것으로 판단하였다.

4.2 연구 데이터

개선이 필요한 항목의 도출을 위하여 본 연구에서 자체적인 기준 측도를 정하였다. 중소기업 대상 정보보호 관리체계 컨설팅 점검 결과 50개사 중 최초 진단 시 ‘c’ 등급을 받은 기업의 비율을 ‘미흡률’로 정의하였다. 즉 50개사 중 25개사가 컨설팅 전 진단 시 A 항목에서 ‘c’ 등급을 받았다면 A 항목의 ‘미흡률’은 50%이다. 최초 진단에서 ‘c’를 받은 기업 중 컨설팅 이후 재점검 시에도 여전히 ‘c’ 등급을 받은

〈표 5〉 연구 데이터 용어정의

용어	정의	비고
미흡률	연구대상 50개사 중 (컨설팅 전) 최초 진단시 'c'등급을 받은 기업의 비율	최초진단시 'c'등급을 받은 기업 수 / 전체기업수(50개사)
미개선율	컨설팅 전 최초 진단 시 'c' 등급을 받은 기업 중 컨설팅 이후에도 여전히 'c'등급을 받은 기업의 비율	컨설팅 이후에도 'c'등급을 받은 기업 수 / 최초진단시 'c'등급을 받은 기업 수

기업의 비율을 '미개선율'로 정의하였다. 즉 50개사 중 최초 진단에서 'c'등급을 받은 기업이 40개사 인데, 그중 컨설팅 이후 점검에서도 여전히 'c'를 받은 기업이 30개사일 경우 '미개선율'은 75%이다. 개선되어야 할 정보보호 관리체계 컨설팅 항목으로 최초 진단 시 전체 기업의 50% 이상이 미 준수(미흡률) 하고 있으며 컨설팅 이후에도 과반수이상의 기업에 대해 전혀 개선이 되지 않은(미개선율) 항목을 선정하였다(<표 5> 참조).

연구대상 항목으로 총 60개의 정보보호 관리체계 컨설팅 항목 중 13개의 항목이 도출되었으며, '정보보호 관리체계' 영역에서 5개 항목, '인원보안' 영역에서 1개 항목, 'IT보안관리' 영역에서 6개 항목, '보안사고관리' 영역에서 1개 항목이 해당되었다. 각 항목별 분석결과는 <표 6>과 같다.

정보보호 관리체계 기반마련 및 운영 항목에서 정보보호정책의 유지관리에 관한 항목은 전체 기업의 72%가 미준수 하고 있었으며 컨설팅을 받은 이후

〈표 6〉 연구 대상 컨설팅 항목 분석결과

구분	영역	항목	미흡률 (컨설팅 전)	미개선율 (컨설팅 후)
1	정보보호 관리체계	정보보호 정책의 정기적 검토	72%	94.44%
2		식별된 정보자산에 대한 중요도 및 보안등급 부여	68%	67.66%
3		주기적·상시적으로 수행하여야 할 정보보호 활동의 식별	48%	100%
4		정보보호 관리체계 점검 및 경영진 보고	64%	96.88%
5		정보보호 관리체계 점검 시 발견된 문제점에 대한 개선조치 이행	66%	96.97%
6	인원보안	연간 정보보호 교육계획을 수립 및 연 1회 이상 교육 실시	58%	96.55%
7	IT보안관리	네트워크 이상행위 분석 및 모니터링 수행	54%	88.89%
8		정보시스템 세션 타임아웃을 적용	50%	100%
9		사용자 PC 단말에서의 네트워크를 통한 정보유출 대책 마련	72%	66.67%
10		내부자료 유출방지를 위한 대책 마련	70%	77.14%
11		보조저장매체를 통한 정보유출 방지를 위한 대책 마련	64%	81.25%
12		정보시스템의 알려진 취약점에 대한 정기적 분석 및 점검 수행	92%	69.57%
13	보안사고관리	침해사고 및 개인정보 유출사고에 대한 예방·대응 체계와 절차 마련	78%	100%

에도 대부분의(94.4%)의 기업에 대해 개선이 되지 않았다. 즉 정보보호 정책을 보유하지 않거나, 보유하고 있더라도 주기적인 제·개정을 하지 않는다는 것이다. 정보보호 정책을 보유하지 않았던 기업이 컨설팅 이후 정보보호 정책을 수립·보유한 비율(개선율)인 56.3%와 비교하여 매우 높은 미개선율을 보이며, 이는 중소기업이 정형화된 양식을 활용하여 정보보호 정책을 수립하는 것에는 어려움이 덜하지만 그것을 지속적으로 제·개정하고 유지보수, 회사의 상황에 맞게 변화시키는 데는 어려움을 겪는 것으로 분석된다.

68%의 기업이 '보유한 자산에 대한 중요도 평가와 보안등급 부여' 활동을 하지 않고 있는데, 정보자산을 식별하고 있는 기업이 대다수(78%)인 점과 대비된다. 즉 회사의 정보자산 자체를 식별하고 목록화 하고는 있으나, 보안의 측면에서 중요도 평가는 이루어지지 않고 있는 것이다. 67% 이상의 기업이 컨설팅 이후에도 해당 활동을 하지 않았다.

정보보호 관리체계 점검 및 개선의 항목은 ① 주기적 또는 상시적으로 수행하여야 할 정보보호 활동을 식별하고 있는가, ② 정보보호 관리체계를 점검하고 경영진에게 보고하고 있는가, ③ 점검하여 발견된 문제점에 대해 개선조치를 하는가의 3가지 세부항목으로 이루어져있다. 첫 번째 항목은 48%의 기업이 미준수하고 있었으며 컨설팅 후에도 모든 기업에서 개선이 되지 않았다. 다른 두 항목의 경우에도 과반수이상(각 64%, 66%)의 기업이 준수하지 않고 있었으며 컨설팅 이후에도 대부분의 기업(1개사를 제외한 모두)이 개선되지 않았다. 즉 중소기업은 정보보호 관리체계의 전반적인 수립·관리 활동에 어려움을 겪고 있는 것으로 분석된다.

인원보안 영역에서 정보보호 교육의 시기, 대상, 방법 등의 내용이 포함된 연간 정보보호 교육계획을 수립하고 계획에 따라 연 1회 이상 교육을 실시하고 있는가에 대한 항목은 58%의 기업이 미준수하고 있었으며 컨설팅 이후에도 97%의 기업이 여전히 준수하지 않았다. 이는 정보보호를 위한 별도의 교육 예산편성이 어려운 중소기업의 여건 또는 정보보호에 대한 인식의 부족과 연결 지을 수 있을 것이며, 정기적인 교육을 위한 계획수립에는 어려움이 있고 정부지원의 교육 등이 있을 때 상시적으로 교육을 실시하기 때문으로 보여진다.

IT보안관리 영역의 네트워크 이상행위 분석 및 모니터링 항목의 경우 침입차단을 위한 방화벽, IPS 등의 장비를 운영하고 있는지의 여부를 묻는 항목으로 89%의 기업이 컨설팅 이후에도 개선이 되지 않았으며 이는 중소기업의 재정적 여건에 따라 단기간에 개선되기 어려운 항목임을 고려할 때 당연한 결과로 판단된다.

정보시스템 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는지를 묻는 항목에 대해 50%의 기업이 미 이행중이였으며 해당 기업 모두가 컨설팅 이후에도 미 이행 하였다. 또한 사용자 PC 단말에서 네트워크를 통한 정보유출을 차단하기 위한 대책마련 여부를 묻는 항목에서 72%의 기업이 미 준수 하였으며 미 준수 기업 중 66.7%가 컨설팅 이후에도 별도의 대책을 마련하지 않았다. 내부자료의 유출방지를 위한 대책 마련의 항목에서도 70%의 기업이 준수하지 않고 있었으며 미 준수 기업 중 77.1%가 컨설팅 이후에도 별도의 대책을 마련하지 않았고, 중요정보 유출방지를 위한 보조저장매체 관리 대책 마련에 대한 항목에서도 64%의 기업이 미 준수, 컨설팅 이후에도 81.3%의 기업이 개선하지 못하였다. 또한 정보시스템의 알려진 취약점에 대한 정기적인 분석 및 점검을 수행하고 있는가에 대한 항목에서 92%의 기업이 준수하지 않고 있었으며, 컨설팅 이후에도 70%의 기업이 여전히 준수하지 않았다. 94%의 기업이 백신 소프트웨어를 활용하고 지속적인 업데이트를 하고 있으며, 활용하지 않았던 기업도 컨설팅 이후 모두 백신 소프트웨어를 활용하는 것과 대비해 볼 때 중소기업의 자체적인 정보보호 역량으로는 이행하기 어려운 것으로 파악된다. 이는 자동화 도구를 도입하여 취약점 분석을 수행할 수 있겠지만 한정된 예산에서 보안 솔루션 도입의 우선순위를 따져 볼 때 이행하기 어려운 점이 있을 것으로 판단된다.

총 13개의 연구대상 컨설팅 항목 중 'IT보안관리' 영역에서 6개의 항목이 도출되었으며 이는 기술적인 조치가 필요한 분야에서 전문가의 확보와 역량이 부족한 중소기업의 특성에 따른 결과로 분석되며 한정된 예산에 따라 보안 솔루션의 도입이 어려워 단기적인 개선이 어려운 점이 있을 것으로 판단된다.

보안사고 관리 영역에서 78%의 기업이 침해사고 및 개인정보 유출사고 대응체계와 절차를 마련하고 있지 않았으며 컨설팅 이후 해당 기업의 모두(100%)가 여전히 개선을 하지 않았다. 한국정보보호산업협회의 2020년 정보보호 실태조사에서 침해사고 대응 활동으로 73%가 '별다른 활동을 수행하지 않음'으로 응답한 것과 상응하는 결과이다.

5. 인터뷰 결과 및 해석

5.1 중소기업 담당자

2020년 한국인터넷진흥원에서 추진한 중소기업 대상 정보보호 컨설팅을 실제로 경험한 중소기업 4개사를 대상으로 대면 인터뷰를 진행하였다. 인터뷰는 컨설팅을 대응한 담당자를 대상으로 2021년 6월 기업 별 각 1시간 내외의 질의응답 형식으로 진행되었다. 정보보호 관리체계 컨설팅 전, 후 개선이 없었던 항목을 제공하고 중소기업의 입장에서 해당 항목이 실효성이 있는지, 컨설팅을 통해 개선이 될 수 있는 사항인지, 현실적으로 이행하기 어려운 항목인지 등의 의견을 물었다. 그 외에도 전체적인 컨설팅 항목 또는 지원사업에 대한 정성적인 의견, 실제 컨설팅 수행 간 애로사항이나 바라는 점 등을 인터뷰하였다. 인터뷰 결과는 다음과 같이 요약된다.

- 중소기업이 이행하고 개선하는데 어려움을 겪은 대부분의 항목이 인력과 예산의 한계와 관련됨
- 정보보호 솔루션의 도입 및 유지보수 비용의 문제로 이행할 수 없는 항목이 다수 존재
- 기술적 부분에 대한 담당자의 이해도 부족으로 중소기업의 보안역량을 고려한 가이드 필요
- 1회성이 아닌 지속적 정보보호 체계 마련을 위한 지원 필요

세부 항목에 대한 기업 담당자의 의견을 보았을 때 정보보호 관리체계 영역의 정보보호 정책의 유지관리 항목(정보보호 정책을 정기적으로 검토하고 제 · 개정하고 있는가)에 대하여 4개 중소기업 담당자 모두 관리 인력의 문제를 답하였다. 중소기업의 경우 현실적으로 정보보호 담당 조직이 없거나, 있더라도 한사람이 여러 가지 업무를 겸직하는 행태를 보이며 업무의 우선순위를 따져볼 때 정보보호에 대한 지속적인 관심이 어려움을 확인하였다. 특히 인력의 변동이 잦은 중소기업의 여건상 담당자가 퇴사하는 등의 경우에 인수인계가 제대로 이루어지지 않는 등의 문제가 있었다. 개정 주기표 및 개정 시 반영되어야 할 항목을 제시하거나 정보보호 정책에 대한 우수사례를 공유하여 지속적인 정보보호 활동을 할 수 있게끔 해달라는 등의 요구가 있었다. 정보보호 관리체계 유지보수 여부 이전에 경영진 차원의 정보보호 인식에 대한 제고가 선행되어야 할 것으로 판단된다.

정보자산에 대해 중요도와 보안등급을 부여하고 있는지를 묻는 항목에 대해서는 담당자의 보안 역량 부족이 문제점으로 드러났다. 자산의 보안등급을 정하는 기준에 대하여 정보보호 담당자의 경험과 역량이 부족하여 정보자산 평가 활동에 어려움을 겪고 있었다. 정보자산의 중요도 및 보안등급 등에 대한 가이드라인과 컨설팅 시 상세한 설명이 필요하다는 의견이 제기되었다. 그 외에도 정보자산에 대한 중요성을 알고 있더라도 시간과 비용 등의 이유로 기업의 전체적인 정보자산 관리에 대한 문서화에 어려움이 있었으며 자산별로 개별적인 관리가 이루어지고 있는 경우가 대다수였다. 정보자산에 대한 보안등급을 부여하고 지속적인 관리가 가능하도록 도움을 주는 도구(프로그램)의 활용 또는 지원이 필요할 것으로 생각된다.

주기적 · 상시적으로 수행하여야 할 정보보호 활동을 식별하는 활동과 정보보호 관리체계 운영에 대한 점검, 점검 결과 문제점에 대한 개선조치 등의 항목에 대해 중소기업은 경영진의 인식 문제를 지목하

였다. 정보보호 관리체계를 전담하는 직원이 없을뿐더러 해당 업무에 대해 관리자가 아닌 일선의 담당자에게 맡겨놓는 경우가 대다수였다. 의무적으로 준수하여야 하는 것이 아닌 사항에 대해 여러 업무를 겸직하는 정보보호 담당자가 지속적이고 주기적인 정보보호 활동을 하는 데는 어려움이 있었다.

인원보안 영역의 연간 정보보호 교육계획 수립과 계획에 따른 연 1회 이상 교육의 실시 여부를 묻는 항목은 체계적이고 지속적인 임직원 정보보호 교육을 요구하고 있는 항목이지만 중소기업은 정보보호 교육 자체에 대한 우선순위가 낮은 것으로 나타났다. 매출과 생산 활동에 우선순위를 두고 있는 현실에 따라 정보보호 관련 교육은 정부 또는 지자체의 지원에 의해 이루어지고 있었으며 그조차도 정보보호 교육이 있는지 모르거나, 있더라도 정보보호 교육을 시간 낭비 또는 휴식시간 등으로 생각하는 사례가 있었다. 그 외에도 정부지원 등의 교육이 대부분 정보보호의 중요성에 대한 내용에서 그쳐 실무적이고 실질적인 정보보호 활동에 도움이 되지 않는다는 의견이 있었다. 계획을 수립하고 이행하는 등의 행정적인 요구사항에 대한 준수 여부 보다는 실질적으로 도움이 되는 정보보호 교육이 지속적으로 이루어질 수 있도록 하는 것이 중요할 것으로 판단된다.

IT보안관리 영역의 항목들은 대부분 중소기업에서 비용과 기술력의 문제로 컨설팅 전과, 후에도 이행하기 힘든 부분이 있는 것으로 나타났다. 네트워크 이상행위 분석 및 모니터링 항목은 예산의 문제로 방화벽을 도입하지 못하는 경우가 있었으며, 도입했다고 하더라도 단순 장비의 운영수준에 그치는 경우가 대부분 이였다. 특히 기술적인 부분에 있어 정보보호 전공자라고 하더라도 네트워크 침입탐지와 모니터링 등의 전문적 내용에 대해서는 어려움을 겪는 것으로 드러났다. 개념에 대한 이해조차 부족한 현실에서 단순히 장비를 도입하였다고 해당 항목이 이행되고 있다고 보는 것에 문제가 있다는 지적도 제기되었다. 담당자의 정보보호에 대한 관심만으로는 인터넷에 검색해보는 등의 행위로 그쳐 실제 네트워크 보안에 대한 적용에 어려움이 있으며 관련 실무 교육 등의 지원이 필요한 것으로 나타났다.

정보시스템의 세션 타임아웃 설정과 관련하여서도 중소기업의 이해도가 낮은 것으로 나타났으며, 해당 내용을 알고 있더라도 업무의 불편함을 야기하는 이유로 현실적인 적용에 어려움이 있었다. 또한 직원 간에도 정보시스템 활용 이해도에 격차가 있어 전사적 차원의 조치가 있어야 이행될 수 있으며, 간단한 프로그램 등으로 쉽게 적용할 수 있는 방법에 대한 요구가 있었다. 또한 중소기업에서는 대부분 업무용 상용 프로그램(ERP, MES 등)이 사용되고 있어 해당 프로그램 제공 업체에서 옵션으로 제공하는 것이 편할 것 같다는 의견도 있으며, 그 외에도 세션 타임아웃 설정을 어느 정도로 설정해야 보안에 효과적인지 등의 이해도가 떨어지는 현실에서 컨설팅 과정에서는 설정 여부만을 묻는 것이 모순이라는 지적이 제기되었다.

사용자 PC 단말에서의 정보유출 대책과 관련하여 중소기업에서는 관련 솔루션의 활용으로만 이행 가능한 것으로 판단하고 있었다. DLP, DRM, 안티바이러스 등의 솔루션이 필요하지만 기업의 예산과, 지원을 받더라도 솔루션 도입의 우선순위로 인해 도입이 어려운 것으로 나타났다. 또한 도입 이후의 유지보수비가 부담이 된다는 의견도 있었다. 사용자 PC 단말에서의 보안과 관련하여 전사적 차원의 규정에 대한 필요성도 있지만 일부 중소기업에서는 세세한 것 까지 규정으로 만들 필요는 없다고 생각하였으며 시간과 인력의 여력이 부족함을 이유로 들었다.

내부자료 유출방지를 위한 대책 마련여부를 묻는 항목 역시 PC 단말의 보안 대책과 마찬가지로 솔루션 도입에 대한 어려움이 제시되었다. 도입비용과 유지보수 비용의 문제로 자체 도입이 어려우며 정보보호의 우선순위를 따졌을 때 비교적 중요하지 않다고 생각하는 부분까지 대기업 수준의 정보보호 체계를 갖추는 것은 어렵다고 생각하는 것으로 나타났다.

보조저장매체를 통한 유출방지를 묻는 항목에 대해서도 솔루션 도입의 어려움을 토로하였으며 사실상 보조저장매체와 관련된 보안에 대한 인식 자체가 부족한 것으로 나타났다. 업무의 편의성을 우선시

하여 보조저장매체의 통제에 대한 부정적 시각도 존재하였다.

정보시스템 취약점에 대한 분석과 점검여부에 대해서는 4개 중소기업 모두 자체적 이행이 현실적으로 불가능하다고 답변하였다. 예산과 운영인력에 대한 어려움이 있었으며 침해사고를 경험한 경우에도 기술적 부분에 대한 이해도 부족으로 사후 대비책을 마련하지 못한 사례도 있었다. 보안에 대한 담당자의 의지가 있어 무료 소프트웨어 도구를 활용하고자 하더라도 어떤 프로그램이 회사에 적합한지 몰라 이행이 어려운 것으로 나타났다.

침해사고 및 개인정보 유출사고에 대한 예방·대응 체계, 절차와 관련하여 중소기업의 인식이 부족한 것으로 나타났다. 4개 중소기업 모두 해당 내용에 대한 컨설팅을 받은 기업임에도 불구하고 침해사고 및 유출사고의 예방과 대응 방안에 대해 정확히 모르고 있는 것으로 드러났다. 보안에 대한 역량 부족으로 인해 도움을 받을 수 있는 경로와 절차에 대해 모르고 있었으며 침해사고와 관련된 자료를 접하여도 세부적인 내용에 대한 이해도는 떨어지는 것으로 나타났다. 유사사례를 바탕으로 그에 대한 대안, 방법 등을 현실성 있게 알려주었으면 좋겠다는 의견도 있었다.

컨설팅 세부 항목에 대한 의견 외에도 컨설팅 방법론과 지원사업에 대한 전반적인 의견이 다수 제기되었다. 많은 양의 컨설팅 항목으로 담당 직원에 대해 질의응답(준수여부를 묻고 답하는) 방식으로 진행되어 해당 직원도 전체적인 회사의 정보·보안 시스템에 대한 이해도가 부족한 채 컨설팅을 수행하였으며 위와 같은 이유로 컨설팅 이후에도 전체적인 기업의 보안수준의 향상 보다는 일부 기능의 적용에 대해서만 조치하였다는 의견이 있었다.

또한 컨설팅 항목에 대한 준수여부만을 묻는데 그쳐 컨설팅 이후에도 적절한 가이드가 제공되지 못했다는 지적이 제기되었다. 컨설팅 이후 솔루션 도입 지원의 경우에도 단순히 기업이 원하는 솔루션을 지원해주는 경우가 있어, 컨설팅결과를 바탕으로 한 적절한 솔루션 추천에 대한 요구가 존재하였다.

기업의 업종과 특성에 대한 분석이 이루어지지 않은 채 보안 시스템의 구축 여부를 묻는 것이 효과성이 떨어진다는 의견도 제시되었으며 기업의 정보보호 수준에 맞는 단계별 지원방법, 1회성 지원이 아닌 지속적 정보보호 체계 마련을 위한 지원방안 등의 필요성이 제기되었다.

5.2 정보보호 컨설턴트 및 정책 담당자

정보보호 컨설턴트는 기업 컨설팅 분야 경력이 10년 이상이고 중소기업 대상 컨설팅 경험이 있는 컨설턴트 3명으로 구성하였으며, 정책 담당자의 경우 한국인터넷진흥원의 기업 정보보호 관리체계(ISMS) 관련 부서 및 중소기업 정보보호 지원부서의 관리자 경력이 있는 2명과 정책 연구위원 등을 역임한 학계 전문가 1명으로 구성, 각각의 의견을 연구에 반영하였다.

인터뷰는 2021년 7월~8월 중소기업 담당자의 인터뷰 결과와 정보보호 관리체계 컨설팅 전, 후 개선이 미흡한 항목을 제공한 후, 대면/비대면 인터뷰를 병행하여 1명당 1시간 내외로 진행되었다. 각 항목별 개선사항에 대한 정성적인 의견과 50인 미만의 기업에도 적용하여야 할지 여부 등을 묻는 내용으로 수행되었으며 정보보호 관리체계 컨설팅 및 지원사업 개선을 위한 정성적 의견도 추가로 반영하였다.

항목별 분석 결과, 정보보호 컨설턴트 3명의 각 항목에 대한 의견은 대체로 일치하였다. 특히 다음 4가지 점검 항목에 대해서는 중요도가 높고 중소기업에 필요성이 높아 이행하여야 할 것으로 보았다.

- 정보자산에 대한 중요도와 보안등급 부여
- 연간 교육계획 수립 및 1회 이상의 교육 실시
- 정보시스템 취약점에 대한 분석 및 점검
- 침해사고 및 개인정보 유출사고에 대한 예방·대응 체계 마련

위 항목과 관련하여 중소기업이 이행하기 어려운 부분은 수준을 완화하여 적용하거나 정부의 추가 지원이 필요할 것으로 평가하였다. 위 내용 외의 다른 항목에 대해서는 그 필요성이 낮거나 중소기업에서 현실적으로 이행이 불가능 할 것으로 판단하였다.

정책담당자 3명의 경우 일부 항목에서 의견이 나뉘었으나 다수의 항목에서 의견이 일치하였으며 다음의 7개 항목에 대하여 전원이 중소기업에서 준수할 필요성이 있을 것으로 보았다. 중소기업이 현실적으로 준수하기 어려운 부분은 기준을 완화하는 등의 방식으로 이행을 유도할 것을 제시하였다.

- 정보보호 정책의 정기적 검토
- 정보자산에 대한 중요도와 보안등급 부여
- 연간 교육계획 수립 및 1회 이상의 교육 실시
- 네트워크 이상행위 분석 및 모니터링
- 보조저장매체 보안 대책 마련
- 정보시스템 취약점에 대한 분석 및 점검
- 침해사고 및 개인정보 유출사고에 대한 예방·대응 체계 마련

연구대상 항목들 대부분이 50인 미만 기업에는 적용이 힘들 것으로 전문가들은 판단하였으나 다음 3개 항목에 대해서는 정보보호 컨설턴트와 정책담당자 모두 기업 규모와 상관없이 중요성이 높아 이행하여야 할 것으로 보았다.

- 연간 교육계획 수립 및 1회 이상의 교육 실시
- 정보시스템 취약점에 대한 분석 및 점검
- 침해사고 및 개인정보 유출사고에 대한 예방·대응 체계 마련

인터뷰 결과, 정보보호 관리체계 컨설팅 항목들이 ISMS-P 항목을 기반으로 하고 있으나 중소기업의 현실과 특성을 반영하지 않아 이행 수준이 낮게 나올 수밖에 없는 항목이 다수 존재하였으며 세부 컨설팅 항목이 명확하지 않아 중소기업 담당자와 컨설턴트(점검자)의 혼란을 가져올 수 있는 항목도 있었다. 특히 기술적 보안조치와 관련된 부분들은 컨설팅 이후에도 정보보호 담당자의 이해도가 떨어져 있었으며 그럼에도 불구하고 관련 솔루션의 도입 여부가 보안 수준의 향상 정도로 평가 되는 것은 문제로 지적되었다. 정보보호 전문가들은 예산이 수반되어야 하는 솔루션의 도입여부를 정보보호 활동의 이행여부로 판단하기보다 대응 절차와 관리 방안 등 항목에 적합한 여러 대안으로 평가하는 것이 적합할 것으로 보았다.

정보보호 관리체계 컨설팅 세부 항목 외에, 일부 전문가는 PDCA(Plan-Do-Check-Act) 사이클에 따른 컨설팅 방법론을 제안하였다. 즉, 최초점검 후 이행점검 시 여전히 이행되지 않은 항목에 대해서 왜 이행되지 않았는지 원인을 조사, 분석 하고 다음 점검 시 반영할 수 있도록 체계를 구축하여야 하는 것이다.

세부 항목별 전문가 인터뷰 결과, 정보보호 관리체계 영역의 정보보호 정책의 유지관리 항목(정보보호 정책을 정기적으로 검토하고 제·개정하고 있는가)과 관련하여 3명의 컨설턴트 모두 중소기업에서 현실적으로 이행하기 어려운 것으로 판단하였다. 정형화된 양식(정보보보 정책)을 제공하여 제정한 이후에는 환경의 중대한 변경 등이 발생하지 않을 경우 개정에 대한 필요성이 높지 않을 것으로 보았으며 유지관리 여부를 묻기 보다는 기업 유형별(제조, IT 등), 규모별 핵심적인 사항들을 포함한 표준 정보보호 정책을 배포하고 정기적으로 업데이트한 내용을 배포하는 식으로 유지하는 것이 적합하다고 의견을 제시하였다. 반면 정책 담당자의 경우 3명 모두 이행되어야 할 사항으로 보았으며 유지관리 활동이 미흡한 것은 컨설팅 전, 후의 점검 시점이 너무 짧았거나, 관련활동에 대한 최고 경영진의 의지와 전파가 부족한 것으로 보았다. 또한 기업의 반기별 성과 점검 회의 또는 연말 사업계획 검토회의 시 해당 항목 관련내용을 포함하여 이행을 할 수 있도록 하는 방법, 중소기업용 표준정책을 전문기관에서 마련하여 제공하고 개정주기를 여건에 맞게 조정하는 등의 대안을 제안하였다.

정보자산에 대해 중요도와 보안등급을 부여하고 있는지를 묻는 항목에 대해서도 정보보호 컨설턴트 3명 모두 중소기업에서 완벽하게 이행하는데 어려움이 있을 것으로 판단하였다. 자산에 대한 중요도를 결정하고 보안등급을 부여하는 활동 자체가 전문성을 요하는 작업으로 판단되며, 표면적으로 그렇게 관리가 된다고 해서 중소기업의 입장에서 실효성이 있지 않을 것으로 보았다. 50인 이상 규모의 기업에만 적용하여야 한다는 의견이 있었으며, 컨설팅 대

상 중소기업에서 반드시 보호해야할 필요가 있는 자산에 대해서만 식별하여 관리하도록 하는 것이 관리 부담이 줄고 정보보호 활동의 목적이 명확해지는 등 효과적이라는 의견도 있었다. 정책 담당자의 경우 3명 모두 해당 항목의 취지에 대해서는 필요성이 있을 것으로 보았으나, 일부 관계자는 기준을 간소화하여야 할 것으로 판단하였다. 중소기업의 입장에서 다소 생소한 업무라고 하더라도 정보자산별 중요도를 결정하고, 보안위협에 따라 가용성/기밀성/무결성 중 어떤 부분에 영향을 미치는지 식별하는 것이 필요하다고 보는 의견이 있었으며, 이는 정보자산에 대한 해킹 등 보안 위협에 대한 대책을 마련하기 위한 기본 준비단계로 중소기업에서 이행하여야 할 것으로 판단하였다. 일부 관계자는 자산의 구입 시 및 점검 시 위험 분석 항목을 추가하는 정도로 간소화하여 진행하는 방법을 제시하였다.

주기적 · 상시적으로 수행하여야 할 정보보호 활동을 식별하는 활동과 정보보호 관리체계 운영에 대한 점검, 점검 결과 문제점에 대한 개선조치 등의 항목에 대해 정보보호 전문가 모두 중소기업에서 준수하기 어려운 항목으로 보았다. ISMS-P 인증 기준에 적합한 항목이라는 의견이 있었으며 보안 전담조직이나 전문성을 갖춘 전담인력이 확보되어야 이행될 수 있는 항목으로 보았다. 특히 주기적 보안 점검을 위한 정보보호 인프라 투자는 소기업에서 더욱 이루어지기 힘들 것으로 평가하였으며 정보보호 분야의 관심도를 측정하기 위해서는 별도 지표의 개발이 필요함을 제시하였다. 정책 담당자의 경우 의견이 나뉘었다. 2명은 현실적으로 중소기업에서 이행하기 어려운 항목으로 보았으나, 정보보호 운영현황이 주기적으로 관리되어야 할 것으로 보는 의견도 있었다. 관리체계 점검과 개선에 있어서 필요성은 인정되나 기업 환경에 맞는 수행방안이 필요하며, 우선순위에 따른 이행이 필요하다는 의견을 제시하였다.

인원보안 영역의 연간 정보보호 교육계획 수립과 계획에 따른 연 1회 이상 교육의 실시 여부를 묻는 항목에 대해 정보보호 전문가 모두 중소기업에서 준수하여야 할 사항으로 보았다. 다만, 중소기업 스스로 교육 콘텐츠를 만들고 교육을 수행하는 것이 쉽지 않을 것으로 보아 정부에서 다양한 콘텐츠(산업군별, 규모별)를 개발하고 지원하여야 할 필요성이 있음을 지적하였다. 또한 개인정보보호법 교육과 같이 온라인으로 교육을 운영하여 중소기업에서 접근성을 높이고 교육 참여율을 높이는 방안을 제시하였다. 정책 담당자들 또한 교육의 필요성을 인정하였다. 중소기업에게 현실적으로 가장 유효한 수단으로 보았으며, 정보보호 컨설턴트의 의견과 마찬가지로 전문기관의 온라인 교육 및 VOD 콘텐츠 등의 지원이 효과적일 것으로 보았다. 재직자 50인 미만의 규모가 작은 중소기업에서는 연간 정보보호 교육 계획의 수립이 부담이 될 것으로 보는 의견도 있어, 별도의 계획보다는 기타 교육 일정에 연 1회 이상의 정보보호 교육을 반영할 수 있도록 유도하고 점검하는 방식의 대안이 제시되었다.

네트워크 이상행위 분석 및 모니터링 활동의 수행 여부를 묻는 항목에 대해서는 컨설턴트의 의견이 나뉘었다. 기본적으로는 정보보호에 투자가 많지 않은 중소기업에서 준수하기 어려운 항목으로 보았으나 운영 서버가 있는 경우에만 적용하여야 한다는 의견이 있었으며, 보안 시스템 또는 보안 서비스를 받고 있는지의 여부만 확인하는 것이 바람직하다는 의견도 있었다. 전자의 경우 기업 내부에 PC만 존재할 경우에는 방화벽 또는 IPS 등과 같은 장비의 필요성이 높지 않을 것으로 판단하였다. 그 외에도 평가항목의 제목은 '네트워크 이상행위 분석 및 모니터링' 임에도 불구하고 실제 컨설팅 시 평가 기준은 방화벽 등의 장비 운용 여부를 묻고 있어 컨설팅 항목에 대한 혼동이 있을 수 있음을 지적하였다. 정책 담당자 역시 해당 항목이 단기간에 개선되거나 중소기업이 자체적인 활동을 하기에 어려울 것으로 보았으며 보안관제서비스를 가입하는 것이 더 효과적일 것으로 보는 의견도 있었다. 그 외에 네트워크 이상행위 분석 및 모니터링 '활동' 보다는 활동을 위한 '대책을 검토하고 수행'하고 있는지 여부를 묻는 내용으로의 평가기준 보완이 필요하다는 의견이 제시되었다.

정보시스템 세션 타임아웃 설정을 묻는 항목과 관련하여서 컨설턴트 모두 중소기업에서 준수해야할 필요성이 낮은 것으로 보았다. 기술적 취약점 점검 항목으로 다른 정보보호 관리체계 점검 항목과 성격이 맞지 않다는 의견이 있었다. 또한 일반적인 정보보호 수준을 제고하는 지표로 활용하기에는 적절하지 않으며 개인정보보호처리시스템에서의 준수 여부(법적 준수사항)만 묻는 것이 바람직할 것으로 판단하였다. 정책 담당자 역시 항목의 준수 필요성이 낮은 것으로 판단하였으며 PC 등의 단말기에서 화면보호기 기능의 활용을 유도하는 것이 대안이 될 것으로 평가하였다.

사용자 PC 단말에서의 정보유출 차단을 위한 대책마련 항목에 대해서 컨설턴트와 정책 담당자 모두 점검 세부항목이 모호하거나 다른 점검항목과 중첩되는 부분이 있어 컨설팅 항목에서 제외하거나 정비하여야 할 필요가 있을 것으로 판단하였다. 네트워크 이상행위 분석, 모니터링 항목 및 내부자료 유출방지 항목 등과 중첩되는 부분이 있으며 특히 점검 세부내용의 깊이가 모호하고 어느 정도의 보안 대책을 수립하여야 하는지에 대한 명확한 기준이 없어 중소기업 입장에서 혼란이 발생할 수 있음을 지적하였다. 일부 정책 담당자의 경우 부담스러운 수준의 전문적인 기술용어를 사용하지 않고, 중소기업 수준에서 이해하고 투자할 수 있는 대상을 고려한다면 포함될 수 있을 것으로 보았다.

내부자료 유출방지를 위한 대책 마련의 항목에서 정보보호 전문가 모두 중소기업이 이행하기에 무리가 있다고 판단하였다. 해당 항목의 준수를 위하여 DRM 솔루션을 도입하여야 하는데 중소기업의 경우 예산의 한계와 조직문화 및 업무효율성 저하 등의 이유로 도입이 힘들 것이며 적용을 하더라도 관리가 잘 되지 않을 것으로 보았다. 또한 DRM 솔루션의 적용 여부는 내부정보의 중요성과 기업의 특성에 따라 결정되어야 할 것으로 판단하였다. 정책 담당자의 경우 의견이 나뉘었는데, 기업의 입장에서 가장 중요한 정보에 대한 대책이기 때문에 기술적, 관리적 대책의 마련이 필요하다는 의견이 제시되었다.

보조저장매체의 제한과 관련하여 일부 전문가는 개인정보 처리여부, 중요정보 보호 여부 등에 따라 필요하며, 중소기업의 입장에서도 최소한의 대책마련은 필요한 것으로 보았다. 반면 산업기밀 유출 등의 위험이 없는 일반적인 중소기업에서 매체제어는 이루어지기 쉽지 않으며 필요시 윈도우 레지스트리 변경, 보안 씰 등의 비용이 들지 않는 방법 등으로 가이드를 하여야 한다는 의견도 있었다. 정책 담당자의 경우 가장 손쉬운 기술적 보안대책으로 판단하여 외장하드의 사용 금지, 보안USB 사용 의무화 등의 조치로서 적용이 가능할 것으로 보았다. 그 외에 보조저장매체 관리에 대한 인식제고 노력이 병행되어야 할 것을 주장하였다.

알려진 취약점 분석 및 점검여부를 묻는 항목에서 정보보호 전문가 모두 중소기업에서 이행하여야 할 필요성이 있을 것으로 보았다. 알려진 취약점이 조치되지 않을 경우 보안 사고의 가능성이 매우 높을 것으로 판단하였으며 정부 및 관련 기관에서 솔루션 도입비용과 무상 서비스 등으로 중소기업에 지속적 지원이 필요할 것으로 입을 모았다. 정책 담당자의 경우 항목의 필요성은 모두 인정하였으나 예산확보 및 인력 운용의 문제로 인해 중소기업에서 이행하기에 어려움이 있을 것으로 보는 의견도 있었다. 이에 따라 평가기준을 정기적인 분석 및 조치 활동보다는 보호대책을 마련하고 있는지를 확인하는 여부로 보완하는 방안이 제시되었다.

정보보호 컨설턴트와 정책 담당자 모두 침해사고 및 개인정보 유출사고에 대한 예방·대응 체계, 절차가 반드시 중소기업에 마련되어 있어야 할 것으로 보았다. 중소기업이 스스로 절차를 만들고 숙지하기 쉽지 않으므로 컨설팅 등을 통해 사고대응 절차를 만들어주고, 업데이트 필요 시 지원하는 식의 지원이 필요하다고 판단하였다. 또한 체크리스트 점검 하는 방식의 컨설팅 보다 실질적인 개선과 인식 수준을 높이기 위한 지원이 필요함을 지적하였다. 대응체계 및 절차서 템플릿을 제공하는 방식도 제시되었다.

중소기업의 현실에 맞지 않고 필요성이 낮은 항목은 제거, 대체 하는 등 경량화 하여 정보보호 관리체

계 컨설팅 항목을 구성하여야 할 것이며 공통사항, 규모별 이행사항, 업종별 이행사항 등으로 구분하여 컨설팅 체계를 구성하는 것이 필요함에 전문가들은 의견을 모았다.

6. 결 론

중소기업은 인력과 예산의 측면에서 한계를 가지고 있어 자체적 정보보호 활동에 어려움을 겪고 있다. 정부에서는 지자체와 협력하여 경영여건이 어려운 중소기업을 대상으로 정보보호 컨설팅을 지속 지원하고 있으나 중소기업의 입장에서 다소 현실에 맞지 않거나 실효성이 떨어지는 등 개선이 필요하다.

한국인터넷진흥원으로부터 정보공개 요청을 통해 받은 정보보호 관리체계 컨설팅 결과를 분석하였을 때 컨설팅 전, 후 모든 시점에서 중소기업의 이행이 저조한 항목이 다수 있었으며, 특정 항목의 경우 이행하지 않았던 기업들 모두가 컨설팅 이후에도 개선이 되지 않았다. 또한 일부 기업의 경우 미흡했던 항목들에 대해 컨설팅 이후에도 전혀 개선이 되지 않는 등 중소기업 여건상 현실적으로 이행하기 어려운 항목이 다수 있었음을 확인하였으며 컨설팅 방법론과 지원체계에 대한 개선이 필요함을 알 수 있었다.

본 연구에서는 정부에서 중소기업을 대상으로 추진한 정보보호 관리체계 컨설팅 항목에 대하여 실제로 컨설팅을 받은 중소기업 담당자와 정보보호 전문

〈표 7〉 연구대상 항목별 정보보호 전문가 의견

점검항목	중소기업 적용여부						재직자 50인 미만 중소기업 적용여부					
	C1	C2	C3	S1	S2	S3	C1	C2	C3	S1	S2	S3
정보보호 정책의 정기적 검토	×	×	×	○	△	△	×	×	×	○	△	△
식별된 정보자산에 대한 중요도 및 보안등급 부여	△	△	○	○	△	△	△	×	×	○	△	△
주기적·상시적으로 수행하여야 할 정보보호 활동의 식별	×	×	×	○	△	×	×	×	×	○	△	×
정보보호 관리체계 점검 및 경영진 보고	×	×	×	△	×	△	×	×	×	△	×	△
정보보호 관리체계 점검 시 발견된 문제점에 대한 개선조치 이행	×	×	×	△	×	×	×	×	×	△	×	×
연간 정보보호 교육계획을 수립 및 연 1회 이상 교육 실시	○	○	△	○	○	○	○	○	△	△	○	○
네트워크 이상행위 분석 및 모니터링 수행	△	×	△	△	△	△	△	×	△	△	△	△
정보시스템 세션 타임아웃을 적용	×	×	×	×	△	×	×	×	×	×	×	×
사용자 PC 단말에서의 네트워크를 통한 정보유출 대책 마련	×	×	×	×	△	×	×	×	×	×	△	×
내부자료 유출방지를 위한 대책 마련	×	△	×	×	○	△	×	△	×	×	△	△
보조저장매체를 통한 정보유출 방지를 위한 대책 마련	○	×	×	△	○	△	○	×	×	△	△	△
정보시스템의 알려진 취약점에 대한 정기적 분석 및 점검 수행	○	○	△	△	○	△	○	○	△	△	△	△
침해사고 및 개인정보 유출사고에 대한 예방·대응 체계와 절차 마련	○	△	△	○	○	○	○	△	△	○	○	○

C1 : 정보보호 컨설턴트 1
C2 : 정보보호 컨설턴트 2
C3 : 정보보호 컨설턴트 3
S1 : 정책 담당자 1
S2 : 정책 담당자 2
S3 : 정책 담당자 3

- ○ : 중소기업이 이행하여야 함
- △ : 필요성은 인정되나 기준을 완화하거나 내용을 대체하여 이행
- × : 필요성이 낮거나 중소기업에서 이행할 수 없음

가, 정책담당자 등 다양한 이해관계자의 인터뷰를 통해 문제점을 분석하고 다음과 같이 개선사항을 도출하였다.

첫째, 중요도의 우선순위가 높은 항목별로 양식 및 템플릿, 가이드라인을 제공하고 대책을 교육하는 등 세부적 지원을 하여 실질적인 중소기업의 보안 수준이 높아지도록 하여야 한다. 실제로 컨설팅을 받은 중소기업을 대상으로 인터뷰를 진행했음에도 불구하고 컨설팅 시 낮은 등급을 받은 항목들에 대해 여전히 낮은 이해도와 인식을 보이고 있는 경우가 있었다. 이는 중소기업의 전체적인 보안 수준을 고려하지 않고 각 컨설팅 항목의 이행 여부만을 확인하는 방법론의 문제로 분석된다. 정보보호 전문가 역시 체크리스트 기반의 점검과 시스템 구축 여부를 확인하는 것이 실제로 중소기업의 정보보호 수준에 큰 도움에 되지 않음을 지적하였다.

둘째, 중소기업 대상 실효성 있는 컨설팅 지원을 위해서는 중소기업의 현실을 반영한 컨설팅 항목과 방법론의 개발이 필수적이다. 중소기업의 경우 해킹 또는 랜섬웨어 등 침해사고를 경험한 뒤 문제의식을 가지는 경우가 많으며 보통의 경우 경영진과 직원의 정보보호에 대한 인식은 낮음을 알 수 있었다. 중소기업의 여건상 정보보호를 전담하여 담당하는 인력은 극소수였으며 대다수의 경우 다양한 업무를 겸직하고 그 우선순위에서 정보보호는 후순위가 되었다.

셋째, 효과적인 정보보호 활동을 위해서는 경영진과 전사적 차원의 보안에 대한 인식이 전제되어야만 한다. 이러한 측면에서 공유 형태의 CISO 또는 정보보호담당자를 지원(정기적으로 현장을 방문하여 점검, 정책 개정, 이슈에 대한 해결방안 제시, 자문 등)하는 등의 방법이 대안이 될 수 있을 것이다.

넷째, 컨설팅 지원을 받는 중소기업의 숫자도 중요하겠지만 그 효과와 질적 측면에서의 고려가 필요하다. 컨설턴트 역시 (목표치를 달성하기 위한) 시간과 인력의 한계로 깊이 있는 컨설팅에 어려움이 있었을 것으로 보여 지며, 어느 정도의 시간 간격을 둔 지속적 지원과 중소기업 정보보호 수준 단계별 지원을 통해 중소기업이 스스로 개선하고, 정보보호 역량이 내재화 되도록 유도할 필요가 있다.

본 연구 결과를 바탕으로 중소기업이 현실적으로 이행할 수 없거나, 필요성과 중요성이 떨어지는 정보보호 관리체계 항목은 삭제되거나 대체되어야 할 것이며 특히 중소기업의 특성(업종, 개인정보보호 보유 여부, 내부정보의 중요성 등)에 따라 항목들을 재구조화하고 다르게 적용하여 효과적인 평가 모델을 구성하여야 할 것이다.

본 연구에서는 실제 컨설팅 결과를 바탕으로 중소기업 관계자 4명과 정보보호 컨설턴트 3명, 정책담당자 3명의 인터뷰를 통해 현장의 목소리와 주관적 의견을 반영하여 결론을 도출, 실증적인 연구를 구성하였지만 다양한 중소기업에 바로 적용하고 일반화하기에는 표본이 적어 어려움이 있다. 이에 향후 연구에서는 다수의 중소기업을 대상으로 개선된 정보보호 관리체계 평가 모델을 배포, 이행 가능 여부와 효과성 등에 대한 검증이 필요하다.

또한 중소기업을 재직자 50인 이상과 미만의 기준으로 분류하여 그 특성에 대한 전문가의 의견을 물었으나 중소기업은 재직자수에 의한 규모 이외에도 다양한 특성에 따라 요구되는 정보보호 분야와 수준이 달라질 것이다. 예를 들어 제조업의 경우 인원수는 많으나 PC 등의 정보자원은 적을 수 있으며, 이 외에도 개인정보 보유 규모나 자체 서버의 보유량에 따라 다양한 정보보호 요구가 존재할 수 있다. 따라서 대표적인 산업 군별 특성에 따라 특화된 정보보호 관리체계 평가모델에 대한 연구가 필요할 것이다.

더불어 중소기업의 정보보호 관리 수준을 제고하는 것에 대하여 컨설팅 세부 항목만이 문제는 아닐 것이다. 컨설팅 방법론과 컨설턴트의 역량 등이 중소기업 정보보호 수준 개선에 큰 영향을 미칠 것이며 이를 위해서는 중소기업 현실을 반영하고 실효성 있는 컨설팅 방법론과 컨설턴트의 필요역량에 대한 새로운 정의가 필수적이다.

참고문헌

곽재연, “중소기업의 정보보호 활동을 위한 지원정책

의 방향성 연구", 한양대학교 대학원 석사학위 논문, 2019.

권장기, 김경일, "자원 제약하의 중소기업 정보보안계획 수립방안 연구", *융합정보논문지*, 제17권, 제2호, 2017, 119-12.

김신석, 유혜정, "중소기업의 개인정보 기술적 보호조치 방안 연구", *한국정보기술학회논문지*, 제18권, 제1호, 2020, 157-169.

김양훈, 장항배, "적정 수준의 중소기업 정보보호 추진 방향", *정보보호학회지*, 제23권, 제4호, 2013, 41-46.

김재남, "중소기업 컨설팅 사례기반 정보보호 효과와 개선방안", *한국컴퓨터정보학회눈문지*, 제21권, 제11호, 2019, 201-208

김정덕, 장항배, 류성렬, "중소기업 정보보호 특성을 고려한 정보보호 관리체계 연구", *중소기업연구*, 제41권, 제4호, 2006, 267-294.

노민선, 이삼열, "중소기업의 산업보안 역량에 대한 영향요인 평가", *한국행정학보*, 제44권 제3호, 2010, 239-259.

박경태, 김세헌, "탐색적 요인 분석을 이용한 기업의 ISMS 인증 시 장애요인에 관한 연구", *정보보호학회눈문지*, 제24권, 제5호, 2014, 951-959.

서동호, 신현민, "기업규모와 특성에 따른 정보보호 관리체계(ISMS) 적용 방안 연구", *한국정보처리학회 학술대회논문집*, 제24권, 제1호, 2017, 227-229.

연합뉴스, "해킹 피해 98%는 중소기업...지역단위 지원체계 필요", 2018. Available at https://www.yna.co.kr/view/AKR20180510147800017?input=1195m (Accessed October 19. 2021).

이정우, 박준기, 이준기, "중소기업 정보보호관리 모델의 개발: 실증연구", *경영정보학연구*, 제15권, 제1호, 2005, 115-133.

이효경, "중소기업 정보보호 지원 관련 법제 현황 및 개선방향", *경제법연구*, 제18권, 제3호, 2019, 73-101.

장상수, "중소기업 정보보호 컨설팅 개선을 위한 방법론 비교 분석", *융합정보논문지*, 제10권, 제8호, 2020, 1-6.

장상수, "국내 중소기업 정보보호 지원 정책 개선 방안에 관한 연구", *융합정보논문지*, 제10권, 제11호, 2020, 332-339.

장항배, "중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계", *멀티미디어학회논문지*, 제13권, 제1호, 2010, 111-121.

한국인터넷진흥원, "정보보호 및 개인정보보호 관리체계 인증제도 안내서", 2021.

한국정보보호산업협회, "2020년 정보보호 실태조사", 2021.

Antunes, M., M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal", *Journal of Cybersecurity and Privacy*, Vol.1, No.2, 2021, 219-238.

Barlette, Y. and V.V. Fomin, "The Adoption of Information Security Management Standards: A Literature Review", *Information Resources Management*, Vol.1, No.4, 2010, 69-90.

Benz, M. and D. Chatterjee, "Calculated Risk? A cybersecurity evaluation tool for SMEs", *Business Horizons*, Vol.63, No.4, 2020, 531-540.

Cholez, H. and F. Girard, "Maturity assessment and process improvement for information security management in small and medium enterprises", *Journal of Software: Evolution and Process*, Vol.26, No.5, 2013, 496-503.

Groner, R. and P. Brune, "Towards an Empirical Examination of IT Security Infrastructures in SME", *Secure IT Systems. NordSec 2012. Lecture Notes in Computer Science*, Vol.7617, 2012, 73-88.

Javaid, M.I. and M.M.W. Iqbal, "A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium

enterprises (SME)", *2017 International Conference on Communication Technologies (ComTech)*, 2017, 78-90

Ključnikov, A., L. Mura, and D. Sklenár, "Information security management in SMEs: factors of success", *Entrepreneurship and Sustainability Issues*, Vol.6, No.4, 2019, 2081-2094.

Kurpjuhn, T., "The SME security challenge", *Computer Fraud & Security*, Vol.2015, No.3, 2015, 5-7.

Mijnhardt, F., Baars, T. and Spruit M., "Organizational Characteristics Influencing SME Information Security Maturity", *Journal of Computer Information Systems*, Vol.156, No.2, 2016, 106-115.

Osborn, E., "Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs", *Terms and Conditions of Use for Oxford University Research Archive*, 2015, 1-20.

Ozkan, B.Y. and M. Spruit, "Addressing SME Characteristics for Designing Information Security Maturity Models. Human Aspects of Information Security and Assurance", *HAISA 2021. IFIP Advances in Information and Communication Technology*, Vol.593, 2020, 161-174.

Ozkan, B.Y. and M. Spruit, "Cybersecurity Standardisation for SMEs: The Stakeholder's Perspectives and Research Agenda", *International Journal of Standardization*, Vol.17, No.2, 2019, 1-25.

Paul, S., "Reinforcing your SME against cyber-threats", *Computer Fraud & Security*, Vol.2017, No.10, 2017, 13-15.

Rae, A. and A. Patel, "Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K.", *Information Security Practice and Experience, Lecture Notes in Computer Science*, Vol.11879, 2019, 362-380.

Saban, K.A., S. Rau, and C.A. Wood, "SME executives' perceptions and the information security preparedness model", *Information and Computer Security*, Vol.29, No.1, 2021

Tawileh, A., J. Hilton, and S. McIntosh, "Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach", *ISSE/SECURE 2007 Securing Electronic Business Processes*, 2007, 331-339.

Valdevit, T., N. Mayer, and B. Barafort, "Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings. EuroSPI 2009: Software Process Improvement", *Communications in Computer and Information Science*, Vol.42, 2009, 201-212.

Yildirim, E.Y., G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey", *International Journal of Information Management*, Vol.31, No.4, 2011, 360-365.

About the Authors

김 이 헌 (heonup@naver.com)

충북대학교 융합보안전공 공학 석사학위를 취득하였다. 충북과학기술혁신원에서 지역 중소기업의 정보보호 역량 강화를 위한 컨설팅 등 지원 업무를 하고 있으며, 주요 관심분야는 정보보호 정책 및 인력, 보안 인프라, 개인정보 보호이다.

김 태 성 (kimts@cbnu.ac.kr)

KAIST 산업경영학과에서 박사를 취득하고, 한국전자통신연구원에서 선임연구원으로 근무한 후, 현재 충북대학교 경영정보학과에서 정교수, 보안경제연구소장, 보안컨설팅연계전공 및 대학원 융합보안전공 주임교수로 재직하고 있다. 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, 병무청 정책자문위원, 한국전력 정보보안 자문위원, 한국지역정보개발원 선임이사, ISMS-P 인증위원회 위원으로 활동하고 있으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.