JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 24 No. 11, pp. 201-208, November 2019
https://doi.org/10.9708/jksci.2019.24.11.201

The Effectiveness of Information Protection and Improvement Plan Based on SMEs Consulting Case

Jae-Nam Kim*

*Professor, Dept. of Social Welfare, Kwangju Women's University, Gwangju, Korea

[Abstract]

In the phono-sapiens era of the intelligence information society, most business activities are increasingly dependent on networks and information systems. SMEs, which occupy the majority of Korean companies, are increasingly possessing the value and technology of their information assets, and their ability to protect core technologies that are the driving force of corporate growth will be the most important competitiveness of enterprises. Accordingly, the Ministry of Science and ICT and the Korea Internet & Security Agency(KISA) provides a foundation for minimizing the damage from cyber threats such as hacking and information leakage by evaluating the current information protection level of SMEs and enhancing information protection capability by supporting a high level of customized information protection consulting.

In this study, we analyze the effectiveness of information protection based on the results of KISA SMEs consulting. In addition, by identifying problems and limitations derived from SMEs information protection consulting results, SMEs should propose measures to improve information security of SMEs that can manage information protection management system more efficiently and effectively.

▸ **Key words**: Intelligence Information Society, SMEs, Cyber Threat, Information Security Consulting, Information Security Management System

[요 약]

지능정보사회의 포노 사피엔스 시대에 대부분 기업 활동은 네트워크 및 정보시스템에 대한 의존도가 더욱 높아지고 있다. 우리나라 기업의 대부분을 차지하고 있는 중소기업은 보유하고 있는 정보 자산의 가치와 기술력이 점차 증가하고 있고 기업 성장의 원동력이 되는 핵심기술에 대한 보호역량은 기업의 가장 중요한 경쟁력이 될 것이다. 이에 따라 과학기술정보통신부와 한국인터넷진흥원은 높은 수준의 기업 맞춤형 정보보호 컨설팅 지원을 통해 중소기업의 현재 정보보호 수준을 평가하고 정보보호 역량을 제고함으로써 해킹, 정보유출 등 각종 사이버 위협으로부터 받는 피해를 최소화할 수 있는 기반을 제공하고 있다.

본 연구에서는 한국인터넷진흥원에서 수행한 중소기업 정보보호 컨설팅 결과를 기반으로 정보보호 효과를 분석하고 중소기업 정보보호 컨설팅 결과에서 도출된 문제점과 한계점을 파악하여 중소기업이 정보보호 관리체계를 보다 효율적이고 효과적으로 관리할 수 있는 중소기업 정보보호의 개선방안을 제안하도록 한다.

▸ **주제어**: 지능정보사회, 중소기업, 사이버 위협, 정보보호 컨설팅, 정보보호 관리체계

• First Author: Jae-Nam Kim, Corresponding Author: Jae-Nam Kim
*Jae-Nam Kim (jnkim@kwu.ac.kr), Dept. of Social Welfare, Kwangju Women's University
• Received: 2019. 09. 23, Revised: 2019. 10. 06, Accepted: 2019. 10. 06.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

Ⅰ. Introduction

기업에서 증가하고 있는 사이버공격에 의한 정보유출 사고 등은 기업의 경제적 손실 및 경제활동을 저해함은 물론 기업의 경쟁력조차 떨어뜨리는 요인으로 지목되고 있다. 대부분 기업에서는 정보보호 관리체계 인증을 통하여 정보보호를 능동적이고 효과적으로 대응하여 기업의 경쟁력을 유지하고 있다[1]. 현재 우리나라는 개인정보보호 관리체계(PIMS)와 정보보호 관리체계(ISMS)를 중심으로 하여 국가 주도로 정보보호 관리 수준 향상을 위한 활동을 전개하고 있는데 과기정통부, 행정안전부, 방통통신위원회는 PIMS와 ISMS를 통합한 정보보호 및 개인정보보호관리체계 인증 등에 관한 고시(ISMS-P)를 2018. 11.에 개정하여 현재는 통합된 인증제도를 운영하고 있다. 그러나 이러한 제도들은 「정보통신망이용촉진 및 정보보호 등에 관한 법률 제47조」의 기준에 의해 ISP, IDC 및 일정 규모 이상의 기업, 대학, 의료기관을 그 대상으로 두고 있기 때문에 국가 전반에 걸쳐 정보보호 수준의 균형적인 성장을 주도하기에는 한계와 어려움이 있다[2].

특히 국내 전체 사업자수의 99% 이상을 차지하는 중소기업은 정보보호 관리체계 제도 대상 범위에서 벗어나 있고 열악한 환경으로 정보보호 체계 마련을 위한 최소한의 컨설팅과 보안투자 및 사후관리 비용 등의 경제적 부담 때문에 정보보호 관리체계를 구축하여 중요자산을 지키고 보호하고자 하는 동기와 인식을 가지고 추진하는 것은 매우 어려운 실정이다. 이와 같이 보안 인프라가 상대적으로 더 취약한 중소기업에게 실질적인 혜택과 도움을 주기 위한 국가차원의 정보보호 지원제도 운영을 위해서는 국내 중소기업의 기술유출 및 탈취 실태 파악, 실제 피해사례 수집, 중소기업의 기술보호 역량수준에 대한 평가, 중소기업 정보유출 방지사업의 실효성 분석 조사가 정확하게 이루어져야 할 것이다[3].

지금까지 우리나라의 정보보호 활동은 비교적 규모와 보안투자 역량이 있는 중견·대기업을 중심으로 이루어졌으나 이제는 정보보호 사각지대에 있는 중소기업과 소상공인을 대상으로 한 정보보호 활동에 좀 더 많은 지원이 필요한 시점이다. 이러한 시점에서 중소기업들이 보유하고 있는 핵심기술 등의 정보자산을 보호하고 안전한 환경에서 기업 성장이 지속적으로 가능하도록 중소기업의 규모와 정보화 수준을 고려한 전략적인 정보보호 체계를 구축할 필요가 있다[4, 5]. 또한 예산과 전담인력 부족으로 정보보호 활동에 소홀한 중소기업이 각종 사이버위협의 표적이 되는 경우가 많아 높은 수준의 정보보호 컨설팅 지원을 통해 중소기업이 지닌 보안 취약점을 정확히 진단하고 정보보호 도입을 원활하게 하여 정보보호 역량 강화를 위한 기반을 조성해야 하는 필요성이 대두되었다.

한국인터넷진흥원 중소기업 정보보호 컨설팅 사업은 정보보호에 소외된 중소기업의 정보보호 역량을 강화하여 각종 사이버 위협으로부터 받는 피해를 최소화 및 중소기업에게 정보보호 활동의 중요성을 인식시키고, 기업 자체적으로 예산과 인력의 투자를 유도하여 정보보호 역량 강화를 위한 기반을 마련하도록 하는 것에 주안점을 두고 있다[6]. 현재 진행되고 있는 중소기업 정보보호 컨설팅은 중소기업 규모와 ICT 시설 보유 정도를 고려하여 기술진단과 정보보호 정책을 기업별 맞춤형 형태로 컨설팅을 지원하고 컨설팅 결과에 의해 발견된 취약점에 대한 보안솔루션을 지원하는 조치가 매칭 형태로 이루어지고 있다.

본 연구에서는 한국인터넷진흥원의 중소기업 정보보호 컨설팅 결과를 기반으로 정보보호 효과를 분석하고 정보보호 관리체계, 개인정보처리방침, 홈페이지 및 기업 인프라 시스템의 기술적 취약점, 모의해킹 등의 각 영역별 세부 진단의 성과와 한계점을 파악하여 중소기업이 정보보호 관리체계를 더욱 효율적이고 효과적으로 관리할 수 있는 중소기업 정보보호에 대한 개선방안을 제안하도록 한다.

Ⅱ. Preliminaries

1. Small and Medium Business Status

우리나라 중소기업 사업체 수는 2017년 기준으로 3,733천개, 종사자수는 15,528천명으로 전체 사업체의 99.9%와 전체고용의 89.8%를 차지하고 있다. 연도별 중소기업 현황은 [Table 1]에 나타나 있는 것처럼 중소기업의 사업체 수와 종업원 수가 지속적으로 증가하고 있다[7, 8, 9].

그러나 정보통신망 사이버 침해범죄는 2014년 2,291건에서 2017년 3,156건으로 약 38% 증가하고 있고[경찰청, 2017년], 또한 사이버침해사고중 97%가 중소기업에서 발생하고 있다[KISA, 2017년 통계]. 중소벤처기업부의 2017년 중소기업 기술보호 역량수준 실태조사 결과에 따르면 중소기업은 해킹의 주요 대상이자 악성코드 유포·경유지로 이용되며 기술 유출금액이 2015년 902억 원, 2016년 1,097억 원, 2017년 1,022억 원으로 매년 증가추세에 있다. 또한 한국인터넷진흥원 2017년 정보보호 실태조사 결과에 의하면 50인 미만의 중소기업의 경우 보안정책 수립은 11.6%, 정보보호 전담조직 운영은 2%, 정보보호 예산 투자 1% 미만이 88.7%를 차지하는 등 중소기업은 정보보호예산, 전문인력 측면에서 열악하여 그 규모의 특성상 중·대기업에 비해 상대적으로 사이버공격에 매우 취약하다고 할 수 있다. 따라서 국내 기업의 대부분을 차지하고 있으나 상대적으로 정보보호 수준이 낮은 중소기업에 대한 정보보호 역량 강화

Table 1. SMEs Status by Year

(Unit : a thousand, thousand person)

Division		2011	2012	2013	2014	2015	2016	2017
Number of Business	all(A)	3,235	3,354	3,419	3,545	3,605	3,676	3,737
	SMEs(B)	3,232	3,351	3,416	3,542	3,601	3,672	3,733
	ratio(B/A)	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%
Number of Employees	all(A)	14,534	14,891	15,345	15,963	16,775	17,051	17,294
	SMEs(B)	12,627	13,059	13,422	14,028	15,127	15,392	15,528
	ratio(B/A)	86.9%	87.7%	87.5%	87.9%	90.2%	90.3%	89.8%

지원 활동은 안전한 기업의 경제활동과 국가적인 경제 손실을 예방하는 디지털 경제 환경 조성을 위한 핵심 과제로 떠오르고 있다.

2. Information Protection Consulting Procedures and Effectiveness

정보보호 컨설팅은 기업이 보유한 정보자산 분류와 보안취약점 분석, 발견된 문제점에 대한 보호대책을 수립하는 일련의 활동을 통해 기업의 정보보안에 대한 인식과 역량 제고 등 보안 수준을 향상시킬 뿐만 아니라 기업의 핵심 기술유출방지를 통한 경영 리스크 제거 및 침해사고 예방과 대응 자생력을 배양하는 것이다[10].

먼저 정보보호 컨설팅의 절차를 간단히 살펴보면 첫째, 정보자산 현황 파악 및 분석과, 홈페이지 등 정보자산에 대한 기술적 · 관리적 · 물리적 보안진단, 모의해킹, 그리고 이에 대한 위험평가 등을 통한 문제점 도출 후 정보보호 마스터플랜, 세부 수행과제 도출 등의 종합대책을 마련하는 업무가 진행된다. 둘째, 정보보안에 대한 인식과 관심을 고취시키고 경영층 주도의 보안환경 조성과 보안투자유발 등 일상에서의 정보보호 생활화를 위해 최고경영자(CEO)를 포함한 관리자, 실무자 등 전 임직원에 대한 보안교육이 이루어지도록 하는 것이다.

정보보호 컨설팅의 효과로는 첫째, 정보보호에 대한 인식전환과 투자로 정보보호 수준이 한층 더 제고됨으로써 기업 핵심기술 등의 정보유출 피해와 같은 경영 리스크를 제거하는데 기여하고 안전한 환경에서 기업 경영을 효과적으로 수행 할 수 있다. 둘째, 체계적인 정보보호 관리활동을 통하여 사이버 위협으로부터의 침해사고 예방과 대응 능력을 자체적으로 갖추게 하고 정보유출 등의 사이버 공격 발생 시 신속한 대처가 가능하게 하는 효과가 있다.

3. SMEs Information Protection Status

중소기업 정보 유출은 국내 기업들의 경쟁력 하락과 함께 기업 매출을 저하시킬 뿐만 아니라 국가 기술 경쟁력을 악화시키는 요소가 된다. 정보 유출은 국내 기업들의 기술이 발전할수록 더욱 증가하고 있으며, 이러한 기술의 중요성과 정보유출의 유해성을 인식하여 「산업기술유출방지법」, 「영업비밀보호법」, 「정보통신망법」등이 제정 되었다. 정보유출 뿐만 아니라 정보보호에 대한 중요성이 부각되어 관련법규와 제도가 생겨났다. 국내의 대표적인 정보보호 인증제도는 PIMS(개인정보보호 관리체계), K-ISMS(정보보호 관리체계)로 시작되어 2018년 11월 하나로 통합된 ISMS-P와 ISO27001(정보보호 관리체계 국제표준)이 있다[11].

중소기업은 민간부분 전체 기업의 99% 이상을 차지하고 있고 사이버범죄의 주요 대상이 되고 있는 실정이다[12]. IT기술의 급속한 발전은 중소기업의 경제 활동에 있어 영향력을 계속해서 확대할 수 있는 기반을 제공하고 있으나, 중소기업이 보유하고 있는 정보 자산에 대한 가치 증가는 사이버범죄 대상이 되는 하나의 중요한 요소로 작용하고 있다. 최근 대부분의 보안 사고가 중소기업들에서 발생하고 있는 것은 중소기업의 정보 자산의 가치는 높아지고 있으나 보안 활동의 사각지대에 노출되고 있음을 보여주는 것이다. 중소기업의 보안 문제는 더 이상 한 기업만의 책임이나 국한된 문제가 아니며 국가 안보 수준까지 영향을 미칠 수 있음을 인지하여야 한다. 따라서 정부는 중소기업의 보안 수준을 개선하고 대책을 강구하는데 보다 많은 관심과 예산 지원 등 다각적인 노력을 아끼지 말아야 할 것이다.

4. Status of SMEs Information Security Management System

정보보호라 함은 컴퓨터와 같이 정보처리능력을 가진 장치를 이용하여 데이터를 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 기술적·물리적·관리적 수단을 강구하는 모든 행위를 의미하며 사이버안전까지를 포함한다[13].

국내 정보보호 관리체계 제도의 경우「정보통신망법」제47조 ②항에서 정한 의무대상자들만이 이행하고 있고 정보보호 활동의 사각지대에 있는 중소기업은 제한된 인력과 예산의 부족 때문에 높은 수준의 정보보호 활동을 자체적으로 수행하는 것이 매우 어렵다는 문제를 가지고 있다.

정보보호 수준은 정보보호 관리체계의 적극적이고 지속적인 운영과 인식 정도에 따라 달라지는 것이다. 그러

나 현재 보급이 이루어지고 있는 정보보호 활동의 가이드라인 ISO27001과 ISMS-P는 중소기업 역량에 대한 고려보다는 일정규모 이상의 조직을 갖춘 기업의 관점에서 개발되었다. 대기업에 비하여 상대적으로 부족한 중소기업의 경험, 예산, 인적 자원 수준은 중소기업이 자발적으로 정보보호 활동에 참여하는 것을 쉽지 않게 하고 있다. 결과적으로 중소기업은 보안의 위협에 더욱 많이 노출되는 상황으로 된 것이다[12].

III. Information Security Consulting for SMEs

1. Conducted Information Security Consulting for SMEs

과학기술정보통신부와 한국인터넷진흥원이 중소기업 정보보호 수준 제고 및 역량 강화를 위해 수행한 중소기업 정보보호 컨설팅 사업은 2018.05.14일부터 2018.12.15까지 진행하였으며 원활한 사업수행을 위해 업무 프로세스를 사전준비, 진단준비, 현장진단, 대책수립, 기술지원 등 5단계로 구분하여 진행하였다. 정보보호 컨설팅 단계별 절차를 보면 1단계에서는 사전준비 단계로 중소기업 정보보호 컨설팅에 선정 된 중소기업에 대한 구체적인 현황 파악 및 진단을 위한 범위 설정 등 컨설팅 수행계획을 수립하였다. 2단계에서는 진단준비 단계로 현장진단 이전 개인정보처리방침 및 사전에 전달 받은 인프라시스템 결과 값(스크립트)의 보안수준 진단 및 모의해킹 등을 실시하였다. 3단계에서는 현장진단 단계로 진단준비 단계에서 전달받은 시스템 결과 값(스크립트)에 대한 보안취약점 리뷰 및 체크리스트 기반의 관리체계를 진단하였다. 4단계에서는 대책수립 단계로 정보보호 관리체계 및 기술진단, 모의해킹 과정에서 도출된 취약점을 위험분석한 후 식별된 고위험에 대하여 대책을 수립하여 정보보호 수준을 높이는 방안을 제시 하였다. 마지막 5단계 기술지원 단계에서는 도출된 취약점을 보완할 수 있는 정보보호 솔루션을 제시하고 기 도출된 취약점의 보완조치에 대한 이행점검 업무를 수행하였다.

본 논문에서는 중소기업 정보보호 컨설팅을 단계별로 진단하여 최초진단, 이행점검, 컨설팅 반영, 솔루션 반영에 따른 보안수준과 진단영역별 보안수준에 대한 정보보호 컨설팅 효과를 분석하도록 한다.

2. Information Protection Consulting Security Level of SMEs

중소기업 정보보호 컨설팅 지원 사업에 선정된 195개 업체를 대상으로 정보보호 관리체계 영역 내 관리적·물리적 진단, 개인정보처리방침, 관리자 페이지 및 인프라 시스템 내 기술적 취약점 진단, 모의해킹 영역을 진단하였다. 보안수준은 진단 영역별 보안수준, 업종별 보안수준, 규모별 보안수준, 정보보호 관리체계 영역별 보안수준, 개인정보처리방침 보안수준, 기술적 취약점 영역별 보안 수준, 웹 취약점 영역별 보안수준을 파악하였다. 본 논문에서는 진단 영역별 보안수준과 규모별 보안수준의 내용만을 참조하였다.

2.1 Security Level per Diagnostic Area

중소기업 정보보호 컨설팅을 신청한 195개 업체의 전체 보안수준은 보통(67.3%) 수준으로 평가되었으며 정보보호 관리체계는 취약(52.4%), 개인정보처리방침은 양호(84.4%), 기술적 취약점 진단은 보통(61.4%), 모의해킹 진단은 보통(71.0%)으로 평가되었다[Table 2].

Table 2. Comprehensive Status of Consulting Results

Management System		Infrastructure System		Overall Security Level
Information Protection Management System	Personal Information Processing Policy	Diagnose a Technical Vulnerability	Mock Hacking Diagnosis (Web Vulnerability)	Usually 67.3%
Weak 52.4%	Good 84.4%	Usually 61.4%	Usually 71.0%	

2.2 Security Level by SMEs Size

선정 업체 규모를 보호대상 중견기업, 중기업, 소기업, 소상공인으로 구분하여 보안 수준을 진단하였다. 중소기업의 규모별 보안수준을 보면 보호대상 중견기업 보안수준은 다른 규모별 수준 대비 높은 것으로 평가되었으나 모의해킹 진단 부분에서는 가장 낮은 보안수준을 보였다. 중소기업 전체적으로 보안수준은 대동소이한 것으로 나타났으나 개인정보처리 방침이 다른 분야에 비해 높은 보안수준을 보여주었고 정보보호 관리체계 분야에서는 보호대상 중견기업을 제외하고 전반적으로 낮게 나타났다[Table 3].

Table 3. Security Level by SMEs Size

(Unit : %)

By Scale	Information Protection Management System	Personal Information Processing Policy	Diagnose a Technical Vulnerability	Mock Hacking Diagnosis (Web Vulnerability)	Average Security Level
Small Business Person	49.9	82.3	63.7	81.0	69.2
Small Business	49.4	78.0	59.6	69.4	64.1
Medium Business	59.1	88.1	64.0	67.5	69.7
Protected Medium Enterprise	99.8	84.0	75.1	45.0	76.0

3. Problems of SMEs Information Security Management

중소기업의 정보보호에 대한 관리적·물리적 보안체계와 기술적 취약 상태를 진단한 결과에서 도출한 문제점을 보면 크게 8가지로 요약할 수 있다.

첫째, 정보보호 정책 및 조직 부분에서 관리체계 및 침해사고 대응절차 수립이 미흡하였다. 대부분의 중소기업들이 정보보호 관리체계 수립과 운영을 위한 정책·인력 및 조직·예산 등을 마련하지 못한 상태에 있으며 침해사고 발생 시 이를 체계적으로 대응하기 위한 절차가 마련되어 있지 않아 침해사고 이후 발생 가능한 동일 이슈에 대해 능동적으로 대응하는데 한계가 있었다.

둘째, 인원보안 및 자산관리 부분에서는 내부정보 유출 대응을 위한 보호대책이 미흡하였다. 중소기업 정보보호 컨설팅 신청 업체 대부분이 내부직원의 주요정보 유출에 대한 위험을 인식하고 있으나, 퇴사자 퇴직 관련 보안절차 및 이동식 저장매체와 사용과 관련한 접근 통제 절차가 수립되어 있지 않았다.

셋째, IT보안관리 분야에서 정보보호시스템 운영 주체가 모호한 문제가 있었다, 회사의 인력규모 혹은 장비 운용과 관련한 전문성을 이유로 정보보호시스템 관리·운영 주체가 지정되지 않아 해당 장비를 관리하지 못하는 경우가 일부 식별되었다.

넷째, 보안사고 관리 부분에서 침해사고 이후 사후관리가 미흡하였다. 동일한 사고를 방지하기 위한 보호대책 수립 및 임직원 보안 교육 등 사후관리가 이루어지지 않았다. 또한 보안 관리에서 PC 보안설정 관련 문제로 임직원 개별 보안인식에 따라 PC 보안설정 수준이 다르게 나타났다.

다섯째, 개인정보관리 분야에서는 개인정보를 처리하는 일부 기관의 경우 개인정보보호법 및 정보통신망법 등 법적 요구사항에 충족하지 못하는 미흡사항들이 다소 존재하였으며, DB관리를 위한 관리적·기술적 보완조치가 취약하였다. 또한 개인정보처리방침에 기재된 개인정보 수집항목과 실제 어플리케이션에서 수집되는 항목이 상이하였다.

여섯째, 관리자페이지 부분에서는 웹호스팅 업체가 아닌 직접적으로 홈페이지를 운영하는 기관의 경우 외부 네트워크에서 관리자페이지에 접속이 가능하거나 로그인 시도 횟수 제한 부재로 인해 자동화 공격 위험 등이 모의해킹을 통해 다수 식별되었다.

일곱째, 계정관리 부분에서는 인프라 보안설정이 미흡하고 중소기업 정보보호 컨설팅을 신청한 기업들의 서버 및 IT 인프라 자산들의 기술취약점을 진단한 결과 대체로 서버 보안설정(계정, 접근관리, 로그 등) 등이 기본 상태로 운영되고 있는 것으로 파악되었다.

여덟째, 모의해킹 분야에서는 관리자 페이지 노출과 홈페이지에서 관리자 페이지에 접근 시 관리자 페이지에 접근이 가능하였다. 파라미터 변조를 통한 비정상 접근 가능하였고 파라미터 변조를 통해 타 사용자의 비밀번호를 변경하거나 접근이 제한된 페이지의 접근이 가능하였다.

본 논문에서는 이와 같이 중소기업 정보보호 컨설팅 과정에서 나타난 여러 가지 문제점을 관리적·물리적 보안체계와 기술적 취약 상태의 보안 관점에서 중소기업 정보보호 개선과 해결방안을 제안하도록 한다.

IV. Analysis and Improvement Plan of Information Protection Consulting Effect of SMEs

1. Analysis of Information Protection Consulting Effect of SMEs

정보보호 컨설팅 효과를 분석하기 위해 모든 업체를 대상으로 컨설팅 진행단계별 정보보호 수준을 점검하였다. 최초진단 시 보안수준 평균이 67.3%로 도출되었으나, 각 기업별 자체 취약점 보완조치와 이행 점검 이후 69.7%, 컨설팅 효과 반영 이후 71.6%, 보안 솔루션 효과 반영 이후 73.5%로 향상되었다. 결과적으로 중소기업 정보보호 컨설팅 및 정보보안 솔루션 구축을 통해 중소기업 보안수준이 최초진단 67.3%에서 73.5%로 향상되어 최초

진단 대비 9.2%가 상승된 것으로 분석되었다[Table 4].

한국인터넷진흥원에서 실시한 중소기업 정보보호 컨설팅은 관리적 보안, 물리적 보안, 기술적 보안의 구성요소로 진행되었다. 정부차원에서 이루어지고 있는 지속적인 정보보호 컨설팅으로 인하여 결과적으로 기술과 정보의 유출에 따른 인적, 물적 손해를 사전에 예방하고, 기업체의 최고경영자에 대한 정보보호의 중요성과 보안의식을 고취 시킬 뿐만 아니라 전사적 보안관리 체계를 구축하여 기업의 경쟁력을 향상 시키고 경제발전에 기여할 것으로 기대한다.

Table 4. Level of Security Level by Progress

(Unit : %)

Step Classification	Information Protection Management System	Personal Information Processing Policy	Diagnose a Technical Vulnerability	Mock Hacking (Penetration Testing)	Average Security Level	Security Level Increase Rate
Initial Diagnosis Result	52.4	84.4	61.4	71.0	67.3	
Implementation Check Result	52.4	88.1	66.7	71.4	69.7	3.6% ▲
Reflecting the Effect of Consulting	60.2	88.1	66.7	71.4	71.6	6.4% ▲
Effect of Solution	63.3	88.1	67.9	74.6	73.5	9.2% ▲
Security Level Improvement Effect	10.9%p ▲	3.7%p ▲	6.5%p ▲	3.6%p ▲		

2. Measures to Improve Information Protection for SMEs

2.1 Problem-Centered Improvement Plan in Information Protection Consulting Process

중소기업 정보보호 컨설팅과 솔루션 제공이 지속적으로 이루어져 효과성과 효율성을 더욱 제고하기 위한 정보보호 컨설팅 개선방안을 컨설팅 절차에서 나타나는 문제점 중심으로 제시한다.

중소기업 컨설팅 절차에서 나타난 문제점으로는

첫째, 최초 홍보·신청서 접수단계에서 중소기업의 컨설팅 사업 내용에 대한 이해가 부족한 기업 담당자를 대상으로 컨설팅 프로세스에 대한 이해도를 높이는 사전 준비단계 진행에 어려움이 많았다.

둘째, 컨설팅 신청 후 포기사유가 다량으로 발생했는데 그 이유는 솔루션 도입 비용부담, 솔루션 리스트에 기업이 원하는 솔루션의 부재, 내부 인력사정으로 인한 담당자 부재 등의 이유로 나타났다.

셋째, 중소기업 담당자의 업무 과중으로 컨설팅 대응이나 회신이 1~2개월 늦어져서 컨설팅 진행 일정이 지연되거나 최종적으로 포기하는 사례가 발생하였고 마스터플랜 과제 도출과 솔루션 선정 시 컨설팅만 받고 솔루션 도입은 진행하지 않으려 하는 경향이 있었다.

넷째, 솔루션 신청서 접수와 견적서 제출 시 기업 담당자의 정보보호 솔루션 이해 부족 및 솔루션 신청절차 상의 문제점이 일부 발생하는 등 신청 프로세스 진행상의 어려움 존재하였다.

다섯째, 솔루션 신청 이후 납품·구축·검수 상의 확인절차가 미흡하였다.

이를 해결하는 방안으로는 성공적인 정보보호컨설팅을 위해서 기업체의 최고 경영진의 정보보호의 중요성과 보안의식에 대한 인식 제고, 의지가 가장 중요하다. 중소기업 영역별 특성과 경영진 및 실무자 등 교육 대상을 고려하여 기업의 정보유출, 랜섬웨어 등 사이버침해사고 피해사례와 보안대책 등 맞춤형 교육 프로그램을 좀 더 세분화하여 개발하고, 정보보호에 대한 인식제고와 정보보호 수준강화를 위해 지역단위의 유관기관, 단체 등과의 합동설명회 등 다양한 방법의 지속적인 홍보 및 교육 체계가 선행적으로 필요하다. 따라서 경영진에서부터 먼저 사이버위협의 심각성을 실감하고 보안에 대한 인식전환이 우선시 될 때 정부차원의 정보보호컨설팅 지원사업에 대한 이해와 자발적인 참여가 높아질 것이다.

또한 중소기업은 예산과 인력, 전문지식 부족, 담당자 부재 등의 이유로 인하여 높은 수준 의 정보보호 활동을 이행하는 것이 어렵다는 현실적인 문제와 적극적인 정보보호 조치가 어려운 환경이므로 중소기업이 자발적으로 정보보호 활동에 참여할 수 있도록 유도하는 충분한 재정적 지원과 중소기업의 컨설팅과 솔루션 선택권을 유동적으로 지원하는 체제가 필요하다. 아울러 중소기업 정보보호컨설팅 이후에는 기업 자체적으로 솔루션 범위, 제품 등을 쉽게 선택할 수 있도록 네트워크, 시스템, 단말, 콘텐츠보안 등 다양한 범주의 중소기업 특성에 맞는 보안제품을 쉽게 이해하고 선택할 수 있도록 설명자료 등을 체계적으로 정리하여 홍보하고 제공할 필요가 있다.

2.2 Improvement Plan of Information Protection Management System

정보보호 컨설팅이 중소기업의 기술을 보호하고 경쟁력을 강화하기 위해서는 정보보안이 철저히 이루어져야 한다. 정보보호 컨설팅의 효과성과 효율성을 제고하기 위한 중소기업의 높은 보안인식과 이행해야 할 사항을 관리적 보안, 물리적 보안, 기술적 보안 관점에서 3가지로 요약하여 제시 한다[Table 5].

중소벤처기업부의 2017년 중소기업 기술보호 역량수준 실태조사 결과에 의하면 중소기업 기술유출사고 주요 원인으로 보안관리, 감독체계 미흡이 47.6%였고 2016년도에는 내부직원에 의한 기술유출피해가 76.9%를 차지하는 등 관리적 측면의 보안대책 개선이 가장 시급한 것으로 나타났다. 따라서 예산, 조직 등 중소기업의 여건상 보안관리 체계 운영이 쉽지 않은 측면이 존재하여 이를 위해 일정규모 이상의 중소기업에 대한 차등화 된 보안관리 체계 개선 등에 대한 정책이 최소한 도입될 수 있도록 정책적, 제도적 연구검토가 필요하다.

Table 5. Security Awareness and Compliance of SMEs in terms of Security Perspective

Security Perspective	Security Awareness and Compliance of SMEs
Administrative Security	· Establish security management regulations and actively manage them. · Assign security officers and departmental security officers and assign responsibility. · Implement periodic information protection training for all employees. · Create a security pledge for all employees and raise awareness and responsibility for security.
Physical Security	· Entire facility personnel access control and records management of company visitors thoroughly. · Enhanced security zones and security zones for hazardous areas where technology and information can be leaked.
Technical Security	· Thorough control of unauthorized personnel access to information security systems. · Homepage administrator access account encryption. · Building a mail server spam filter for Internet security. · Periodic maintenance and maintenance of network systems, new versions of updates for Windows security, vaccine testing and treatment.

2.3 Improvement Plan Focusing on Characteristics of SMEs

중소기업은 규모와 특성으로 보아 IT인력과 정보보호 관련 전문성이 부족하고, 정보보호 전문 인력을 별도로 두는 경우가 드물어 정보보호에 따른 실질적인 운영이 어려운 실정이다. 이러한 중소기업의 환경을 고려하여 정부와 지자체의 주도하에 추진 가능한 개선방안을 제시하도록 한다.

첫째, 중소기업의 분야, 특성, 규모, 환경에 적합한 맞춤형 정보보호 관리체계를 마련하고 정보보호 컨설팅에서 정보보호 시스템 구축까지 중소기업의 정보보호가 체계적으로 이루어지도록 표준화된 프로세스를 만들어 정부차원의 컨설팅 사업이 단발성이 아닌 지속적으로 제공되고 확대될 필요성이 있다.

둘째, 중소기업 스스로 보안체계를 마련하고 보안수준 제고를 위해 중소기업 업종, 규모, 환경 등 특성에 맞는 자가진단 가이드북을 개발하여 보급하고 중소기업 스스로 정보보호에 대한 인식전환과 실천이 이루어지도록 유도할 필요가 있다.

셋째, 정부의 역할로 중소기업진흥공단 지역본부나 지역별 산업단지관리공단 및 중소기업 관련협회 차원에서 중소기업이 정보보호 관련 전담부서와 인력, 예산 등을 마련할 수 있도록 지원하고, 정보보호 전담 부처인 과학기술정보통신부와 한국인터넷진흥원 등과 협력하여 중소기업 정보보호 수준제고를 위해 체계적으로 지원해줄 수 있는 다양한 프로그램들을 강구할 필요가 있다.

넷째, 무엇보다도 중소기업이 자발적으로 정보보호 활동을 시작하고 강화 할 수 있도록 정부차원의 유인책이 필요하며 이를 위한 연구 및 각종 제도적 장치를 마련하는 검토가 필요하다. 즉 개인의 건강관리는 스스로 하는 것이 가장 최선의 예방이 되는 것처럼 정보보호컨설팅 지원 사업 등의 정부 예산을 지속적으로 투입하기는 한계가 따르므로 많은 중소기업이 스스로 정보보호를 실천할 수 있도록 그 환경을 만들어 주는 것을 우선시 하는 것이 무엇보다 중요하다.

V. Conclusions

중소기업은 지금까지 해킹의 주요 대상으로 사이버 위협에 크게 노출되어 있음에도 불구하고 예산과 인력, 전문지식 등이 부족하여 적극적인 정보보호가 이루어지지 않아 전반적으로 보안수준이 취약한 상황에서 벗어나지 못하고 있는 실정이다. 기업의 기밀정보나 개인 정보 유출, 랜섬웨어 감염 등으로 인한 기업 활동의 제약 및 금전적 피해 등은 현재 중소기업의 가장 큰 문제이며 정보보호 대책을 마련하지 않으면 안 되는 상황이다. 이에 따라 한국인터넷진흥원에서는 지역에 소재하고 있는 중소기업의 정보보호 역량을 강화하여 각종 사이버 위협으로부터 받는 피해를 최소화하고 중소기업에게 정보보호 활동의 중요성을 인식시키기 위

하여 중소기업 정보보호 컨설팅 사업을 추진하고 있다. 이러한 정보보호 컨설팅은 개인이나 기업의 모든 정보자산에 일어날 수 있는 잠재적 위험에 대하여 체계적으로 분석하고 그 결과에 따른 대책을 수립하여 조직과 관리자가 그 대책을 실현하도록 지원하는 것이다.

중소기업 정보보호 수준은 기업체 최고 경영자의 정보보호 중요성과 보안의식에 대한 높은 인식에 따라 좌우될 수 있다. 또한 정보보호 관리체계에 의한 운영과 체계적인 활동 정도에 따라서 달라질 수 있는 것이다. 국내에서 현재 운영되고 있는 정보보호 활동의 가이드라인 ISO27001과 ISMS-P는 중소기업이 적용하기에는 무리가 있으므로 중소기업이 정보보호 활동을 체계적으로 이행하고 정보보호의 중요성 인식과 더불어 자발적으로 참여하여 실효성을 거둘 수 있도록 중소기업 환경에 맞는 정보보호 가이드라인 마련 등 기존 지원체계 등을 재분석하고 검토하여 좀더 개선된 프로그램으로 정보보호서비스를 제공해야 할 것이다.

결과적으로 스마트 혁명의 포노 사피엔스 시대에 중소기업의 정보보호 관리체계는 중소기업의 경제 활동에 있어 혁신과 경쟁력 강화, 생산성 향상을 확장할 수 있는 중요한 기반으로 제공되어 질 것이다. 중소기업 정보보호 관리체계 구축을 위한 프로세스 등 좀 더 체계화 된 다양한 프로그램 제공이 이루어진다면 중소기업이 정보 보호 활동에 보다 더 적극적으로 참여하도록 동기를 부여할 수 있을 뿐만 아니라 중소기업이 스스로 정보보호 활동에 참여할 수 있는 계기가 될 것으로 기대된다.

이제 중소기업의 보안 수준은 더 이상 그 기업체만의 문제가 아니라 국가 안보에까지 영향을 끼칠 수 있음을 깊이 인식하여 중소기업의 보안 수준을 향상시키기 위한 노력이 요구되고 정부 차원에서 좀 더 적극적인 정책으로 받아들여 중소기업의 자생력을 강화할 수 있도록 아웃리치와 온 루프 서비스(Out Reach & One Roof Service) 전달체계가 구축되어 중소기업이 사이버 위협으로부터 자유로울 수 있어야 할 것이다.

현재 이루어지고 있는 한국인터넷진흥원의 중소기업 정보보호 컨설팅 사업은 중소기업의 보안체계를 구축 하는데 최고의 보안 기술력과 다양한 컨설팅 경험을 보유한 보안전문가들이 직접 참여하여 정보보호 정책설계와 중소기업에 요구되는 사항을 최적으로 충족시켜줄 수 있는 컨설팅 서비스가 좀 더 발전된 양상으로 계속 진행되어야 할 것이다.

ACKNOWLEDGEMENT

This paper was supported by Research Funds of Kwangju Women's University in 2019(KWU I19-060).

This paper, I have studied the contents of “SMEs Information Security Consulting Project (2018)”, which was a member of the Korea Internet & Security Agency(KISA)’s Information Security Management Committee.

REFERENCES

[1] YsPark, “An Application method of the Information Security Management System to Control Items : Focusing on Semiconductor Industry”, Graduate School of Information Sciences Soongsil University, 2018.

[2] CoKim, “Balancing the Level of Information Protection through SMEs Information Protection Management System Standards”, 2017.

[3] Ministry of SMEs and Startups, “Final Report of Actual Survey of Technology Protection Level of SMEs in 2018”, 2019.

[4] CsRyu, “Knowledge Sharing Model of Government Supported SMEs Informatization Project”, Korea Business Review, 1(2), pp. 85-97, 2008.

[5] YhKim & HbChang, “Propulsion Direction of Appropriate Level of SMEs Information Protection”, Korea Institute of Information Security and Cryptology, 23(4), 41-46, 2013.

[6] Korea Internet & Security Agency(KISA), “SMEs Information Protection Consulting Result Report”, 2018.

[7] Statistics Korea, “National Business Survey”, 2017.

[8] http://stat.kbiz.or.kr/

[9] Ministry of SMEs and Startups, “Status of SMEs in Korea”, SME Statistics & Statistics DB Search, 2019.

[10] HgShin, “Security Diagnosis and Improvement Examples of SMEs”, Korea Industrial Technology Protection Association, 2012.

[11] BgLee, “Information Security Management System Suitable for SMEs”, Graduate School of Information Sciences Soongsil University, 2017.

[12] CoKim, “Activation Plan of SMEs Information Protection Activity”, Telecommunications Technology Association, 2017.

[13] Ministry of Science and ICT, “Criteria for Information Protection of Cloud Computing Services”, 2017.

Authors

Jae-Nam Kim received the B.S., M.S. and Ph.D. degrees in Computer Science and Statistics from Chonnam National University, Korea, in 1984, 1989 and 2006, respectively.

Dr. Kim joined the faculty of the Department of Computer Science at Kwangju Women's University, Gwangju, Korea, in 1992. He is currently a Professor in the Department of Social Welfare at Kwangju Women's University, He is interested in Welfare Information System, Welfare Statistics.