Journal of Convergence for Information Technology
Vol. 10. No. 8, pp. 1-6, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.08.001

중소기업 정보보호 컨설팅 개선을 위한 방법론 비교 분석

장상수
한국인터넷진흥원 연구위원

Comparative Analysis of Methodology for Improving Information Security Consulting for SMEs in Korea

Sang-Soo Jang
Researcher, Korea Internet & Security Agency

요 약 정부는 중소기업 정보보호 활동의 어려움을 해결하고자 정보보호 컨설팅 지원 사업을 수행하고 있으나, 중소기업에 적용하는 정보보호 컨설팅 방법론이 주요정보통신기반시설(CIIP), ISMS, ISO27001 등과 같은 검증된 방법론을 적용하지 않고 컨설팅 수행업체별 다양한 방법을 적용하다 보니 중소기업 형태, 규모 등 조직 상황에 따라 적절한 대응이 어렵다는 것이다. 이러한 중소기업 정보보호 컨설팅의 문제점을 개선하고 보다 효과적이고 실효적이며 표준적인 방법론을 개선하기 위하여 현행 제도에서 적용하고 있는 정보보호 컨설팅 방법론을 비교 분석하여 중소기업에 적합한 정보보호 체계를 구축하는 정보보호 컨설팅이 될 수 있도록 하고자 하였다. 본 연구에서 제시한 중소기업 정보보호 컨설팅 방법 개선 방안을 통해 중소기업 규모나 사업 형태에 상관없이 모든 기업에 적합한 정보보호 컨설팅이 가능하여 컨설팅 품질 제고에 이바지하고 중소기업이 정보보호 활동에 만족하고 지속해서 이행되기를 기대한다.

주제어 : 주요정보통신기반시설(CIIP), ISMS, ISO27001, 컨설팅, 정보보호 체계, 보안 위협, 방법론

Abstract The government is carrying out information security consulting support projects to solve the difficulties of SME information protection activities. Since the information security consulting methodology applied to SMEs does not apply the proven methodology such as the critical information and communication infrastructure(CIIP), ISMS, ISO27001, etc. It applies various methods for each consulting provider. It is difficult to respond appropriately depending on the organizational situation such as the type and size of SMEs. In order to improve such problems of SME information security consulting and to improve more effective, effective and standard methodology, the information security consulting methodology applied in the current system was compared and analyzed. Through the improvement plan for SME information security consulting method suggested in this study, it is possible to provide information security consulting suitable for all enterprises regardless of SME size or business type.

Key Words : Critical Information Infrastructures Protection, ISMS, ISO27001, Consulting, Information Security System, Security Threats, Methodology

1. 서론

국내 정보보호 컨설팅은 2001년 금융·통신·에너지 등 정보통신기반 시설을 보호를 시작으로「정보통신기반 보호법」「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 일정 규모 이상의 정보통신서비스제공자는 취약점 분석·평가를 주기적으로 받도록 의무화되었다. 법적 제도적 의무 대상자를 보안컨설팅을 해왔지만, 사각지대에 놓여 있던 중소기업에 대해서는 제도적

*Corresponding Author : Sang-Soo Jang(ssjang0116@gmail.com)
Received March 24, 2020
Revised August 3, 2020
Accepted August 20, 2020
Published August 28, 2020

관리 대상 주체가 아니므로 자율적으로 보호조치를 요구해왔다[1,2]. 때문에, 예산 및 인력 등 경영여건이 어려운 중소기업은 스스로 정보보호 활동에 한계가 있었다. 이에 2014년 이후로 정부는 본격적으로 중소기업에 대한 정보보호 컨설팅을 지원해오고 있다.

중소기업에 대한 맞춤형 표준적 정보보호 컨설팅 방법론이 없어 컨설팅 업체의 방법론에 의존하다 보니 다수의 컨설팅 업체가 컨설팅을 수행하거나 매년 다른 업체일 경우 정보보호 수준을 측정하기 어렵고 컨설팅 품질 자체의 격차가 있는 것이 사실이다. 이는 보안컨설팅의 타당성, 실효성이나 효과성 면에서 문제 발생 원인이 되고 있다.

본 연구에서는 중소기업 정보보호 컨설팅 서비스의 효율적인 방법을 제시함으로써, 중소기업이 받게 되는 컨설팅 서비스의 수준을 향상하는데 필요한 정보를 제공함으로써, 향후 중소기업 정보보호 컨설팅 지원 사업의 만족도를 향상하는 방안을 수립하는데 기반이 될 것이다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서 정보보호 컨설팅 선행 연구를 검토한다. 3장은 중소기업 정보보호 컨설팅 사례를 비교 분석한다. 4장에서 개선 방안을 제시하고 5장에서 결론으로 마친다.

2. 선행 연구

안혜연(2001)은 “정보보호 컨설팅 방법론과 적용” 연구에서 보안컨설팅 단계를 현상분석, 위험관리, 보안모델링, 보안관리의 네 단계로 수행된다는 것을 제시하였다. 정보보호 컨설팅 서비스 유형을 취약점 진단 서비스, 애플리케이션 보안 모듈 설계, 전자상거래 보안, 취약점 분석 및 안전한 인트라넷 설계, 통합 보안 모듈 구축 등의 다섯 가지로 구분하였다[1].

박순태 외 2명(2009)은 “주요정보통신기반시설 보호를 위한 취약점 분석·평가 관리 방안”연구에서 취약점 분석·평가 컨설팅 수행 시 기반시설 및 정보보호 조직의 규모에 따른 맞춤형 취약점 분석·평가 적절성 검토 프로세스를 적용할 수 있도록 하였다. 점검항목 또한 시설 및 조직의 규모에 따라 유형별로 분류하여 적용할 수 있도록 하였다[2].

취약점 분석·평가 품질검토를 위해 품질검토 계획작성, 검토 수행, 보고, 사후조치 등 4개 프로세스를 제시하였다. 또한, 취약점 분석·평가 절차로는 환경 및 요구사항분석, 취약점 분석 및 위험평가, 체계설계 및 계획수립, 프로젝트 관리, 교육, 기술이전 및 사후관리 등 5개 프로세스를 제시하였다[2].

김태성 외 4인(2019)은 “중소기업 정보보호 성과측정 모델 및 방법 개발”에서 국내 중소기업 정보보호 컨설팅 지원 사업에서 기본 컨설팅의 경우 원격점검, 현장 컨설팅 2단계로 수행하고 종합컨설팅의 경우, 사전분석, 원격점검, 현장 컨설팅, 이행점검 등 4단계로 구분하여 수행하고 있다. 다만, 컨설팅 성과에 대한 측정지표가 없어 사업 연속성 등에 문제가 있어 성과측정 지표를 제시하였다[3].

홍성욱 외 1인(2020)은 “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도의 효과적인 운영방안” 연구에서 인증대상 기관별 인증기준 적용의 모호성을 제기하였다. 성격과 규모가 다른 인증대상 기관(공공기관, 대기업, 정보통신서비스제공자, 중소기업, 병원, 학교 등)의 같은 결함 사항에 대해 같은 인증기준으로 결함을 받도록 하는 것이 공정하지 않은 경우가 발생하게 되면서 같은 인증기준을 모든 인증 대상기관에 적용하는 것이 맞는 것인지에 대한 인증기준 적용대상의 모호성이 발생하게 된다는 것을 제기하였다[4].

개선 방안으로 인증 대상기관의 유형을 구분하고 유형에 따라 인증심사 시 적용하는 통제 항목이나 세부 점검항목을 다르게 적용함으로써 인증 대상기관별 인증기준적용의 모호성을 개선할 수 있다고 제시하였다[4].

선행 연구를 검토한 결과 규모가 큰 주요정보통신기반시설이나 ISMS 컨설팅은 위험관리가 중요한 프로세스로 들어가 있으나 중소기업 컨설팅에서는 위험관리 부분은 생략되어 있다. 공통적인 절차로는 현황분석, 보호 대책수립 및 이행, 사후관리 부분이 존재하고 있다.

3. 사례 분석 및 비교

정보보호 컨설팅의 법적 정의로는 전자적 침해행위에 대비하기 위한 정보시스템의 취약점 분석·평가와 이에 기초한 보호 대책의 제시 또는 정보보호 관리체계 구축 등을 주된 목적으로 수행한 컨설팅을 말한다[5].

정보보호 전문가가 조직의 잠재적인 정보보호 위험을 파악하고 위험 분석 및 평가를 통해 조직에 최적의 보호 대책을 제시하며 침해사고 예방, 대응, 복구가 가능하도록 지속적인 위험관리와 정보보호 체계를 갖추

도록 하는 서비스라 할 수 있다.

한국정보보호산업협회에서 조사한 “2019 국내 정보보호 산업 실태조사”에 따르면 정보보안 관련 서비스 분류를 보안컨설팅, 보안시스템 유지관리, 보안관제, 보안 교육 및 훈련, 공인/사설 인증서 등 5개로 분류하고 있다.

여기서 다시 보안컨설팅 서비스 종류에는 정보보호 정책수립, 보안점검서비스, 위험 분석 및 평가, 네트워크 보안 아키텍처 설계, 보안솔루션 제안, 보안 교육 등으로 분류하고 있다[6].

3.1 주요정보통신기반시설 취약점 분석·평가 컨설팅

「정보통신기반 보호법」에서는 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행하도록 규정하고 있으며, 주요정보통신기반시설의 지정, 취약점의 분석·평가, 보호 대책의 수립을 하도록 하고 있으며 이러한 업무를 수행할 수 있는 정보보호 전문서비스 기업을 지정하여 수행하도록 하고 있다[7].

컨설팅 서비스 유형의 하나인 취약점 분석·평가는 악성코드 유포, 해킹 등 사이버 위협에 대한 주요정보통신기반시설의 취약점을 종합적으로 분석 및 평가·개선하는 일련의 과정을 의미한다.

주요정보통신기반시설의 안정적 운영을 위협하는 사이버보안 점검항목별 세부 점검항목을 도출하여 취약점 분석을 하며 발견된 취약점에 대한 위험등급 부여, 개선 방향 수립 등의 유기적인 평가를 수행하게 된다.

구체적인 주요정보통신기반시설 수행 절차는 1단계로 취약점 분석·평가 계획수립, 2단계 취약점 분석·평가 대상 선별, 3단계 취약점 분석 수행, 4단계 취약점 평가 수행 단계로 수행하게 된다[7].

3.2 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 구축 컨설팅

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 인증을 받고자 하는 자가 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인증기관이 증명하는 제도를 운용하고 있다. 인증기준에서는 관리체계 수립 및 운영, 보호 대책 요구사항, 개인정보 처리 단계별 요구사항 등 3개의 도메인을 요구하고 있다[8].

국내 정보보호 컨설팅 업체에서는 위험관리 기반의 주요정보통신기반시설 취약점 분석·평가 기준이나 ISMS-P 인증기준에 따르도록 관련 절차에 따라 맞춤형 정보보호 컨설팅을 수행하게 된다. 즉 이러한 취약점 분석·평가나 ISMS-P 인증기준은 정보보호 컨설팅 표준 모델로 활용되며, 현재 정보보호 컨설팅 업체에서는 법에서 정한 기준을 따라야 하므로 규모나 유형에 따라 약간의 차이가 있을 수 있으나 대부분 정보보호 컨설팅 방법론으로 적용하고 있다.

3.3 중소기업 정보보호 컨설팅

국내의 중소기업 정보보호 수준 제고 및 침해사고 예방・대응 역량 강화를 위하여 한국인터넷진흥원에서는 ‘지역 중소기업 정보보호 지원’ 사업을 추진하고 있다. 이는 「지역정보보호지원센터」를 통해 지역의 중소기업에 대한 정보보호 컨설팅 서비스를 제공하고 있다. 여기에서는 지역 중소기업에 대한 정보보호 관리체계, 정보시스템 취약점 점검, 현장 맞춤형 컨설팅, 개인정보보호 등에 대한 정보보호 컨설팅을 수행하고 있다. 그러나 표준적인 기준이나 방법을 정하지 않고 컨설팅의 수행하는 서비스 업체의 역량이나 방법론에 의존하고 있다[9].

한국인터넷진흥원에서 실시한 2018~2019년 중소기업 정보보호 종합컨설팅 사례로 A사(2018)의 경우 컨설팅 수행 방법을 보면 사전준비, 진단준비, 현장진단, 대책수립, 기술지원 등 5단계로 수행한 바 있다. B사(2019) 경우 사전분석, 원격점검, 현장 컨설팅, 이행점검 등 4단계로 컨설팅을 수행하였다. 컨설팅 점검기준 자체도 A사의 경우 점검항목(387개), B사의 경우(219개)로 제각각이며, 실제 대상 기업의 규모나 유형에 맞는 통제 항목으로 적용이 어렵게 되어있다[10,11].

이렇게 중소기업의 규모나 유형을 고려하지 않고 컨설팅 서비스 업체의 방법론에 의존하다 보니 최적화된 컨설팅 수행이 어렵고 매년 진단하는 수행 업체가 다르다 보니 표준적인 정보보호 수준을 측정하는 데 한계가 있다[10,11].

3.4 정보보호 컨설팅 방법론 비교 분석

Table 1에서 주요정보통신기반시설이나 ISMS-P에서는 위험관리 과정을 반드시 하도록 규정하고 있다.

조직의 규모에 상관없이 데이터 중심의 위험관리 기반의 방법으로 보호하고자 하는 정보자산의 중요도에 따라 취약점 분석을 하고 위험평가를 해서 보호 대책을 수립하고 있다. 위험관리 방법론을 적용함으로써 중소기업의 유형이나 규모에 상관없이 자연스럽게 과투자나 실효성 없는 보안컨설팅 수행이 아니라 조직에 적합한 맞춤형 보안컨설팅이 이루어질 수 있다.

이는 정부 기관이든 대기업이든 중소기업이든 조직의 유형이나 규모에 상관없이 위험관리 기반의 방법을 통해 조직에 적합한 정보보호 수준을 정하도록 하고 있다. 그러나 현재 중소기업 정보보호 컨설팅의 경우 컨설팅 방법이 수행 업체마다 다르고 표준적인 모델(프레임워크)을 따르지 않다 보니 현장에서 혼란을 가중하고 있다. 매년 중소기업 정보보호 컨설팅 수행 업체에 따라 정보보호 방법론이 다르고 점검기준이 다르다 보니 중소기업들의 정보보호 수준을 측정하기 어렵고 컨설팅 결과와 보호 대책수립에 일관성이 없고, 보호 대책을 수립하는데 비효율적이고 비효과적인 문제가 발생하고 있다.

Table 1. Information Security Consulting Methodology and Procedure

Methodology and Procedure	CIIP	ISMS-P	SME Consulting	
			A Co. (2018)	B Co. (2019)
Step 1	Risk Management Planning	Environment Implementation	Preparation	Preparation
Step 2	Risk Management	Risk Management	Remote Check	Check Preparation
Step 3	Analysis	ISMS Operation	Site Consulting	Site Check
Step 4	Assessment	Check and Improvement	Performance Check	Countermeasure Recommend
Step 5				Technical Assistance

또한, Table 2는 정보보호 컨설팅을 수행하는 점검항목을 나타낸다. 조직에서 활용하는 통제 항목으로 주요정보통신기반시설(233개), ISMS-P(102개)로 모두 위험관리 과정을 포함하고 있다. 그러나 중소기업 컨설팅 점검항목에는 데이터 기반의 위험관리 과정이 없고 일반적인 통제 항목으로만 구성되어 있어 모든 중소기업에 적용하기에는 한계가 있다. 중소기업의 규모나 업종별 형태에 따라 위험관리 기반이 아닌 체크리스트 기반으로 하면 모든 중소기업에 적용하는데 어려움이 발생하고 있다.

한국인터넷진흥원에서 실시한 2018~2019년 중소기업 정보보호 컨설팅의 경우 위험기반, 데이터 중요도에 따라 통제 항목을 선택하는 방식이 아닌 모두 적용하도록 하는 체크리스트 방식이다 보니 중소기업에 적용하는 통제 항목이 너무 형식적이거나 규모나 유형을 고려하지 않는 통제 항목으로 실효성이 떨어지거나 적용조차 어려운 항목이 대부분인 것으로 확인 되었다[12].

Table 2. Information Security Consulting Check List

Check List	CIIP	ISMS-P	SME Consulting	
			A Co. (2018)	B Co. (2019)
Security Management	46	16	95	63
Technical	159	64	251	115
Web	28		14	14
Privacy	-	22	27	27
Total	233	102	387	219

4. 중소기업 정보보호 컨설팅 방법(모델) 개선 방안

문헌연구와 정보보호 컨설팅 방법에 대한 분석결과 Fig. 1과 같이 컨설팅 단계로 중소기업에서도 규모나 업종 등에 상관없이 모든 조직에 적용 가능한 위험관리 기반의 정보보호 컨설팅 방법을 제시하고자 한다. 통제 항목에서도 위험관리 방법으로 가게 되면 체크리스트 기반(위험 분석 및 평가 없음)의 방법보다 효율적이고 효과적인 무엇을 어떻게 보다는 위험관리에서 정해지는 결과에 따라 보호 대책들은 선택적으로 적용하도록 제시하고자 한다. 이러한 방법은 조직의 규모, 비즈니스 유형, ICT 정도 등에 의존하지 않고 모든 조직에 적용 가능하다는 것이다.

본 논문에서 제시한 개선된 중소기업 정보보호 컨설팅 방법은 우선 정보보호관리 프로세스를 도입하여 1단계 현황분석, 2단계 위험관리, 3단계 보호 대책수립, 4단계 사후관리를 제시하였다. 1단계 현황분석 단계는 사업분석, 범위설정, 현황분석을 제시하였다. 2단계 위험관리 단계는 정보자산을 식별하고 데이터 중요도에 따라 자산을 평가하는 단계이다. 위험 분석 및 평가 단계는 관리적, 물리적, 기술적 위협 및 취약점 분석·평가

단계이다. 취약점 분석이 끝나면 위험평가 단계로 점검 결과에 따라 발견된 취약점별 위협 등급 식별 및 개선 방향 수립을 하게 되며 위험등급은 상·중·하 등으로 구분하여 표시한다. 3단계는 보호 대책수립 단계로 위험평가 결과에 따라 보호 대책과 계획을 수립하고 보호대책을 선정 및 구현, 교육 및 훈련 등 단계이다. 마지막 4단계로 사후관리 단계는 법규준수 검토 및 보완조치, 보호 대책 이력관리, 자체점검 및 수시점검 등 단계이다. 이러한 관리과정은 정보보호 생명주기로 정기적으로 반복시행하게 된다.

제시된 위험관리, 데이터 기반의 컨설팅 방법론은 주요정보통신기반시설이나 ISMS-P에서 검증이 완료된 바 있으며, 이러한 제도를 도입한 지 15년 이상 국내 정보보호 표준 컨설팅 방법론으로 자리매김하고 있다. 다만, 그동안 중소기업의 경우 일률적인 수행업체별 체크리스트 기반의 방법을 적용하다보니 중소기업의 업종이나 규모에 적절한 대응이 어렵고 매년 수준을 측정 비교 하기가 곤란하였다[13].

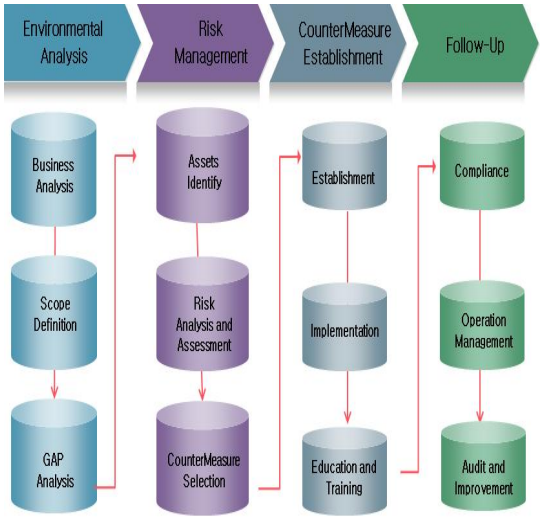

Fig. 1. SME Information Security Consulting Model Improvement(Proposal)

5. 결론

본 연구에서는 그동안 수행해왔던 중소기업에 대한 정보보호 컨설팅 방법에 대해 비교 분석을 통해 개선된 방법을 제시하였다. 그동안 체크리스트 기반의 정보보호 컨설팅에서 위험관리기반, 데이터 기반의 개선된 방법론으로 자산식별, 위험 분석 및 평가, 보호 대책수립이라는 과정을 추가하여 소규모 조직에서부터 대규모 조직, 어떠한 유형의 사업 형태, ICT 도입 여부와 상관없이 적용 가능한 방법을 제시하였다. 따라서 이러한 위험관리 기반, 데이터 중심의 정보보호 컨설팅 방법은 중소기업에 적합한 모델이라 할 수 있다. 제시된 방법론은 절차나 방법에 대한 표준적인 프로세스로 조직 규모에 유연하게 대응할 수 있으므로 컨설팅의 모호성이나 과도한 자원 투입 등을 해결할 수 있는 정보보호 컨설팅 방법에 있어 실효적이고 효과적인 방법을 제시하고 있다.

본 연구에서 제시한 위험관리 기반, 데이터 중심의 중소기업 정보보호 표준 컨설팅 모델은 우리나라의 수많은 소상공인, 영세기업, 중소기업 등에 정보보호 수준 제고를 위하여 매우 효율적인 방법론으로 많은 활용이 기대된다.

REFERENCES

[1] H. Y. Ahn. (2001). *Information Security Consulting Methodology and Application. Korea Institute of Information Security And Cryptology. 11(3),* 49-56.

[2] S. T. Park, W. S. Yi & B. N. Noh. (2009). *SME Vulnerability Analysis and Assessment to Project for Critical Information Infrastructure Protection Management Plan. Korea Institute of Information Security And Cryptology. 19(6),* 32-40.

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

[4] H. Y. Ahn. (2020). Effective Management of Personal Information & Information Security Management System(ISMS-P) Certification. *Korea Academy Industrial Cooperation Society, 21(1),* 634-640.
DOI : 10.5762/KAIS.2020.21.1.634

[5] Ministry of Science and ICT(MSIT), (2017), *Notification on Preliminary Check of Information Security.* Public Notice 2017-7. Sejong.

[6] Korea Information Security Industry Association(KISIA). (2020). *2019 Survey of Information Security Industry in Korea.* Seoul.

[7] Ministry of Science and ICT(MSIT). (2013). Critical *Notification on Information*

Infrastructure Protection Vulnerability Analysis and Assessment Standard. Public Notice 2013-37. Sejong.

[8] Ministry of Science and ICT(MSIT), (2018), *Notification on Certification of Personal and Information Security Management System*. Public Notice 2018-80. Sejong.

[9] https://www.kisa.or.kr

[10] Korea Internet and Security Agency(KISA), (2018), *SME* Information Security Consulting *Support Report. 2018,*

[11] Korea Internet and Security Agency(KISA), (2019), *SME* Information Security Consulting *Support Report. 2019*

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

[13] Korea Internet and Security Agency. (2020). *2019 SME Information Protection Consulting Result Report.* 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, 융합 보안, ISMS
· E-Mail : ssjang0116@gmail.com