논문 2010-2-5

지식정보보안 컨설팅전문업체 제도 개선방안 고찰

정연서*, 박진섭**

Improvement of Standard on a Information Security Consulting Service Provider for Information Infrastructure

Youn-seo Jeong*, Jin-sub Park**

요 약

1991년 사이버공격(해킹, 웜, 바이러스, DDoS패킷공격)들로부터 국가의 중요한 기반시설들을 보호하기 위하여 정보통신기반보호법을 제정하였다. 법 규정에 따라 주요 통신시설들에 대하여 기반시설로 지정하였으며, 해당 시설들에 대한 취약점을 점검, 분석하고 보호대책과 계획을 수립하고 시행하기 위해 지식정보보안 컨설팅전문업체 지정제도를 도입하였다. 그러나, 현재의 지정제도의 평가기준은 여러 가지 문제점들을 안고 있다. 본 논문에서는 먼저, 현재 국가의 정보보호 제도들을 조사하고, 국내 보안컨설팅 시장과 인력 채용 현황에 대하여 분석하였고, 지식정보보안 컨설팅전문업체 지정기준의 문제를 분석하고 개선사항들을 제안하였다.

Abstract

In 1991, the protection law for information communication is made in order to protect national important infrastructure from cyber attacks(hacking, worm, virus, DDoS). According to the law, infrastructure of communication is being appointed as the main information communication infrastructure. By analyzing and evaluation the weak points of infrastructure, we imported the rules made by the information security consulting service provider to establish and perform protection policies and plans. However, There have been various problems in current listing standards for information security consulting service provider. In this paper, we did some research about system and service on information security for information infra structure of nation. In addition, we investigated for current situations of workspace and employment of information security industry. Finally, we analyzed the problem of current listing standards and proposes the better method for evaluation of information security consulting service provider for Information Infrastructure.

Keywords: security, security policies, information security policy

Ⅰ. 서 론

1999년 CIH 바이러스로 인해 국내 PC의 4% 수준인 30여만대가 감염되어 피해를 입었으며, 금전적으로는 20여억원의 피해가 발생하였다. 2000년에는 야후, CNN 방송 등 유명 사이트들이 해커들의 DDoS 공격으로 수시간동안 마비되는

* 한국전자통신연구원 (주저자: jys847@etri.re.kr)
** 대전대학교 (교신저자: jspark@dju.kr)
접수일자: 2010.10.20 수정완료: 2010.11.15

사건이 있었으며 국내에서도 PC방 서버 조사중 대기업, IDC 등 다수의 국내사이트가 해킹당한 흔적이 발견되었으며 앞서 발생한 DDoS 공격에 사용된 것으로 추정되는 도구들이 설치되어 있는 것이 발견되었다. 이후 1.25인터넷대란[1]과 7.7대란[2]이 발생하여 우리나라는 물론 전세계 각국에서는 많은 피해를 경험하였다.

해킹이나 바이러스에 의한 피해가 지속적으로 늘어나고 해킹과 바이러스가 혼합된 새로운 형태의 공격들이 나타남에 따라 세계 각국에서는 자국의 주요 기반시설들의 보호를 위한 기구와 제도를 마련하여 운영하고 있다. 우리나라에서도 주요 정보통신기반시설들을 보호하기 위한 범정부적대응체계 구축을 위해 2001년 정보통신기반보호법을 제정, 공포하고 7월부터 시행하여 오고 있다[1,2,17].

정보통신기반보호법외에도 정보통신망 이용촉진 및 정보보호등에 관한 법률, 정보통신산업진흥법, 통신비밀보호법, 전기통신기본법, 전기통신사업법, 전파법 등 관련된 많은 관련 법률들과 지침이 제정되고 정비되고 있다.

현재 주요정보통신기반보호, 정보보호안전진단, 정보보호관리체계인증 등 정보보호를 위한 다양한 제도들이 시행중에 있으며, 새롭게 만들어지고 있다[13]. 정부에서는 이같은 일을 수행하기 위한 전문업체를 심사를 통해 선정하고 '지식정보보안 컨설팅전문업체'자격을 부여하고 있다. 그러나, 지식정보보안 컨설팅전문업체 지정은 2001년 수립된 절차 및 기준으로 유지되고 있고 산업환경의 변화와 더불어 운영함에 있어 여러 가지 문제점이 지적되고 있다[9-13,15,16]. 본 논문에서는 현재 운영되고 있는 지식정보보안 컨설팅전문업체 지정을 위한 제도를 살펴보고 문제점을 분석, 개선점을 제시하고자 한다.

2장에서는 현재 보안컨설팅 시장을 분석하고 관련된 제도들의 현황에 대해서 조사한다. 3장에서는 전문업체 지정제도와 업체현황을 기술하고, 4장에서 지정기준과 개선점을 제시하고 마지막으로, 결론을 맺는다.

1) 수분만에 전세계 7만5천여대의 서버가 감염되어 국가 전체적으로 인터넷이 마비됨(2003.1.25)

2) 청와대, 국회 및 주요정부기관 및 포털, 은행 등 주요 사이트들을 대상으로 한 DDoS 공격으로 대상 사이트가 마비됨(2009.7.7.)

II. 정보보호제도와 보안컨설팅 시장현황

정부에서는 사이버공격 예방과 피해를 줄이기 위해 관련법에 의거하여 주요정보통신기반보호(Critical Infrastructure Protection : CIIP), 정보보호안전진단(Information Security Check Service : ISCS), 정보보호관리체계인증(Information Security Management System : ISMS)과 같은 다양한 제도를 만들어 시행하고 있다[16]. 주요정보통신기반보호는 국가의 주요기반시설을 지정하고 시설에 대한 취약점 점검과 보호대책을 수립하는 것으로 기반시설에 대한 취약점진단 및 정보보호컨설팅을 수행하기 위한 전문업체를 지정하고 자격을 부여하고 있다. 이와 같은 유사한 제도는 미국과 영국도 시행하고 있으며, 국가 주요기반시설에 대한 방어 및 대책수립을 지원하고 보안커설팅을 제공하기 위하여 'Safe Program'과 'IT Check Health Service'를 마련하여 제공하고 있다[8].

2.1 정보보호 기반구축을 위한 시행제도

2.1.1 주요정보통신기반보호(CIIP)

우리나라에서는 주요기반시설들을 보호하기

위해 2001년부터 '주요정보통신기반보호제도'를 설립하고 운영하고 있다. 국가의 주요정보통신기반시설을 해킹 등 위협으로부터 보호할 수 있도록 취약점 분석·평가, 보호대책 수립 등에 필요한 기술을 지원하여 동 기반시설의 안정적인 운영을 도모하기 위한 제도이다. 기반보호시설 선정은 국가/공공뿐만 아니라, 민간이 운영/관리하는 정보통신기반시설을 포함하여 전자적 침해행위 발생시 국가안보, 국민의 기본생활 및 경제안정에 중대한 영향을 미치게 되어 보호가 필요하다고 인정되는 정보통신기반시설을 지정하게 된다.

기반시설로 지정된 기관 또는 시설에서는 지정된 시설의 전반에 걸쳐 정기적 혹은 필요시 취약점점검을 실시하여야 한다. 그리고, 시설내 중요 정보의 기밀성, 무결성, 가용성을 유지하고 영향을 미칠 수 있는 전자적인 침해행위 등 다양한 위협요인을 파악하고 보호대책을 수립하여야 하며 안정성 및 정보의 신뢰성을 확보하여야 한다.

2.1.2 정보보호안전진단(ISCS)

정보보호 안전진단 제도는 주요 정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 관리적·기술적·물리적 정보보호지침(안전진단기준)를 이행하고, 안전진단수행기관으로부터 안전진단을 받음으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다. 2003년 인터넷 대란 이후 인터넷 인프라와 기업들의 보안점검을 의무화("정보통신망이용촉진및정보보호등에관한법률" 제45조(정보통신망의안정성 확보 등), 제46조의3(정보보호안전진단))하기 위하여 만들어져 2004년 말부터 시행되었다.

2.1.3 정보보호관리체계인증(ISMS)

정보보호관리체계인증은 2002년 4월 처음 시행되었다. 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화 하고 지속적으로 관리·운영하는 시스템 즉 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계(이하 "정보보호관리체계"라 한다)에 대하여 제3자의 인증기관(한국인터넷진흥원)이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도로 의무사항은 아니고 대상사업자가 자율적으로 신청하게 되어 있다[17].

이와 같은 제도 이외에도 행정안전부에서는 공공기관이 개인정보를 보유하는 신규시스템 구축사업, 기존시스템 변경사업, 개인정보파일을 다른 기관과 연계하는 사업 등의 시작에 앞서 개인정보영향평가를 실시하고 있다. 개인정보영향평가(Privacy Impact Assessment : PIA)는 정부의 각 기관이 컴퓨터시스템을 새로 설치할 때 개인정보가 유출될 가능성이 있는지를 점검하는 것으로 시스템 구축전에 개인정보 침해에서 안전한지 여부를 점검한다. 공공기관의 개인정보 영향평가는 현재 계류 중인 개인정보보호법이 국회를 통과하게 될 경우 의무적으로 수행하게 된다.

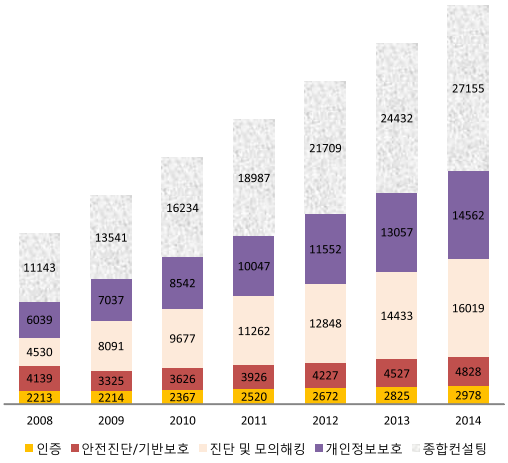
그리고, 또 행정안전부는 2009년말 'G-ISMS 인증지침'을 훈령으로 제정·고시한 데 이어, 시험인증을 위한 정보보호관리체계 적용을 실시하고 있다[14]. G-ISMS(Government-ISMS)는 행정기관의 정보보호 수준을 객관적이고 체계적으로 점검·관리하기 위한 제도로 전자정부법 시행령 개정과 더불어 진행되고 있다.

2.2 정보보호 컨설팅시장 현황

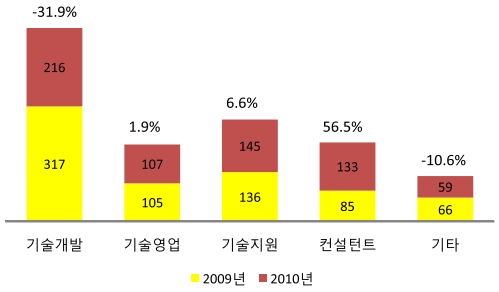
국내의 정보보안기업의 총 매출 실적은 2008년 738,879백만원에서 2009년도에는 807,223백만원(68,344백만원, 9.2%증가)으로 조사되었다. 우리나라의 정보보안컨설팅 산업이 자리를 잡고 활발한 업무수행을 하게 된 것은 전문업체지정제도가 크게 역할을 하였다. 2009년 '보안컨설팅' 분야는 DDoS 사태에 따라 인프라에 대한 보안 수요가 늘어났으며 개인정보보호 및 기업 내부정보보호의 중요성이 강조되고 있다. 정보보호사업 분야중에서 '보안컨설팅'분야의 매출액은 34,208백만원으로 2008년 매출액 28,064백만원보다 6,144백만원(21.9%) 증가하였으며, 국내 정보보호 시장 전체에서 차지하는 비중은 매년 소폭 증가하고 있다(2008년 3.8%->2009년 4.24%). 2014년까지 예상되는 연평균성장률(CAGR)은 15.2%[3]로 65,540백만원 규모로 성장할 것으로 전망되고 있다[6,7].

컨설팅 유형으로 보면 '진단 및 모의해킹'과 '개인정보보호' 컨설팅 부분의 매출이 전년 대비 크게 증가하였다. 이와 같은 증가는 1.25인터넷대란, 7.7대란 등의 이유도 있지만 여러 가지 정보보호제도들과 새롭게 준비되고 추진되는 행정안전부 등의 시행제도들 때문이라고도 볼 수 있을 것이다.

정보보호에 대한 인식의 전환과 함께 각종 법안과 제도의 신설로 인해 시장규모과 수요는 점차 증가할 것으로 예상되고 있다. 기업을 대상으로 한 분야별 채용 예상인력 조사결과도 이 같은 현실을 반영하고 있다. 그림 2에서 알 수 있듯이 정보보호관련 기업들을 대상으로 조사된 기업들의 2009년, 2010년 인력채용현황과 계획을 살펴보면 기술개발인력이나 타 인력들은 감소하거나 한자리수 증가인 반면에 컨설팅 인력의 경우 56.5%의 채용증가율을 보이고 있는 것으로 조사결과 나타나고 있다[7].



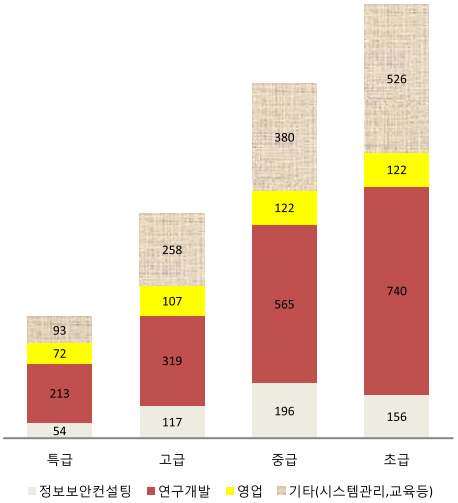
[그림 1] 보안컨설팅 매출전망(단위:백만원)



[그림 2] 지식정보보호 인력 채용계획(단위:명)

그리고 정보보호에 종사하고 있는 인력들의 직종에 따른 수준을 살펴보면 그림3과 같이 나타났다. 컨설팅관련 인력의 경우 특급 54(10.3%), 고급117 (22.4%), 중급 196(37.5%), 초급156 (29.8%)로 나타났으며, 연구개발직의 경우는 특급 213 (11.6%), 고급 319 (17.4%), 중급 565 (30.8%), 초급 740 (40.3%)로 나타나고 있다.

3) 2008년 조사된 2013년까지 보안컨설팅의 CAGR은 11.1%였음



[그림 3] 직종 및 수준별 인력현황(단위:명)

III. 지식정보보안 컨설팅전문업체 지정제도와 현황

3.1 관련법과 지식정보보안 컨설팅전문업체 지정제도

'정보통신기반보호법'의 제정 목적은 사이버테러리즘에 대비한 주요 정보통신기반시설의 보호대책을 수립·시행하여, 동 시설의 안정적 운용을 확보함으로써 국가의 안전과 국민생활의 안정을 보장하기 위함이다. 앞에서 살펴본 바와 같이 주요기반시설들을 지정하고 보호대책을 마련하도록 의무화하고 있다. 기반보호법은 정보통신기반보호에 대한 평가 기술 지원을 담당할 전문기관을 구성 운영하여 주요 정보통신기반시설의 지정과 정보통신기반시설의 취약성을 분석하고 위협요인을 평가하여 그 결과에 따른 보호대책 수립[9조]을 담고 있다. 행정, 방송통신, 금융, 에너지, 건설·.교통, 사회복지 등의 분야로 나누어 10개 중앙행정기관 산하 90개 관리기관, 126개 시설이 기반시설로 지정되어[5] 있으며 확대되고 있다.

기반시설의 취약점을 분석평가하기 위해서는 해당기관에서 전담반을 운영하거나 기반보호법[9조 2,3항]에 명시된 기관(한국정보보호진흥원, 정보공유·분석센터, 지식정보보안 컨설팅전문업체, 한국전자통신연구원)에서 실시할 수 있도록 규정되어 있다. 기관에서 규정에 맞는 전담반을 별도로 구성하는 것은 현실적으로 쉽지 않아 대부분의 경우 외부기관에서 컨설팅을 수행하고 있으며, 기반시설의 취약점 분석평가를 위해 '정보통신산업진흥법' 제 33조에 의한 지식정보보안 컨설팅전문업체 제도를 시행하고 있다[3,4].

3.2 지식정보보안 컨설팅전문업체 지정현황

지식정보보안 컨설팅전문업체는 2001년 9월 정보보호전문업체의 지정심사에 관한 고시지정에 따라 동년 11월 9개의 전문업체[4]가 신규 지정되었다. 2002년 10월 2차 지정심사에 따라 4개 업체[5]가 새로 지정되어 모두 13개 기관이 자격을 획득하게 되었다. 2003년과 2004년 2개회사가 회사사정 등으로 인해 지정취소 되고 2004년과 2005년 기한종료(3년유효)에 따른 재지정심사에서 3개 업체가 탈락하여 8개 업체[6]가 자격을 유지하였다. 양수·양도 규정과 절차에 따라 2005년 (주)시큐어소프트는 이니텍(주)으로 심사를 거쳐

4) 시큐아이닷컴(주), 마크로테크놀러지(주), (주)시큐어소프트, (주)안철수연구소, (주)에스티지시큐리티, (주)에스큐브, (주)에이쓰리시큐리티컨설팅, (주)인젠, (주)해커스랩

5) (주)인포섹, (주)안랩코코넛, (주)퓨처시스템, (주)한국IBM

6) 시큐아이닷컴(주), (주)시큐어소프트, (주)안철수연구소, (주)에스티지시큐리티, (주)에이쓰리시큐리티컨설팅, (주)인젠(주)인포섹, (주)안랩코코넛

자격을 양도하였고 이니텍(주)은 다시 2008년 롯데정보통신(주)으로 양도하였다. 2007년 재지정과 회사합병((주)안철수연구소, (주)안랩코코넛)으로 인하여 7개 업체가 자격을 유지하게 되었고 2010년 7월 (주)인젠시큐리티서비스가 (주)인젠으로부터 자격을 양도받아 현재 모두 7개 전문업체[7]가 지정되어 있으며 기한종료에 따른 재지정 심사(2010년 11월기한)가 해당 6개 업체를 대상으로 진행되었으며 모든 업체가 자격을 재인정 받았다[17].

전문업체들은 지정된 기반시설 및 일반기업들을 대상으로 보안컨설팅과 안전진단, 개인정보영향평가, 보안진단, 취약점평가분석, G-ISMS 등의 사업에 주도적으로 참여하고 있다.

Ⅳ. 지식정보보안 컨설팅전문업체 지정기준

4.1 지정기준

지식정보보안 컨설팅전문업체 지정은 지식경제부에서 정보통신산업진흥법 제 33조(지식정보보안 컨설팅전문업체의 지정)에 의거하여 보안컨설팅 능력을 보유한 업체(법인)를 규정에 따라 지정하게 되어 있다[3].

컨설팅전문업체의 지정기준[8]은 기본요건과 업부수행능력 세부평가기준으로 나눌 수 있으며, 기본요건(인력요건, 자본요건, 설비요건, 정보보호관리규정)을 모두 만족하고 업부수행능력평가(경험, 전문화정도, 신뢰도, 기술개발실적, 종합심사, 기타)를 70점이상 획득하면 된다. 전문업체 자격은 3년간 유효하며 기한만료전에 재지정 심사를 실시하여 적격한 업체에게는 다시 자격을 부여하고 있다. 필요시 심사를 거쳐 양도·양수도 가능하다[4].

4.2 지정 요건 및 개선사항

현재 운영되고 있는 절차와 심사기준은 2001년 수립된 이래 큰 변화없이 현행 유지되고 있다. 그 동안 제기된 문제점을 반영하고 변화되는 산업환경에 맞추어 검토와 개정이 필요하다.

기본요건은 4가지 항목으로 분류되어 있으며 내용은 표1과 같다.

기본요건의 경우 기준만 충족되면 자격을 부여받는 항목으로 구성되어 있다. 기준요건과 개선점을 살펴보면 다음과 같다.

[표 1] 지식정보보안 컨설팅전문업체 지정 기본요건

항 목	내 용
인력요건	기술인력 15인(고급 5명이상)
자본요건	납입자본금 20억원이상
설비요건	신원확인 및 출입통제 설비 구비 취약점분석 및 보호대책수립 업무지원 설비 기록 및 자료의 안전한 관리 설비
규정요건 (정보보호관리규정구비)	업무수행구역보호대책 인력에 대한 보호대책 문서 및 전산자료에 대한 보호대책

인력요건의 경우 일반인력의 자격부여가 대학 유관관련학과 졸업이상이면 요건이 되므로 전문성이 떨어지고 있어 강화가 필요하고 실제 능력을 지닌 해킹능력자들에 대한 인력인정요건의 추가도 검토가 필요하다. 설비요건의 경우 취약점 점검 업무환경의 변화로 인하여 원격점검이 거의 진행되지 않고 있어 설비요건의 개정이 필요하다. 현재 취약점수행 대상 시설에서 직접 휴대용 장비를 이용하여 수행되는 경우가 많이 늘어났으므로 이에 대한 문서 및 전산자료에 대한 보호대

7) 시큐아이닷컴(주), (주)안철수연구소, (주)에스티지시큐리티, (주)에이쓰리시큐리티컨설팅, 롯데정보통신(주), (주)인젠시큐리티서비스

8) 정보통신산업진흥법 제 33조~제 39조에 규정, 동법 시행규칙 제 7조 ~제 17조

책 강화가 필요하며 전문업체의 내부자료 보안에 관련된 강화된 설비요건과 보호대책 마련도 시급히 필요하다.

업무수행능력 세부평가 기준의 경우도 업체들 간의 실제 차별화된 심사를 위한 항목들로 개정이 필요하다. 현재의 기준으로는 실질적인 업무능력평가가 되기 어렵고 일정 기준을 충족하는 것은 업체의 의지만 있다면 크게 어렵지 않다.

[표 2] 지식정보보안 컨설팅전문업체 업무수행능력 세부평가 기준과 개선방안

항 목		개선 및 검토
경험	최근 3년간 정보보호컨설팅실적	- 실제 투입된 인력 산정필요 - 실적기준의 상향이나 기간 조정필요
전문화 정도	고급기술인력의 수	- 고급인력의 수와 병행하여 해킹전문가 보유 신설 필요 - 특수분야 경력자 항목 검토 필요 - 총매출액 대비 정보보호 매출액 비율 항목 삭제 검토필요
	기술인력중 특수분야 경력자의 수	
	총매출액대비 정보보호분야 매출액 비율	
신뢰도	부채비율	- 추천서, 상훈실적 항목 삭제 검토필요
	자기자본이익율	
	추천서의 수	
	상훈실적	
기술 개발 실적	정보보호분야정부과제수행실적	- 취약점 점검도구나 컨설팅도구 개발 실적 추가필요 - 정보보호분야는 너무 광범위하므로 분야를 세분화할 필요 있음
종합 심사	기술책임자의 자질과 경험	- 기술책임자분만 아니라 전체 기술인력의 자질을 관리/평가할 수 있는 방법필요 - 신청업체 정보보호대책 세부요건 강화필요 - 컨설팅을 수행한 기업의 만족도(평가) 산정필요 - 정보보호전문지식 항목의 현실적인 세부검사 항목 마련필요
	신청업체 자체의 정보보호대책	
	컨설팅방법론	
	정보보호전문지식	
기타	벤처기업부가점	- 벤처기업부가점 항목 삭제 검토필요
	조달법령에 따른 부정당업자 지정여부	

먼저, 경험항목을 살펴보면 대부분의 업체가 충족하기 쉽다. 산정기간을 줄이거나 기준금액(3년간 20억원의 실적)을 상향하는 것이 필요하다. 전문화정도의 경우는 고급인력의 수만으로 해당 업체의 전문화를 판단하기 어려우므로 고급인력 뿐만이 아닌 전체인력으로 확대하고 전문성을 실질적으로 점검하기 위한 새로운 방안을 모색할 필요가 있다.

해킹그룹의 운영이나 해킹기술개발, 대회입상과 같은 사항들도 점검항목으로 추가하여 종합적으로 판단하는 것이 필요하다. 특수분야 경력자의 보유도 초기 시행시 기술인력의 부족으로 인해 추가된 항목이므로 삭제가 필요하다. 또, 총매출액 대비 정보보호분야 매출액 비율은 대기업이나 타사업을 병행하여 하고 있는 기업에게는 불리한 항목이므로 폐지도 타당할 것으로 보인다. 신뢰도 항목에서는 추천서와 상훈실적이 실질적인 컨설팅전문업체의 자질을 평가하는 것과는 크게 관련이 없으므로 삭제가 타당할 것이다.

기술개발실적 항목에서는 정보보호분야 정부과제 수행실적이 너무 광범위하므로 보안컨설팅과 관련된 분야로 세분야해서 수정하거나 삭제를 검토하는 것이 타당할 것으로 보인다. 종합심사 항목은 인터뷰와 발표 등으로 판정을 하는 영역으로 보다 객관적인 능력평가를 위해 상세한 판단기준들을 추가 개발할 필요성이 있다. 세부항목별로 살펴보면 기술책임자만을 판단하여 업체의 인력 자질을 판단하는 것은 현실적으로 어려우므로 전체 기술인력의 자질을 관리할 수 있는 평가방안 마련이 필요하다. 그리고, 지식정보보안 컨설팅전문업체들의 자체 내부 보안규정과 시행이 현실적으로 시대에 떨어져 있는 부분들이 있으므로 삭제와 추가 등의 개정이 필요하다. 전문업체가 수행한 사업에 대한 만족도를 평가받아 반영하는 방안도 고려해 볼 수 있으며, 정보보호 전문지식을 평가하는 항목의 경우 현실적으로 맞

지 않아 이를 다른 항목으로 대체하거나 현실적인 평가방안 개발이 필요할 것으로 판단된다.

4.3 정책 및 업무수행환경 개선사항

4.3.1 정보보호 제도관리 일원화

정보통신기반보호법에 규정되어 있던 주요정보통신기반시설 및 지식정보보안 컨설팅전문업체와 관련된 법률과 시행령, 시행규칙, 고시는 정보통신부의 행정조직 개편에 따라 행정안전부는 정보통신기반보호법에 근거한 주요정보통신기반시설의 지정 및 관리 총괄업무를 맡고 지식경제부에서는 지식정보보안 컨설팅전문업체의 지정업무를 담당하고 있다. 또, 주요 정보통신망기반시설들은 방송통신위원회에서 관할하고 각 중앙행정기관은 산하 주요 기반시설들을 관리하고 있다. 전문업체지정은 지식경제부로 이관되었으며 여러법률에 있던 관련조항들을 '정보통신산업진흥법'에 포함하여 제정되었다. 이와 같이 현재 정보보호 관련된 제도와 관리가 지식경제부, 행정안전부, 방송통신위원회로 나누어져 있어 효과적인 시행과 관리를 위해서는 빠른 시일 안에 단일화가 필요하다.

4.3.2 인력 및 수행실적 통합관리

현재 업체 지정과 재지정시 필수적으로 제출되는 개인별 컨설팅 참여이력과 교육관리 카드 등 관련 서류들은 심사를 위해 각 업체별로 관리되고 있다. 심사시 필수적으로 제출하게 하고 있는데 본래의 취지와는 다르게 형식적으로 지나칠 수 있다. 신고된 기술인력들의 컨설팅 참여이력, 실적과 교육이력 등을 시스템으로 구축하여 통합관리하는 방안이 필요하다. 그리고, 이직이나 퇴사인력의 사후관리도 일정기간동안 필수적으로 이루어져야 할 것이다. 그리고, 해킹 및 방어, 취약점 점검 등 기술개발을 위한 지원과 해당 인력의 양성을 지원할 수 있는 방안도 검토가 필요하다.

4.3.3 현실적인 컨설팅단가 반영

보안컨설기술팅 사업의 경우는 인력이 가장 큰 역할을 담당하게 되지만 현재, 낮은 임금단가와 불확실성으로 인하여 인력들의 이직률이 높다. 그리고, 컨설팅 업무가 상시 있지 않은 관계로 인해 다수의 사업이 동시에 진행될 경우 경험이 적은 인력이 투입되는 경우가 생기게 된다. 현재의 수행사업에 비해 많은 기술인력을 유지할 수 없는 점을 감안해 참여율 개선방안도 필요할 것으로 보인다. 그러나, 무엇보다도 전문업체들이 제대로 된 대가기준 반영이 필요하다. 보안컨설팅 전문인력은 유관학과 졸업, 보안업체 경력을 구비하고 업무상 신원조회를 필해야 하는 등의 요건으로 희소성이 있는 반면에 IT 범용인력에 적용되는 SW대가 기준으로 책정되어 있어 공공기관의 예산이 작고 경쟁으로 인한 저가 수주로 인해 결국은 양질의 서비스 제공이 어려워지고 있다.

4.3.4 품질관리 방안

현재 보안컨설팅은 소수 인력에 의존하는 경우가 많다. 기술인력들의 경험과 노하우가 축적되거나 관리되고 있지 않고 있으며, 수행인력에 따른 업무 수행 결과물의 품질이 차이가 있다. 경험이 부족한 인력의 참여로 인해 전문업체에서 수행된 안전진단이나 보안컨설팅의 실효성도 지적되고 있다. 3년간 자격인정 기간이 지난 후 기본요건과 형식적인 업무수행능력평가로는 전문업체의 수준을 평가하기 어려운 현실을 감안해 평가기준의 개정으로 중간점검과 실질적인 능력을 점검하거나 관련 부처나 전문기관에서 컨설팅

의 품질을 상시 관리하기 위한 방안 마련도 필요하다.

4.3.5 시장관리 및 경쟁력 강화

근래들어 기존업체와 신규로 시장에 진입하려는 업체들의 입장이 대립하고 있다. 현재 기준은 대기업보다는 벤처, 중소기업에 유리하게 되어 있다. 진입장벽을 재검토할 필요는 있겠지만 무분별한 업체의 증가는 과열경쟁으로 이어질 수 있으므로, 시장의 규모에 맞는 적정한 수의 업체 유지가 필요하다. 기본요건강화와 수행능력 평가 기준의 강화로 기존 업체의 경쟁력을 강화하고 미달하는 업체에 대하여서는 과감한 퇴출방안을 마련하는 등의 조치도 필요하다.

V. 결 론

기존 제도의 확대와 개인정보영향평가, G-ISMS등 새로운 제도의 시행으로 인해 보안컨설팅 시장은 점차 확대될 것으로 기대되고 있다. 이를 반영하듯 컨설팅분야의 CAGR[9]과 채용인력의 수도 높아지고 있다. 아직은 작은 시장규모와 낮은 인력 대가기준으로 인한 인력관리와 수행결과의 낮은 품질 등 여러 가지 문제들이 나타나고 있어 정부의 제도개선과 지속적인 시장 지원책도 필요할 것으로 보인다. 그러나, 지식정보보안 컨설팅전문업체들의 지속적인 기술개발과 양질의 인력관리를 위한 투자와 노력도 반드시 필요하다.

본 논문에서는 현행 실시되고 있는 지식정보보안 컨설팅전문업체 지정제도와 운영에 대하여 살펴보고 컨설팅전문업체의 사업영역과 시장현황에 대하여 분석하였다. 그리고, 컨설팅전문업체의 자격을 부여하는 기준요건들을 살펴보고 개선사항들을 제시하였다. 제시된 의견들은 지식정보보안 컨설팅전문업체의 보다 개관적이고 실질적인 능력평가를 위한 참고자료로 활용되고 나아가서는 전문업체의 경쟁력 향상과 유지에 도움이 될 것으로 기대한다.

9) 보안컨설팅분야 CAGR, 2008년 자료: 11.1%(2007-2013), 2009년 자료:15.2% (2008-2014)

참 고 문 헌

[1] 정보통신기반보호법, 2009.8.23
[2] 정보통신기반보호법, 시행규칙 2008.3.3
[3] 정보통신산업진흥법, 2010.9.23
[4] 정보통신산업진흥법, 시행규칙 2009.8.28
[5] 2010 국가정보보호백서, 2010.4
[6] 국내 정보보안산업 시장 및 동향조사, 한국정보보호진흥원 연구보고서, 2008.12
[7] 국내 지식정보보안산업 시장 및 동향조사, 한국인터넷진흥원 연구보고서, 2009.12
[8] 정보보호컨설팅전문업체 지정기준 개선연구, 한국정보보호진흥원 연구보고서, 2003.8
[9] 오병민, 정보보호안전진단 5년 그 현주소는? 보안뉴스, 2009.1.22
[10] 오병민, 정보보호안전진단평가, 허술한 관리로 '구멍', 보안뉴스, 2010.6.24
[11] 오병민, 허술한 '정보보호안전진단', DDoS 공격 무방비, 보안뉴스, 2009.10.13.
[12] 김정완, 보안컨설팅시장, 악순환 고리 끊어야 산다, 보안뉴스, 2009.2.17
[13] 김정완, 국내 정보보호컨설팅의 현주소, 보안뉴스, 2009.2.17
[14] 이유지, 전자정부 정보보호관리체계(G-ISMS) 인증제 도입 급물살, 디지털데일리, 2010.1.11
[15] 김정완, 대기업 보안컨설팅 시장 진출 과연 보안시장 확대인가?, 보안뉴스, 2009.2.19
[16] 이상균, 지경부-보안업계 정보보호업체 추가 지정 놓고 대립, 이투데이, 2009.10.26.
[17] 한국인터넷진흥원 인프라보호관련 주요사업 소개자료 , http://www.kisa.or.kr/business/public /main.jsp

저 자 소 개

정 연 서(Youn-seo Jeong)

1996년 2월: 충북대학교 컴퓨터공학과 석사
2001년 8월: 충북대학교 컴퓨터공학과 박사
2001년 8월～현재: 한국전자통신연구원

<관심분야> 네트워크/정보보호 시험평가, 정보보안, 보안성평가

박 진 섭 (Jin-sub Park)

1991년 2월: 중앙대학교 컴퓨터공학과 박사
1988년 3월~현재: 대전대학교 컴퓨터공학과 교수

<관심분야> 정보보호관리체계, 시스템모델링 및 성능평가, 컴퓨터네트워크