Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.545

국내 정보보호 교육체계 연구*

김 동 우,[1†] 채 승 완,[2] 류 재 철[1‡]
[1]충남대학교 컴퓨터공학과, [2]한국인터넷진흥원

A Study on Domestic Information Security Education System*

Dong-woo Kim,[1†] Seung-woan Chai,[2] Jae-cheol Ryou[1‡]
[1]Chungnam National University, [2]Korea Internet & Security Agency

요 약

최근의 사이버 공격은 내부 직원을 목표로 하거나 불특정 다수의 PC를 이용하는 등 지능화, 대규모화 되고 있어 기술적인 보안대책만으로 대응하는데 한계가 있으며, 관련 인력이 중심이 되는 종합적인 대책이 필요하다. 그러나 정보보호 전문 인력을 양성하는데 있어서 근간이 되는 국내의 정보보호 교육체계는 정보보호 교육 중장기 계획 부재, 교육 프로그램에 대한 검증 부족, 교육기관 간의 정보 교류 부재 등 여러 가지 문제점을 가지고 있다. 본 논문에서는 국내 정보보호 교육체계의 문제점을 해결하고 사이버 정보보호 환경을 개선하기 위한 정보보호 교육 발전 방안을 제안한다. 본 논문에서 제안하는 정보보호 교육체계 발전 방안은 국가 정보보호 교육 마스터플랜의 기획 및 추진, 정보보호 교육 프로그램 인증제도 도입, 정보보호 전문인력 DB 운영, 정보보호 전문 인력에 대한 다양한 혜택 개발 등의 세부 방안을 포함한다.

ABSTRACT

There is a limitation on counteracting recent cyber-attacks with only technical security measures because they become more intelligent and large-scale to aim at employees instead of systems directly or to be conducted with unspecified multiple PCs. Thus, comprehensive measures revolved around related manpower are necessary to deal with them. However, domestic information security education system which is the base of professional manpower training lacks medium-and long-term plans for information security education, verification of education programs, and information sharing among educational institutions. This paper suggests information security education development plans for resolving problems on domestic education systems and improving cyber information security environment such as a national information security education master plan, certification system introduction of education programs, and professional manpower database management.

Keywords: Information Security, Education System, Professional Manpower Training

I. 서 론

최근 들어 지능화, 대규모화 되고 있는 사이버 공격에 대응하기 위해서 보다 근본적인 보안대책의 수립을 요구하는 목소리가 높아지고 있다. 특히 최근 유행하고 있는 APT(Advanced Persistent Threat) 공격은 단순히 기술적인 공격뿐만 아니라, 조직, 사람, 정보 등을 망라한 사회공학적 공격을 동반해서 이루어지고 있다. 이는 곧 그 동안 단기적인 처방 중심으로 수립된 보안 대책으로는 최신 해킹 공격을 막아낼 수 없음을 의미한다. 예를 들어 DDoS 공격 발생 이후에 DDoS 대응 장비가 특수를 이룬다거나 개인정보보호

접수일(2013년 1월 16일), 수정일(2013년 3월 29일), 게재확정일(2013년 4월 1일)
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No. 2012-0006419)
† 주저자, scotty@home.cnu.ac.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

법 시행 직전 개인정보보호 솔루션 판매의 급격한 성장 등, 일시적이고 단기적인 대책으로는 최신의 해킹 공격을 막아내는데 한계가 있다.

'100% 완벽한 보안은 없다'라는 명제에 누구나 동의를 한다 하더라도 공격 기술이 발전함에 따라 방어 기술도 함께 발전해온 것이 사실이다. 국내의 경우만 하더라도 지난 몇 해 동안 정보보호 기술에 대한 투자는 꾸준히 증가 추세에 있으며, 많은 기관이나 기업이 안티바이러스나 침입차단시스템과 같은 기본적인 보안 시스템을 이미 보유하고 있는 상태이다[1]. 그럼에도 불구하고 사이버 침해사고가 꾸준히 증가하고 있다는 사실은 단순 기술 위주의 보안대책이 아닌 보다 종합적인 보안대책이 필요하다는 주장을 뒷받침해준다.

앞서 언급한 APT 공격의 대표적인 사례라고 할 수 있는 2011년 4월 발생한 농협 해킹 사건이나 같은 해 발생한 미국의 유명 보안업체인 RSA를 대상으로 한 해킹은 모두 내부 직원을 목표로 해서 이루어졌다. 즉, 기술적인 보안대책과 함께 조직내에서 업무를 수행하고 있는 인력의 보안의식 및 대응이 공격 방어에 있어서 매우 중요한 부분을 차지하고 있음을 알 수 있다. 그러나 국내의 경우 인력 양성을 위해서 필요한 정보보호 교육을 실시하고 있는 기업은 여전히 전체 기업의 20%에도 미치지 못하고 있는 실정이다[1]. 더욱이 최근 들어 보안 컨설팅 사업이 폭발적으로 증가하고 있음에도 정보보호 전문 업체들은 전문 인력의 부족으로 인해서 사업을 포기하는 상황이 발생하고 있다[2]. 몇 년 전부터 정보보호 전문 인력의 부족 현상이 문제로 지적되어 오고 있으나, 여전히 이에 대한 해결책이 없음을 보여주고 있는 단적인 예라 할 수 있다.

첨단의 해킹 공격에 대응하기 위해서는 정보보호 전문 인력의 확충과 일반인의 정보보호 의식 향상이 동시에 요구됨에도 불구하고, 국내 실정은 2가지 부분 모두에서 매우 부족한 현상을 보이고 있다. 이와 같은 인력 문제가 발생하는 데는 여러 가지 이유가 있을 수 있지만 국내에서 체계적인 정보보호 교육이 이루어지지 않고 있다는 사실도 주요한 원인으로 볼 수 있다.

미국의 경우, 이미 2009년부터 국가적인 차원에서 정보보호 교육에 대한 종합적인 계획을 수립하여 시행하고 있다[3]. 국내에서도 행정안전부 중앙공무원교육원, 한국인터넷진흥원 등에서 정보보호 관련 교육을 제공하고 있고, 다수의 민간 정보보호 교육기관이 운영 중에 있다. 그러나 미국과 같이 국가적인 차원의 마스터플랜이 존재하지 않는 가운데, 다양한 교육 프로그램의 부재, 정보보호 교육기관의 정보 교류 부재 등으로 인해 큰 실효를 거두지 못하고 있는 실정이다. 또한 대부분의 정보보호 교육이 취업준비생이나 업무 담당자를 대상으로 하고 있어, 초·중·고 학생을 비롯한 일반인의 정보보호 의식 향상에는 도움이 되지 못하고 있다.

점점 지능화되고 복합적으로 행해지는 최근의 해킹 공격 기술에 대응하기 위해서는 정보보호 전문 인력의 양성과 함께 일반 사용자의 정보보호 의식 향상이 필수적이다. 그리고 이와 같은 인적인 부분의 향상을 위해서는 체계적이고 계획된 교육 프로그램이 반드시 필요하다.

이에 따라 본 논문에서는 국내의 정보보호 수준 향상을 위한 정보보호 교육 체계를 제안하고자 한다. 제안하고자 하는 정보보호 교육 체계는 정보보호 업무와 직간접적으로 관련되어 있는 업무 담당자뿐만 아니라 초·중·고 학생 및 일반인도 대상으로 하는 다양한 대책들을 포함한다.

본 논문의 구성은 다음과 같다. 2장에서 미국의 정보보호 교육 체계 현황 및 국내 정보보호 교육 체계 현황을 분석하고, 3장에서 국내 정보보호 교육 체계의 문제점을 기술하며, 4장에서는 3장에서 도출된 문제점을 해결할 수 있는 체계를 제안한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련 동향 분석

2.1 미국의 정보보호 교육체계

2.1.1 NICE 개요

지속적으로 사이버보안의 중요성을 강조해오고 있는 미국 정부는 사이버보안 수준 강화에 있어서 정보보호 교육이 매우 큰 역할을 차지한다는 판단 하에 2011년 8월 '사이버보안 교육을 위한 국가 계획(NICE: National Initiative for Cybersecurity Education)'을 발표하였다[4].

국토안보부(DHS: Department of Homeland Security), 국방부(DoD: Department of Defense), 국가안보국(NSA: National Security Agency) 등 20여개 정부부처가 참여하고 있는 NICE 계획은 정보보호 업무 종사자나 전공자뿐만 아니라 초·중·고 학생 및 일반인에 이르기까지 전국민을 대상으로 정보보호 기술 및 의식 수준의 향상을 목표로 하고 있다. 이러한 정보보호 교육 강화의 궁극적

인 목적은 안전한 디지털 국가의 유지이다. 이와 같은 목표를 달성하기 위해 설정한 세부목표는 다음과 같다.

○ 세부목표 1: 사이버 위협에 대한 미국민의 인식 수준 제고

○ 세부목표 2: 정보보호 업무에 참여할 수 있는 숙련된 인재 확보

○ 세부목표 3: 정보보호 업무에 있어서 국제경쟁력 확보 및 유지

2.1.2 NICE 추진체계

NICE 계획의 전체적인 운영은 국토안보부에서 주도하고 있으나 실무적인 내용은 미국 국립표준기술연구소(NIST: National Institute of Standards and Technology)에서 수행하고 있다. 앞서 기술한 3가지 세부목표를 달성하기 위해서 〔그림 1〕과 같이 사이버보안 인력구조 전략 수립을 중심으로 4개의 프로그램을 운영하고 있는데 각 프로그램별 주요 내용은 다음과 같다.

〔그림 1〕 NICE 추진체계

○ 프로그램 1(국가 사이버보안 의식 향상): 국가 사이버보안 의식 향상을 위해서 국토안보부에서는 '인터넷 사용과 사이버보안 인식 향상을 위한 대국민 캠페인 활동 및 강좌'를 제공한다. 세부목표 1과 연관된다.

○ 프로그램 2(사이버보안 교육): 교육부와 국가과학재단에서 주도하며, 사이버보안 교육 프로그램을 개발하여 유치원 및 초·중·고 학생에게 제공한다. 세부목표 2와 연관된다.

○ 프로그램 3(사이버보안 인력 구조 전략): 세부목표 3과 연관되며, 사이버보안 인력 관리 프레임워크 확립에 중점을 둔다. 이를 위해서 사이버보안 인력의 직업숙련도 평가, 미래 사이버보안 요구사항 예측을 위한 사례 제공, 취업 및 직업 유지를 위한 국가 전략 정의 등의 업무를 수행한다. 세부목표 3과 연관된다.

○ 프로그램 4(사이버보안 인력양성 및 훈련): 프로그램 3과 함께 세부목표 3과 연관된다. 주로 연방기관에 근무하는 사이버보안 인력의 훈련 및 업무 능력 향상을 목표로 한다. 프로그램 4는 다시 〔표 1〕과 같이 4개의 영역으로 나뉜다. 방첩교육이 포함되는 등 사이버 보안 전문인력에 보다 특화된 프로그램임을 알 수 있다.

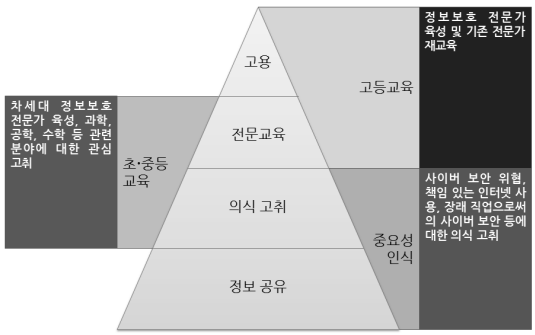
〔표 1〕 NICE 프로그램 4 구성

구분	주관기관	주요업무
1영역	국토안보부, 연방 CIO 위원회	일반 IT 사용 교육
2영역	국방부, 국토안보부	IT 인프라, 운영, 관리, 정보보증 교육
3영역	NCIX, 법무부, 국방부(DC3), 국토안보부(USSS)	관련 법 및 방첩교육
4영역	국가안보부	사이버보안 운영 특성화 교육

※ CIO: Chief Information Officer (최고정보책임자)
※ NCIX: National Counterintelligence Executive (방첩국)
※ DC3: DoD Cyber Crime Center (국방부 사이버 범죄 센터)
※ USSS: DHS US Secret Service (국토안보부 미국 비밀서비스)

2.1.3 NICE 추진전략

NICE 계획은 〔그림 2〕에서 보는 바와 같이 일반 정보보호 교육에서부터 취업 교육에 이르기까지 그 대상이 다양하다. 일반인 대상으로는 정보보호 관련 정보 공유 및 정보보호 의식 고취에 중점을 두고 있으며, 유치원 및 초·중·고 학생에게는 정보보호의 근간이 된다고 할 수 있는 과학, 기술, 공학 및 수학 관련 교육을 강조하고 있다. 또한 대학·대학원생 및 정보보호 관련 업무 종사자를 대상으로 보다 전문적인 교육을 제공한다.



〔그림 2〕 NICE 계획 추진전략

이와 같은 추진전략을 통해서 미국 정부가 얻고자 하는 기대효과를 앞서 살펴본 3개의 세부목표와 대비하여 살펴보면 〔표 2〕와 같다.

NICE 계획의 3가지 세부목표 가운데, 국가안보국(NSA) 등 정보보호와 직접적으로 관련이 있는 정부기관에서 특히 관심을 가지고 있는 사항은 국제경쟁력 확보 및 유지이다. 이는 숙련된 정보보호 전문가 육성이 뒷받침 되지 않는 상태에서 기술적 방안만으로는 더 이상 사이버안전을 충분히 보장할 수 없다는 관련 기관들의 위기의식에서 시작된 것이다. 미국에서도 정보보호 관련 직종은 새롭게 떠오르고 있는 분야로써, 여러 가지 면에서 미성숙한 분야이다. 직무에 대한 정의가 기관이나 회사별로 다른 경우가 많고, 관련 인력의 취업이나 경력 관리, 재교육 등이 미비한 실정이다. 이런 상황을 개선하기 위해서 NICE 계획에서는 인적 자원 관리 측면에서의 정보보호 프레임워크 개발을 진행하고 있다. 현재 진행중인 정보보호 인력 관리 프레임워크 개발 계획의 내용을 살펴보면 〔표 3〕과 같다.

정보보호 인력 관리 프레임워크에는 정보보호 분야 종사자에 대한 교육 프로그램도 포함되는데, 특히 교육 프로그램의 표준화에 역점을 두고 있다. 교육도구, 교육 방법론 등을 체계화 하고 공공 부문과 민간 부문

〔표 2〕 NICE 계획의 기대효과

세부목표	기대효과
사이버 위협에 대한 미국민의 인식 수준 제고	온라인 위협에 대한 일반국민의 지식수준 향상
	보안위협에 대한 이해 증진 및 지식수준 향상
	사이버보안 관련 자료제공
정보보호 업무에 참여할 수 있는 숙련된 인재 육성	유치원 및 초·중·고 교육 과정에서 과학, 기술, 공학, 수학 교육 강화
	고교 교육과정에서 컴퓨터 과학 교육의 양적·질적 수준 향상
	컴퓨터 및 IT 관련 학과(대학·대학원)에서 정보보호 관련 커리큘럼 확대
	대학원의 정보보호 관련 연구 및 개발 지원
정보보호 업무에 있어서 국제경쟁력 확보 및 유지	국제경쟁력 있는 정보보호 인력 양성 프레임워크 개발
	사이버보안 훈련 과정 확대
	취업, 자격증 및 경력관리 활성화 방안 연구

〔표 3〕 정보보호 인력관리 프레임워크 개발 계획

일정	내용
2012년	정보보호 관련 직무 표준화 및 표준화 내용의 연방기관 적용
2013년	정보보호 전문가에게 필요한 기술의 기준지표 정의
2015년	기타 정부기관에서 정보보호 관련 직무표준 적용
	민간 부문에서 정보보호 관련 직무표준 적용
	NICE 계획 시행 이후 배출된 정보보호 인력의 수준 측정
	정보보호 전문인력 20% 확대
	정보보호 자격증 제도 활성화

의 정보 교류를 적극 장려함으로써 내실 있는 정보보호 전문 인력 교육이 되도록 노력하고 있다. 이와 동시에 교육의 효과를 극대화하고 전문 인력의 수준 검증을 위해서 자격증 제도를 정비할 계획이다.

2.1.4 US 사이버 챌린지

NICE 계획 외에도 미국 정부는 다양한 형태의 정보보호 교육 활동을 수행하고 있는데, 그 중 하나가 2010년 시작된 US 사이버 챌린지(USCC: US Cyber Challenge)이다. 1만명의 정보보호 전문인력 확보를 목표로 운영되고 있는 민관 합동 정보보호 전문인력 육성 프로그램인 USCC는 국가 정보보안 감사위원회(NBISE: National Board of Information Security Examiners)가 주도하고 있다. 고등학생 및 대학(원)생을 대상으로 운영되고 있는 USCC의 핵심 프로그램은 여름방학 기간 동안 운영되는 사이버 캠프이다.

매년 7, 8월, 2개월 간 운영되는 사이버 캠프에는 온라인 경쟁에서 승리한 고등학생 및 대학(원)생이 참가할 수 있는데, 대게 260-280명에게 참가할 수 있는 기회를 준다. 참가자들은 정부기관 및 산업체의 정보보호 전문가로부터 보안 심화 교육을 받게 된다. 모든 학생은 무료로 캠프에 참가하며, 경비는 마이크로소프트사 등 기업체의 기부를 통해서 해결하고 있다. 또한 캠프 종료후에는 산업체 시찰 및 취업 기회가 주어진다.

이 제도의 성공은 다른 나라에도 영향을 끼쳐 영국 정부는 이 제도를 벤치마킹하여 유사한 프로그램을 시행하고 있다.

지금까지 살펴본 바와 같이 미국 정부는 자국의 사

이버 보안 수준 향상을 위해서 정보보호 교육의 강화를 가장 중요한 요소로 파악하고 이를 위해 정부 차원에서 많은 노력을 기울이고 있다. 미국 정부의 정보보호 교육 계획은 정보보호 전문 인력의 확대 및 수준 강화에 중점을 두면서 동시에 전국민의 정보보호 의식 제고를 목표로 하고 있다. 날로 심각해지는 사이버 보안 위협에 대처하는데 있어서 가장 중요한 대응 수단은 바로 인력임을 보여주고 있다. 종합적인 정보보호 교육 체계가 미비한 국내의 경우도 현재 정보보호 교육 현황을 점검하고 개선점을 찾아야 할 시점이다.

2.2 국내 정보보호 교육 현황 분석

2.2.1 국내 정보보호 전문 인력 현황

국내 정보보호 교육의 현황을 분석하기에 앞서 정보보호 전문 인력의 구성 현황에 대해서 살펴보고자 한다.

〔표 4〕를 보면 2011년도 정보보호 관련 사업체에 종사하는 인력은 모두 26,458명이다. 이 가운데 IT 관련 전공자가 16,924명이지만 정보보호 관련 학과 전공자는 1,603명에 불과하다. 또한 인문사회 등 비 IT 학과 전공자가 9,534명에 이르는 것으로 나타났다〔5〕.

〔표 4〕 국내 정보보호 인력 현황(2011년) (단위:명)

구분		인력 현황	
IT 관련학과	정보보안(호)학과	1,603	16,924
	전자, 통신, 컴퓨터 관련 학과	15,321	
인문사회 등 비 IT 학과		9,534	
합계		26,458	

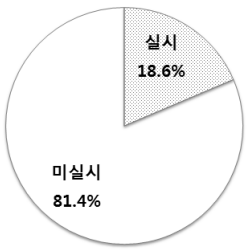
현재 국내에서 정보보호 업무에 종사하는 인력 가운데 비전공자가 많은 부분을 차지하고 있음을 알 수 있다. 대학 교육에서 배출하는 전공자의 급격한 증가를 기대하기 어렵다는 점을 감안할 때, 대학 졸업 이후에 이루어지는 정보보호 교육의 중요성을 알 수 있다.

한편, 〔표 5〕의 국내 정보보호 인력 채용 현황에서 정보보호 관련 사업체에서 경력직 직원을 선호하고 있음을 확인할 수 있다〔5〕. 즉, 현재 사업체들이 국내 정보보호 교육 체계 안에서 배출되는 인력보다는 관련 업무 경험을 보유한 인력을 선호하고 있음을 알 수 있다. 이는 곧 국내 정보보호 교육 체계의 개선이 필요함을 보여주는 사례라고 할 수 있다.

〔표 5〕 국내 정보보호 관련 사업체 분야별 인력 채용 현황(2011년) (단위:명)

기술개발		기술영업		기술지원		컨설턴트		기타	
신입	경력	신입	경력	신입	경력	신입	경력	신입	경력
379	589	132	166	192	266	96	111	96	90
968 (45.7%)		298 (14.1%)		458 (21.6%)		207 (9.7%)		186 (8.8%)	

2.2.2 사업체 정보보호 교육 현황

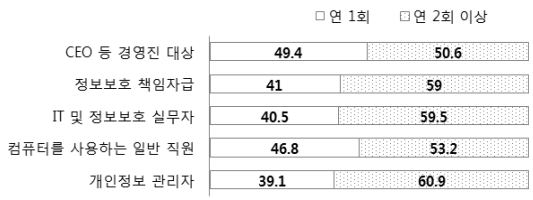


〔그림 3〕 국내 사업체 정보보호 교육 실시 현황

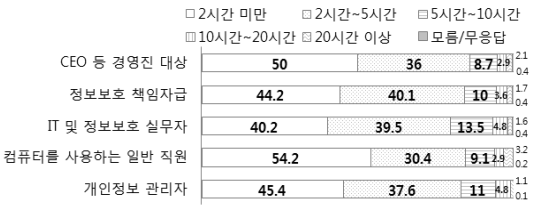
2010년에 위탁교육을 포함해서 정보보호 교육을 실시하고 있는 사업체는 〔그림 3〕과 같이 18.6%로 나타났다〔1〕.

정보보호 교육을 실시하고 있는 사업체의 비율이 매우 낮음을 알 수 있다.

정보보호 교육을 실시하는 사업체의 경우에도 연간 1회, 2시간 미만의 교육만을 실시하는 곳이 많은 것으로 나타나고 있다(〔그림 4〕, 〔그림 5〕 참조)〔1〕. 정보보호의 중요성이 날로 커지고 있음에도 불구하고 사업체에서의 관련 교육에 대한 투자는 여전히 매우 미미한 실정임을 알 수 있다.



〔그림 4〕 연간 정보보호 교육 횟수



〔그림 5〕 연간 정보보호 교육 시간

2.2.3 공공분야 정보보호 교육

정부기관 사이트를 목표로 한 7·7 DDoS 공격, 농협 해킹 사건 등에서 알 수 있듯이 국가 및 공공기관은 언제나 해킹 공격의 주요 대상이 된다. 최근 해킹 공격이 지능화되면서 국가·공공기관의 PC를 좀비 PC화 시키는 공격이 늘어나고 있다. 국가·공공기관의 정보보호 업무 담당자뿐만 아니라 일반 사용자에 대한 정보보호 교육 강화가 필요함을 알 수 있다.

이와 관련하여 공무원을 대상으로 하는 정보보호 교육은 행정안전부 중앙공무원교육원을 통해 이루어지고 있다. 행정안전부에서는 사이버 위협에 대비하여 전담조직 및 인력의 전문성을 강화하기 위해 전담인력에 대한 체계적이고 지속적인 교육과 국가의 정보자산 보호를 위한 체계적인 프로세스가 정립될 수 있도록 직무 분석에 따른 맞춤형 교육과정을 개발하였다. 효과적인 정보보호 환경 구축을 목적으로 중앙행정기관, 지자체 및 소속기관의 정보보호 업무 담당 공무원을 대상으로 정보보호 교육을 실시하였다. 교육과정은 신규자(기본과정), 관제실무, 침해대응 등 6개 과정으로 〔표 6〕과 같다〔6〕.

〔표 6〕 행정안전부의 정보보호 실무자 대상 교육과정

대상	기본과정	실무과정	심화과정
정보보호 관리자	정보보호 기본 실무	사례 중심의 사이버 위협 대응 방안	
정보보호 담당자		해킹 및 대응 실무	사이버대응 체계 구축
보안관제 담당자		보안관제 실무	침해사고 분석/대응

2011년의 경우, 중앙·지자체 228개 기관 대상으로 교육 수요 조사 시 1,395명이 신청함에 따라 교육 수요 초과로 과정별 정원을 30명에서 50명으로 확대하였다. 교육 횟수도 12회에서 15회로 확대하였으며, 최종적으로 475명이 교육을 이수하였다〔6〕. 정보보호에 대한 높은 관심을 확인할 수 있는 대목이다.

이와 별도로 행정안전부에서는 2011년 개인정보보호법의 시행과 함께 개인정보보호 교육 제도를 운영하고 있다. 이 교육은 중앙·지자체, 공사·공단 등 공공기관과 의료·노동·교육·금융 등 민간분야의 개인정보보호 담당 및 취급자를 대상으로 한다. 이 교육을 위해서 행정안전부에서는 대학, 정보보호전문업체, 한국인터넷진흥원 등의 전문가 65명으로 구성된 개인정보보호 강사단을 운영하고 있다〔7〕.

한편, 국가보안기술연구소는 2012년 7월 국가정보보안교육원을 설립하였다. 국가정보보안교육원은 2011년 8월 정부가 발표한 '국가 사이버안보 마스터플랜'의 후속조치 가운데 하나이다. 국가정보보안교육원은 공공기관 인력의 보안인식 수준 향상과 정보보안 전문인력 양성을 목표로 설립되었다. 이를 위해서 사이버안보 정책 과정, 보안담당자 실무능력 향상을 위한 보안실무 과정, 각 부처별 보안 관련 현안 문제 해결을 위한 사이버전 전문가 교육과정 등을 운영한다〔8〕.

2.2.4 대학/대학원 정보보호 교육

2011년 기준 국내에는 4년제 대학교에 20개, 전문대학에 3개의 정보보호 관련 학과들이 설치되어 있으며, 대학원 과정으로 23개의 학과(일반대학원 11개, 전문대학원 2개, 특수대학원 4개, 협동과정 6개)에서 정보보호 관련 전공을 운영하고 있다. 2011년 전문대학 이상의 정규 교육기관에서 배출한 인력은 978명이며, 대학 694명, 대학원 240명, 전문대학 44명이다〔6〕.

대학교 전체의 정보보호 관련 학과는 2010년도 대비 재적인원수는 7%, 전임교원수는 6% 감소하였고, 배출인원은 5% 증가하였다. 특히 현재 확보된 전임교원은 교육과학기술부 이공계 교원확보율 기준으로 50% 이하 수준인데, 이는 전문인력을 양성하기에 충분하지 않은 것으로 보인다〔6〕.

2.2.5 민간분야 정보보호 교육

한국인터넷진흥원(KISA)은 지식정보보안 분야의 고급인력 양성을 위해서 고용계약형 지식정보보안 석사 과정, 지식정보보안 전문인력 양성 과정 등을 운영하고 있다〔6〕.

고용계약형 지식정보보안 석사 과정은 정보보호 인력 수급난을 겪고 있는 지식정보보안업계에 석사급 맞춤형 인재를 양성하여 공급하기 위해 마련된 정책으로 2009년 처음 시작되었다. 이 사업에서 기업과 대학은 컨소시움을 맺어 공동으로 사업을 제안하는 방식을 통해 대학 인력을 선발하여 교육을 진행한다. 기업의 의견과 수요를 반영하고 기업 현장인력의 강사 활용, 학생의 인턴쉽 활용, 산학협력 R&D 과제 수행 등 운영에서도 기업과 대학이 공동으로 참여하고 있다〔6〕.

지식정보보안 전문인력 양성 과정은 지식경제부가

〔표 7〕 지식정보보안 전문인력 양성 과정 운영 현황

구분	과정명		횟수	인원
정규	디지털 포렌식		6	129
	지식정보보안 컨설턴트	주니어(기초)	3	98
		시니어(심화)	3	102
	보안관제		4	82
합계			16	410
수시	Skill-up 과정		8	320
	지식정보보안 보습과정		5	50
합계			13	370

중심이 되어 추진하고 있으며, 지식정보보안산업 재직자를 대상으로 하는 실무 중심의 교육과정이다. 2011년 기준 〔표 7〕과 같은 교육과정을 운영하였으며, 실무 중심으로 교육과정이 구성되어 있음을 알 수 있다〔6〕.

정보보호 분야에서 민간교육은 매우 활발한 편인데, 이는 교육에 대한 수요가 다양한 형태로 존재하기 때문이다. 2011년 기준 정보보호 관련 민간 교육기관은 19개이며, 주요 교육과정은 〔표 8〕과 같다〔5〕.

〔표 8〕에서 보는 바와 같이 현재 민간 정보보호 교육기관은 대부분 취업 등을 대비한 실용적인 교육을 중점적으로 제공하고 있다. 특히 자격증 과정이 활성화되어 있음을 알 수 있는데, 국내외 정보보호 전문 자격증 현황은 〔표 9〕와 같다.

〔표 8〕 민간 정보보호 교육기관의 교육 현황

기관명	교육과정
넷칼리지	데이터 통신 보안 과정, 정보보호 엔지니어 전문가 과정 등
와이즈로드	CISSP, CISA, CISM 과정 등
라이지움	CISSP 과정 등
라카데미	정보보호 전문가 자격증 과정
비트캠퍼스	컴퓨터 보안이론 등
삼성SDS 멀티캠퍼스	CISSP 대비 과정, 네트워크 보안 실무 등
쌍용정보통신 교육센터	보안 네트워크 프로그램 개발자 과정 등
썬 교육센터	CISA 자격증 대비 과정 등
솔데스크	해킹보안 전문가 과정 등
시스원 교육센터	정보보안 교육과정 등
아이티뱅크	정보보호 전문가 자격증 과정 등
아이티뱅크 멀티캠퍼스	정보보안 전문가 과정 등
이지스원	정보보안 전문가 과정 등
인섹시큐리티	침해사고 분석 대응 실무
한국정보보호 교육센터	정보보안 전문가 과정 등
한국정보보호 인식(주)	정보보안 전문가 과정 등
i2SEC 국제 정보보안교육센터	정보보안 전문가 과정 등
한국 HP 교육센터	정보보호 기초 과정 등
KH정보교육원	보안 전문가 과정 등

〔표 9〕 정보보호 전문 자격증 현황

구분	명칭	구분	주관기관
국내	정보보안기사, 산업기사	기사, 산업기사	지식경제부
	정보보호전문가 (SIS)	1급, 2급	한국인터넷진흥원
	인터넷보안전문가	1급, 2급	한국정보통신 자격협회
	정보보안관리사 (ISM)	-	한국정보평가협회
	해킹보안전문가	1급, 2급, 3급, 주니어	한국해킹보안협회
	사이버포렌식조사 전문가	-	한국생산성본부 / 사이버포렌식 전문가 협회
	디지털포렌식 전문가	1급, 2급	한국인터넷진흥원 / 한국포렌식학회
국외	정보시스템전문가 (CISSP)	-	ISC2
	정보보호관리자 (CISM)	-	ISACA

2011년 기준 국내 자격증인 정보보호전문가 자격시험에는 6,787명이 응시해서 8.1%에 해당하는 551명이 자격을 취득하였으며, 디지털포렌식 전문가 자격시험은 191명이 응시하여 39.8%에 해당하는 76명이 자격을 취득하였다. 국외 정보보호 전문 자격증인 CISSP의 경우, 전 세계적으로 79,323명의 자격자가 활동하고 있는데, 이 가운데 한국인은 2,724명이다. 국내에서 정보보호 관련 자격증 취득에 대한 관심이 매우 높다는 것을 알 수 있다〔6〕.

2.2.6 초·중·고 및 일반인 정보보호 교육

악성 댓글, 안티 카페 등 사이버 폭력 행위, 사이버 머니 사용 등을 위한 부모의 주민등록번호 도용 등이 문제가 되면서 청소년의 인터넷 사용 문화를 개선하기 위한 노력이 필요해지고 있다. 2013년 또는 2014년부터는 인터넷 윤리에 대한 신규 교과서가 보급될 예정이다. 이와 관련하여 방송통신위원회와 한국인터넷진흥원은 인터넷 윤리 교육 활성화를 위해 일선 학교와 교과서 제작 출판사들이 활용할 수 있는 인터넷윤리 교육 참고자료집을 개발하여 2012년 4월에 배포하였다. 이 참고자료집은 현행 교육과정 및 교과서 내용

을 분석하여 이와 관련된 다양한 인터넷 윤리 콘텐츠 목록을 매칭하여 제시함으로써, 수업 및 교과서 집필 시 바로 활용할 수 있다[9]. 한편, 방송통신위원회에서는 인터넷 윤리교육 정보서비스를 운영하고 있으며, 해당 사이트에서는 초·중·고 및 대학생, 교원을 대상으로 인터넷 사용에 대한 자가진단 및 동영상 등 다양한 형태의 교재를 제공하고 있다[10].

초·중·고 학생을 대상으로 하는 정보보호 교육이 주로 인터넷 윤리에 중점을 두고 있다면, 일반인을 대상으로 하는 정보보호 교육은 IT 교육 과정에 정보보호 관련 내용이 포함되어 있는 경우가 일반적이다.

교육과학기술부는 사이버 침해 대응과 개인정보보호에 대한 체계적인 교육을 목표로 2012년 8월 정보보호교육 지역센터를 지정하였다. 정보보호교육 지역센터는 [표 10]과 같이 3개 권역내에 소재하는 국·공립·사립 4년제 대학에 위치하고 있으며, 교육과정은 크게 4가지 항목으로 구성되어 있다. 정보보호교육 지역센터의 주요 교육대상은 교육공무원이며 대학(원)생과 청소년도 포함하고 있다. 특히 정보보호 관련 특성화 고등학교 학생을 대상으로 현장실습 과정을 운영하고 있다.

[표 10] 교과부 정보보호교육 지역센터 및 교육과정

구분	전담지역	교육과정
1권역 (고려대)	서울, 경기, 인천, 강원, 제주	- 기본과정 - 전문과정 - 특수분야 연수과정 - 유료과정
2권역 (충남대)	충북, 충남, 대전, 전북, 전남, 광주, 세종	
3권역 (부산대)	경북, 경남, 대구, 울산, 부산	

III. 국내 정보보호 교육의 문제점

앞서 2장에서는 다양한 형태의 국내 정보보호교육의 현황을 살펴보았다. 본 장에서는 점차 지능화되고 복잡해지는 사이버 침해에 대응하는데 있어서 국내 정보보호교육이 가지고 있는 문제점에 대해서 다음과 같은 관점에서 살펴보고자 한다.

○ 정보보호 교육 중장기 계획 부재
○ 교육 프로그램에 대한 검증 부족
○ 교육기관 간의 정보 교류 부재
○ 전문 강사 확보의 어려움
○ 일반인의 정보보호 인식 제고를 위한 교육 프로그램 부재

3.1 정보보호교육 중장기 계획 부재

국가 사이버안보 마스터플랜에 의하면 정보보호 기반 강화를 위해 인력확보 차원에서 정부기관의 정보보호 인력 증원 및 국가 핵심기반시설 운영기관의 보안 전담인력 확보 등을 계획하고 있다. 그러나 국가·공공기관의 정보보호 인력에만 초점을 맞추고 있으며, 결정적으로 인력 양성에 대한 중장기적인 교육계획은 포함하지 않고 있다[11].

국가 사이버안보 마스터플랜을 바탕으로 부처별로 소관분야에 대한 세부 추진계획을 수립 및 시행토록 하고 있지만 정부차원에서의 정보보호교육에 대한 마스터플랜이 제시되지 않다보니 부처 및 교육 기관별로 최신 유행 아이템 위주로 교육이 진행되고 있는 실정이다.

행정안전부의 경우, 2011년까지는 정보보호 실무자 대상 교육 과정이 활발하게 운영되었으나[6], 2012년부터는 개인정보보호와 관련된 교육만 유지되고 있다[12]. 교육과학기술부의 정보보호교육 지역센터의 경우 2013년까지의 운영 계획은 세워져 있지만 장기적인 계획은 수립되지 않고 있다. 또한 공공, 민간, 대학(원), 초·중·고 교육의 대부분이 자격증이나 개인정보보호 등 실무적이고 최신 유행하는 아이템에 중점을 두고 있다. 교육대상자의 수준이나 환경에 맞게 체계적으로 교육을 진행하는 큰 틀이 부족하다고 할 수 있다.

주요 정보보호 교육기관의 교육내용 및 교육 대상을 살펴보면 [표 11]과 같다. [표 11]에서 보는 바와 같이 교육 프로그램의 교육대상이 대부분 중복되며, 교육내용 역시 유사하다는 것을 알 수 있다. 이와 같은 현상이 발생하는 것 역시 체계적인 정보보호 교육을 위한 마스터플랜의 부재에서 원인을 찾을 수 있다.

3.2 교육 프로그램에 대한 검증 부족

현재 진행되고 있는 정보보호 교육의 효과를 측정할 수 있는 수단이 부족하다. 민간 교육기관의 경우에는 취업률, 자격증 취득 비율 등으로 그 효과를 측정할 수 있다. 하지만 현재는 단순한 만족도 조사 등을 제외하고는 교육 프로그램의 내용을 검증하고 개선하려는 노력이 부족하다. 대부분의 교육이 실무 위주로 이루어지고 있는데, 교육을 수료한 수강생들이 교육내용을 얼마나 실제 업무에 활용하고 있는지 분석한 자료는 전무하다시피 하다. 2시간에서 10주까지 비교적

단기교육 중심인 현 정보보호 교육 프로그램이 교육 대상자들의 정보보호 지식이나 인식 제고에 기여하고 있는지를 검증할 필요가 있다. 또한 교육생들의 수준 측정, 교육 프로그램 자체에 대한 객관적인 평가 등 다양한 방법의 검증 체계가 필요하다.

〔표 11〕 교육기관간 교육내용 및 교육대상 비교

구분	교육내용	교육대상
행정안전부 중앙공무원 교육원	- PC 안전관리 클리닉 - 정보보호능력 향상 - 해킹이해 및 침해대응	공무원
국가정보보안 교육원	- 사이버안보 정책 - 보안 기본/실무 - 정보통신기반시설 보안 - 클라우드 컴퓨팅 보안위협과 대응 - 모바일 보안위협과 대응 - 보안관제	국가·공공기관 정보보호 실무자 및 담당자
지식정보보안 전문인력 양성과정	- 인터넷 윤리 - 시스템 해킹 및 보안 - 역공학, 침해사고 분석 - 유무선 네트워크 보안 - 디지털 포렌식	정보보호 실무자 및 담당자
민간교육기관	- CISSP 등 정보보호 자격증 과정 - 네트워크 보안 - 해킹 및 대응	취업 대상자 정보보호 실무자 및 담당자
교육과학기술부 정보보호교육 지역센터	- 개인정보보호 관리/실무 - 웹, 네트워크 취약점 분석 및 대응 실무 - 모바일 보안 실무 - 침해사고 대응 및 디지털 포렌식 - 해킹 및 대응 기술	교육공무원 대학(원)생 청소년

3.3 교육기관 간의 정보 교류 부재

교육기관 간의 정보 교류는 강사, 교재, 교육 노하우, 관심도가 높은 아이템, 교육 장소의 교류 등 다양한 형태로 나타날 수 있다. 그러나 공공, 민간, 초·중·고, 대학·대학원 등 분야가 다양한 점을 감안 하더라도, 현재 국내 교육기관 간의 정보 공유나 교환이 이루어지지 않고 있다. 또한 외국기관과의 정보 교류도 미미한 실정에 머무르고 있어 국제적인 정보보호 교육 이슈를 받아들이는데 한계가 있다. 공공 분야에서 민간 교육기관에 위탁 교육을 의뢰하는 일부 경우를 제외하고는 교육기관 간의 정보 교류가 이루어지는 사례는 찾기 힘들다. 이는 유사한 교육대상을 상대로, 유사한 교육과정을 양산하는 문제를 발생시키며, 또한 정보 교류의 부재는 강사의 질을 떨어뜨리는 결과로 나타날 수 있다.

3.4 전문 강사 확보의 어려움

지식정보보안 전문인력 양성 과정의 경우, 강사진 전원이 한국인터넷진흥원의 연구원으로 구성되어 있으며, 행정안전부의 개인정보보호 교육은 대학, 정보보호전문업체, 한국인터넷진흥원 등의 전문가를 강사로 활용하고 있다. 일부 공공기관의 경우에는 민간 정보보호 교육기관에 정보보호 교육을 위탁하여 운영하고 있다. 전문강사 육성 및 지원제도가 미비하다보니 교육에 전념할 수 있는 수준높은 강사가 부족할 수밖에 없으며, 이로 인해 주로 공공기관이나 민간기관의 정보보호 전문가를 강사로 활용하고 있는 실정이다.

이와 같은 전문가 활용은 실제 업무를 수행하고 있는 인력이 교육을 진행한다는 점에서 전문성을 확보할 수 있다는 장점이 있지만, 대부분의 강사들이 자신들의 업무를 수행하면서 정보보호 교육을 수행하는 상황에서는 교재 개발, 강의 준비, 과제 검토 등 교육 수행 측면에서 양질의 교육을 기대하기 어려운 것이 사실이다. 강사 본연의 업무에 차질을 줄 수 있다는 우려 또한 존재한다. 양적으로 전문 강의를 진행할 수 있는 인력이 부족하기 때문에 일부 소수의 인력이 여러 분야에서 강의를 진행하는 경우가 발생하기도 한다.

인력 부족으로 야기되는 더 큰 문제는 강사 자신의 전문 분야가 아닌 다른 분야에 대해서도 강의를 하는 경우가 발생하기도 한다는 점이다. 정보보호 교육은 여러 가지 세부 분야로 구성되며 각 분야가 많은 전문성을 요구한다. 단순히 정보보호 전문가라 해서 자신의 전문 분야가 아닌 다른 분야의 교육까지 진행할 경우에는 교육 내용이 부실해질 가능성이 높아진다.

대부분의 교육 프로그램이 강사가 직접 교재를 제작하고 자신의 전문지식과 노하우를 활용하여 강의를 진행하는 현실을 고려할 때, 양질의 강사 확보는 정보보호 교육 개선을 위해서 가장 중요한 요소 가운데 하나라고 할 수 있다.

3.5 일반인의 정보보호 인식 및 대응능력 제고를 위한 교육 프로그램 부재

앞서 서론에서 이미 기술한 바와 같이 최근의 해킹 공격은 특정 서버나 서비스를 공격하기 위해서 인터

넷에 연결되어 있는 일반 PC를 좀비 PC로 만들어 버린다. 이런 해킹 공격에 대응하기 위해서는 일반인의 정보보호 의식 수준 및 대응 능력의 향상이 필요하다. 그러나 현재 일반인을 대상으로 하는 정보보호 교육의 대부분은 인터넷 윤리와 개인정보보호에 치중하고 있다.

사이버 공격으로 인한 피해가 막대한 경제적 손실, 국가 기능 마비 등 심각한 피해를 일으킬 수 있다는 점을 일반인들에게도 인식시키고, 이에 대응하기 위해서 올바른 인터넷 사용뿐만 아니라 안티 바이러스 제품 등 정보보호 제품의 사용 능력 향상 등 다양한 노력이 필요하다.

IV. 국내 정보보호 교육체계 제안

본 장에서는 앞서 기술한 정보보호 교육의 문제점을 해결하고 국내 사이버보안 환경을 강화하기 위해서 정보보호 교육 분야에 필요한 사항에 대해서 제안하고자 한다.

4.1 정보보호교육 마스터플랜

3장에서 기술한 바와 같이 현재 국내 정보보호교육의 가장 큰 문제점 가운데 하나는 체계적인 마스터플랜 없이 여러 기관이 독자적인 방법으로 정보보호교육을 진행하고 있다는 점이다. 이로 인해서 발생할 수 있는 중복투자, 교육의 질 저하, 강사 확보의 어려움 등을 해결하기 위해서는 국가적인 수준에서 장기적으로 추진할 수 있는 마스터플랜의 수립이 필요하다. 정보보호 마스터플랜에 포함되어야 하는 내용으로 다음과 같은 사항들을 고려해야한다.

- ○ 교육과정 개발: 최신 해킹 및 대응 기술, 정보보호 관련 법제화 현황, 정보보호 기초 등 다양한 정보보호 관련 이슈를 고려한 교육과정의 개발이 필요하다. 교육 대상 및 내용에 따라 단기과정 중·장기 과정 등 다양한 세부 교육과정을 개발해야 한다.
- ○ 장기적인 교육계획 수립: 단기적인 교육과정의 개발뿐만 아니라 국제 동향, 교육대상의 연령 및 직업 등을 고려한 장기적인 교육계획을 수립해야 한다.
- ○ 표준 교재 개발: 충실한 교육이 진행되기 위해서는 양질의 교재 개발이 필수적이다. 강의시 기본 교육자료로 활용이 가능한 교재를 개발하기 위해서는 관련 분야의 다양한 전문가 활용이 필수적이다.
- ○ 강사 인력 확보: 전반적으로 정보보호 관련 인력이 부족한 가운데 양질의 강의를 제공할 수 있는 강사 인력 역시 매우 부족한 실정이다. 다양한 방법을 통한 강사 인력 확보가 반드시 필요하다.
- ○ 사이버보안 교육장 확보: 국가적인 차원의 사이버보안 교육장을 구축하여 대학 및 민간 교육기관 등에서 모의 해킹 등의 용도로 공동 사용하도록 함으로써 교육 효과를 높일 수 있다.
- ○ 최신 동향 분석: 정보보호 기술 및 정책은 발전 속도가 매우 빠르다. 교육에 최신 해킹 및 대응 기술 등 최신 동향이 반영되지 않는다면, 실제로는 활용이 불가능한 지식만 얻게 될 가능성이 매우 크다. 교재 및 강사에 반영할 수 있는 최신 정보보호 동향의 분석이 항상 이루어져야 한다.

정보보호 교육 마스터플랜은 정보보호 전문가, 교육 전문가, 정책 전문가 등 다양한 분야의 전문가로부터 의견을 수렴하여 작성되어야 하며, 국가 사이버보안의 미래를 책임진다는 사명의식 하에 적극적으로 추진되어야 한다.

4.2 정보보호 교육 프로그램 인증제도 도입

정보보호 교육의 효과를 극대화하기 위해서는 정보보호 교육 프로그램의 수준 향상이 필수적이다. 정보보호에 대한 대학 수준의 교육과정을 예로 들면 기본적으로 컴퓨터, 정보통신 등의 IT관련 교과목들이 주를 이루고 3,4학년에 정보보호 관련 과목 몇 개가 추가되는 정도이다. 대학에서 정보보호 관력학과를 운영하기 위한 교육과정의 개선이 필요하며, 대학원 교육과정과의 차별성 및 연계성을 갖도록 하여 양질의 교육이 이루어질 수 있도록 해야 한다. 그 밖에, 교육생들의 수준측정, 교육 프로그램 자체에 대한 객관적인 평가 등 다양한 방법의 검증체계가 고려되어야 한다.

항상 양질의 교육수준을 유지하기 위해서는 상시적인 교육 프로그램의 검증이 이루어져야 하며, 이를 위해서 교육 프로그램 인증 제도의 도입이 필요하다.

교육 프로그램 인증을 위해 크게 2가지 방안을 고려할 수 있다. 첫 번째는 정보보호 교육기관과 교육 프로그램을 인증하는 제도의 도입이며, 두 번째는 수강생 수준 측정 프로그램의 운영이다.

이미 국내에서는 공학 교육의 수준 향상 및 평가를 위해서 공학교육 인증 제도를 운영하고 있다. 공학교육 인증 제도는 '프로그램의 교육 목표', '프로그램 학습성과 및 평가', '교과 영역', '학생', '교수진', '교육 환경', '교육 개선', '전공분야별 인증 기준' 등 8개 기준을 기반으로 하여 공학교육 프로그램을 인증하고 있다[13]. 미국의 경우, 1932년 설립된 ABET (Accreditation Board for Engineering and Technology)에서 대학과 대학의 전공과정이 양질의 교육을 제공하기 위한 최소한의 기준을 제시하고 이를 인증하고 있으며, 미국 공과대학의 95%가 참여하고 있다[14]. 정보보호 교육 역시 이와 같은 인증 제도를 통해서 양질의 교육 제공이 가능하다.

또한 NSA는 미국 전역에서 대학에 소속된 정보보증우수교육센터 145곳을 선정하여 지원하고 있다. 학생에 대한 장학금 지원, NSA 인턴쉽 체험 등의 혜택을 제공하는 정보보증우수교육센터에 선정되기 위해서는 다음과 같은 심사 기준에 의해 평가 받아야 한다.

○ 커리큘럼 공유 등 타 기관과의 협력 활동
○ 타 전공 학생을 위한 정보보호 과목 개설
○ 대학의 정보보호 수준
○ 학생의 정보보호 분야 연구에 대한 지원 제도
○ 교수진의 대외 활동
○ 정보보호 자원 확보
○ 정보보호 교육의 활성화 정도
○ 정보보호 교육을 위한 별도의 센터 설립 여부
○ 교수진의 규모 및 강의 부담

이와 같이 정보보호 교육 기관 또는 교육 프로그램 자체에 대한 인증 제도를 실시해 인증 기관 또는 프로그램을 지속적으로 관리함으로써 정보보호 교육 프로그램의 수준을 유지할 수 있다.

정보보호 교육 프로그램에 대한 직접적인 평가와는 별도로 정보보호 교육을 수료한 수강생의 수준을 측정함으로써 해당 교육 프로그램을 검증할 수 있다. 수강생에 대한 평가 시험, 취업률, 만족도, 수강생이 속한 기관의 만족도 등 다양한 요소를 통해서 수강생의 수준을 측정할 수 있다. 이를 위해서 정보보호 교육 수강생을 대상으로 수준측정 시험실시 등의 제도 개선이 필요하다.

4.3 정보보호 전문 인력 DB 운영

모든 교육 프로그램에 있어서 양질의 강사 확보는 교육 프로그램의 수준 향상을 위해서 필수적이다. 국가차원에서 정보보호교육 수요자와 강사의 수를 분야별, 수준별로 면밀히 파악하고 교육내용, 교육수준에 적합한 전문강사를 확보하기 위한 노력이 필요하다. 강사의 전문분야 내에서 교육이 진행되면 전문성을 유지하여 양질의 교육을 보장할 수 있다.

또한 전체적인 현황이 파악되면 분야별, 수준별로 부족한 강사를 집중적으로 양성하여 강사비율을 안정적으로 유지할 수 있다. 이를 위해 정보보호 전문강사를 육성 및 지원하는 제도를 마련해야 한다.

이 제도는 정보보호 전문인력 DB를 확보하는 데서 시작할 수 있다. 정보보호 분야는 발전과 변화의 속도가 빠르기 때문에 외부 전문인력의 강사 활용이 필수적이다. 전문 인력 확보를 위해서는 국내 화이트해커 및 화이트해커 그룹과 지속적으로 관계를 유지하면서 인력 DB를 운영해야 한다. 나아가 외국의 정보보호 전문가들과도 교류를 통해 관계를 유지하면서 적극 활용해야 한다.

또한 이제 국내의 정보보호 연구의 역사도 깊어져 현업에서 은퇴한 인력이 나오고 있다. 이와 같은 고급 전문인력을 적극적으로 활용할 수 있다면 정보보호 교육 체계 개선에 많은 도움을 받을 수 있다. 특히 정보보호 교육은 기술 교육뿐만 아니라, 윤리, 국가관 등을 병행해야만 하는데, 은퇴자들이 멘토 역할을 한다면 효과를 증대시킬 수 있다.

4.4 정보보호 교재 개발

앞서 문제점에서 기술한 바와 같이 현재 국내의 정보보호교육의 교재는 강사가 독자적으로 개발하여 활용하는 경우가 대부분이다. 전문강사도 아닌 상태에서 교재 개발의 부담까지 더해지기 때문에 이전에 이미 활용된 내용이나 다른 사람이 작성한 내용을 재활용하거나 강의 내용을 충분히 담지 못하는 경우가 빈번하게 발생할 수밖에 없다.

정보보호 표준 교재를 개발하여 교육에 활용할 수 있다면 이러한 강사의 부담을 줄이고, 교육에 집중할 수 있도록 함으로써 교육 수준의 향상이 가능하다.

또한 중장기적인 계획 아래에서 교재 개발이 이루어진다면, 수강생의 연령, 환경, 요구사항을 고려하여 완성도 높은 교재 제작이 가능하다.

4.5 교육 이수생에 대한 다양한 혜택 개발

정보보호 전문인력이 활용할 수 있는 혜택으로는 일부 공공기관 및 군에서 정보보호 자격증 취득자에게 제공하는 취업(입대) 시 우대 정책이 거의 유일하다. 해킹 및 대응을 비롯해 정보보호 분야가 젊은 인력의 활발한 참여를 필요로 한다는 점에서 좀 더 다양한 혜택이 개발될 필요가 있다.

예를 들어 현재 고려대학교 사이버국방학과는 4년간 장학금과 졸업 장교 임관이 가능한데, 이와 같은 제도가 더욱 확대되어야 한다.

4.6 사이버보안 교육장 구축

내실 있는 정보보호 교육을 위해서는 모의 해킹, 취약점 분석 등 실습 교육이 병행되어야 한다. 그러나 모의 해킹 등의 활동은 시스템에 영향을 줄 수 있기 때문에 교육생이 직접 실습할 수 있는 기회는 많지 않으며, 대부분 강사가 준비한 데모 영상을 시청하는 형태에 머물고 있는 실정이다.

이러한 문제를 해결하기 위해서 국가적인 관리 아래에서 다양한 교육기관이 공동으로 사용할 수 있는 사이버보안 교육장 구축이 요구된다. 최근 많은 발전을 이루고 있는 가상화 기술 등을 이용하여 교육장을 구축하고, 전담인력이 관리하도록 함으로써 정보보호 교육의 효율을 보다 더 높일 수 있다.

4.7 정보보호 인프라 강화

직접적으로 정보보호 체계와 관련 있는 사항은 아니지만, 정보보호 교육이 활성화 되는데 있어서 우선적으로 이뤄져야 하는 것은 정보보호 인력을 활용할 수요처의 확대 및 정보보호 인력에 대한 지원 강화이다.

많은 수의 정보보호학과 졸업생들이 정보보호 전문업체로 진출하고 있는데, 대부분의 정보보호 전문업체의 규모가 작아 좋은 처우를 기대하기 어려운 것이 사실이다. 그 외 연구소, 공공기관 등에 진출이 가능하나 해당 기관에서 수용하는 인력이 그리 많지 않은 실정이다. 따라서 정부부처 내 정보보호 직군 설치, 사이버국방, 사이버 포렌식 기관의 확대 등 정보보호 전문인력의 활용을 확대 시킬 수 있는 노력이 필요하다. 사이버무기 개발을 담당하는 사이버방위산업체 등의 육성 등도 고려할 수 있으며, 정보보호 분야 병역특례 제도 운용 등 다양한 혜택을 개발해야 한다. 그리고 대학의 정보보호학과 및 해킹 동아리에 대한 지원을 강화하여 우수 인재를 조기에 영입할 수 있어야 한다. 뿐만 아니라 현재 대학내 해킹 동아리에 집중되어 있는 지원을 고등학교나 대학 밖의 해킹 동아리로 확대해야 한다.

또한 업체, 공공기관 등에서 활동하고 있는 정보보호 전문인력에 대한 지원을 강화해야 한다. 현재 정보보호 업무는 많은 사람들에게 기피 대상이 되고 있는데, 이는 많은 업무량에 비해 처우가 좋지 않고 보안사고 발생 시 징계의 대상이 되기 때문이다. 처우 개선과 함께 우수 기관 및 인력에 대한 포상 확대 등 관련 인력에 대한 다양한 혜택을 개발해야 한다.

4.8 일반인에 대한 정보보호 교육 확대

초·중·고 학생이나 주부, 노인 등 일반인에 대한 정보보호 교육을 확대해야 한다. 예를 들어 PC에 악성코드 탐지 프로그램이 설치되어 있지 않거나 설치되어 있더라도 일반인의 경우 사용법을 몰라 업데이트를 수행하지 않음으로써 악성코드에 노출될 위험이 있다. 따라서 일반인을 대상으로 간단한 악성코드 탐지 프로그램 작동방법을 비롯한 사이버 침해 위협에 대한 교육이 강화되어야 한다.

또한 최근에는 조작이 간단한 해킹 프로그램의 수도 크게 늘어 전문적인 지식이 없더라도 해킹을 시도해볼 수 있는 상황이다. 이런 위험은 특히 초·중·고 학생 등 아직 윤리관이 뚜렷하지 않은 계층일 경우에 더욱 커질 수 있다. 이런 위험을 최소화하기 위해서는 인터넷 사용에 대한 윤리관 확립 등 전반적인 정보보호 인식 수준을 향상시킬 수 있는 교육이 병행되어야 하다.

4.9 정보보호교육 총괄기관 설립

지금까지 기존 정보보호 교육을 개선하기 위한 방안을 제안하였다. 마지막으로 이런 방안을 장기적인 계획에 따라 안정적으로 추진하기 위해서 정보보호교육을 총괄할 수 있는 기관 또는 조직의 설립을 제안한다. 정보보호 교육 강화에 가장 적극적인 미국의 경우에도 여러 정부부처가 참여하고 있지만, NIST라는 단일 기관에서 NICE 계획을 주도하고 있다. 국내도 정보보호 교육 체계를 총괄하는 조직이 존재할 경우 다음과 같은 장점을 취할 수 있다.

○ 정보보호 교육 체계 조기 정비: 교육기관, 민간, 공공기관, 군 등이 독자적으로 정보보호 교육을 수행하는 현재의 체계를 정보보호 교육 마스터플랜을 효율적으로 추진하는 체계로 정비하는데 소요되는 비용과 시간을 최소화할 수 있다. 또한 정보보호 교육 인증제도와 같은 신규 제도의 운영 추진이 용이하다.

○ 중복투자 최소화: 정보보호 교육 강화의 필요성이 높아지고 있는 현 시점에서 각 교육기관이 유사한 분야에 중복 투자함으로써 발생할 수 있는 비용 낭비와 비효율성을 최소화할 수 있다.

○ 정보공유 확대: 교육 콘텐츠, 인력, 최근 이슈 등 다양한 형태의 정보 교류가 총괄기관을 중심으로 이루어질 수 있게 되어 자연스러운 교육의 질 향상을 기대할 수 있다.

○ 피드백 접수 및 반영: 현재는 정보보호 전문업체 등 실무 현장에서 교육에 대한 요구사항이 발생하여도 이를 교육기관에서 접수하고 반영할 수단이 전무하다시피 하다. 그러나 총괄기관이 존재할 경우에는 피드백을 접수할 수 있는 창구가 명확해지기 때문에 실무 현장의 요구사항을 빠르게 교육 현장에 적용할 수 있다.

총괄 기관의 설립을 위해서 본 논문에서는 3가지 방안을 제안하고자 한다. 첫 번째 방안은 독립적인 정보보호교육 총괄 기관의 설립이다. 정보보호교육 정책을 강력하게 시행하기 위해서는 정보보호교육 관리를 일원화 시켜 추진해야 한다. 두 번째는 기존 정보보호 교육기관 가운데 하나의 기능을 확대하여 정보보호 교육을 총괄하도록 하는 것이다. 정보보호 교육 마스터플랜 수립 등 필요한 업무를 조속히 시행하기 위해서는 관련된 경험 및 인력을 확보하고 있는 기존 정보보호교육 기관에서 정보보호교육을 총괄하도록 해야 한다. 마지막으로 세 번째 방안은 공공기관, 군, 학교, 민간분야 등 모든 정보보호 교육기관들이 참여하는 정보보호 교육 협의체의 구성이다.

정보보호 교육 총괄 기관의 주요 업무는 앞서 기술한 정보보호 마스터플랜의 세부 내용 수립 및 시행이다. 3가지 방안 모두 현재 공유되는 목표 없이 각 분야에서 이루어지고 있는 정보보호 교육의 체계를 일원화하고 교육의 질과 수강생의 만족도를 향상시키는데 기여할 수 있다. 3가지 방안의 장단점을 비교하면 〔표 12〕와 같다. 강력한 정책 추진, 제도 정비 등을 위해서는 신규기관을 설립하는 것이 유리하나, 초기 설립 비용 및 인력 확보 등에 어려움이 예상되며, 효율 극대화를 위해 계속해서 타 기관의 협조를 얻어야 하는 부담이 있다. 기존 정보보호 교육 기관 가운데 하나를 확대하여 총괄기관으로 운영하는 경우에는 초기 설립 및 운영비용을 최소화하는 것이 가능하나, 타 기관과의 업무 조정이 필요하다는 어려움이 있다. 협의체 형태의 총괄기관을 설립한다면, 강력한 정책을 추진하는 데는 어려움이 있을 수 있으나, 적은 비용으로 각 분야의 적극적인 참여를 유도해내고 다양한 정책을 발굴하는데 유리하다.

나아가 정보보호 교육 총괄 기관에서 강의나 교육과 관련된 업무뿐만 아니라 정보보호 관련 직무의 표준화, 정보보호 인력의 수준 측정 등 다양한 정보보호 교육 관련 업무에 기여하도록 함으로써 정보보호 분야의 국가 경쟁력 확보에 기여할 수 있다.

V. 결 론

IT 분야에서 세계적으로 선두권을 유지하고 있는 우리나라는 정보보호 분야에서도 선도적인 역할을 수행하고 있다. 그러나 그 동안 정보보호 환경 구축이 기술 중심으로 이루어져왔다면, 앞으로는 기술에 더해 인력이 중요한 역할을 할 것으로 예측된다. 특히 사이버 공격이 지능화 되고 광범위하게 이루어지면서 소수

〔표 12〕 정보보호 교육 총괄 기관 수립 방안 비교

구분	장점	단점
방안 1. 신규 기관 설립	- 강력한 정책 추진 및 제도정비 가능 - 일관된 마스터플랜 수립 및 시행 가능	- 초기 설립 비용 및 시간 소요 부담 - 설립을 위해 부처간 협의 필요 - 타 기관 협조 유도 부담
방안 2. 기존 기관 확대	- 초기 설립 및 운영비용 절감 - 기존 기관의 운영 노하우 등의 활용 가능	- 기존 기관의 업무 부담 증가 - 타 기관과의 업무 조정 부담
방안 3. 정보보호교육 협의체 구성	- 초기 설립 및 운영비용 절감 - 각 분야의 참여 유도 용이 - 다양한 정책 발굴 및 적용 가능	- 강력한 정책 추진의 어려움

정보보호 전문가가 국가 사이버 안보 및 개인정보 보호를 책임질 수 없는 환경으로 빠르게 변화하고 있다.

급변하는 환경에 대처하기 위해서는 무엇보다도 기존 정보보호 전문가의 수준 향상, 신규 정보보호 인력의 양성, 그리고 일반인들의 정보보호 인식 제고 등 인력 발전을 위한 다양한 노력이 필요하다. 이러한 노력이 결실을 맺을 수 있는 가장 구체적인 방법은 정보보호 교육의 강화이다.

이에 따라 본 논문에서는 국내 정보보호 교육의 현황을 살펴보고, 정보보호 교육 중장기 계획 부재, 교육 프로그램에 대한 검증 부족, 교육기관 간의 정보 교류 부재, 전문강사 확보의 어려움, 일반인의 정보보호 인식 제고를 위한 교육 프로그램 부재 등의 문제점을 지적하였다. 그리고 이와 같은 문제의 해결을 위해서 국가 정보보호 교육 마스터플랜의 기획 및 추진, 정보보호 교육 프로그램 인증 제도 도입, 정보보호 전문인력 DB 운영, 정보보호 표준 교재 개발, 교육 이수생 등 정보보호 인력에 대한 다양한 혜택 개발, 사이버보안 교육장 구축, 일반인에 대한 정보보호 교육 확대, 정보보호 협의체와 같은 총괄기관 설립 등 국내 정보보호 교육 발전을 위한 방안을 제안하였다.

제안한 발전 방안을 토대로 여러 면에서 아직 미미한 실정인 국내 정보보호 교육 체계를 개선하고, 이를 통해 보다 발전적인 국가 정보보호 환경 구축이 가능할 것으로 기대된다. 그러나 제안된 발전 방안을 통해서 국내 정보보호 교육의 발전을 가져오기 위해서는 기존 정보보호 교육기관뿐만 아니라 정보보호 관련 기관 및 업체, 대학 및 연구소 등의 정보보호 전문가, 그리고 일반인 등 관련된 모든 분야에서 많은 노력을 기울여야 한다. 또한 지속적으로 교육 체계를 점검하고 개선해 나아갈 때 내실 있는 정보보호 교육 체계 확립이 가능하다.

참고문헌

〔1〕 방송통신위원회, 한국인터넷진흥원, 2011년 정보보호실태조사(기업편), 2012년 3월.

〔2〕 디지털데일리, http://ddaily.co.kr/news/news_view.php?uid=89780, 2012년 4월.

〔3〕 백악관, 사이버보안 정책리뷰, 2009년 5월.

〔4〕 NIST, National Initiative for Cybersecurity Strategic Education Plan - Building a Digital Nation, 2011년 8월.

〔5〕 한국인터넷진흥원, 2011 국내 정보보안산업 실태조사, 2011년 12월.

〔6〕 방송통신위원회, 행정안전부, 지식경제부, 2012 국가정보보호백서, 2012년 5월.

〔7〕 행정안전부 개인정보보호 종합지원 포털, http://www.privacy.go.kr/edu/tea/EduTeacherList.do, 2013년 3월 확인.

〔8〕 전자신문, http://www.etnews.com/news/computing/security/2614550_1477.html, 2012년 7월.

〔9〕 방송통신위원회, 한국인터넷진흥원, 초·중·고 인터넷윤리 교육 참고자료집, 2012년 4월.

〔10〕 인터넷 윤리교육 정보서비스, http://www.nethics.kr/new_intro.jsp, 2013년 3월 확인.

〔11〕 관계부처 합동, 국가 사이버안보 마스터플랜, 2011년 8월.

〔12〕 행정안전부, 2013년 교육계획 운영(안), 2013년 2월.

〔13〕 한국공학교육인증원, 공학인증기준2005 설명서, 2008년 7월.

〔14〕 정원일, 하재철, “공학교육 인증을 위한 정보보호 심화 프로그램,” 정보보호학회지, 19(1), pp.75-82, 2009년 2월.

〈저자소개〉

김 동 우 (Dong-woo Kim) 학생회원
2009년 2월: 목원대학교 정보전자영상공학부 졸업
2011년 2월: 충남대학교 컴퓨터통신및보안 석사
2012년 3월~현재: 충남대학교 컴퓨터통신및보안 박사과정
〈관심분야〉 모바일보안, 디지털포렌식, SCADA보안, 정보보호정책

채 승 완 (Seung-woan Chai) 정회원
1990년 2월: 수원대학교 경제학과 졸업
1992년 2월: 단국대학교 경제학 석사
2001년 3월: 일본 니이가타대학(新潟大學) 경제학 박사
2005년 11월~현재: 한국인터넷진흥원 수석이코노미스트
〈관심분야〉 정보보호, 보안경제, 보안인력양성

류 재 철 (Jae-cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 네트워크보안, 암호학, 보안프로토콜