한국산학기술학회논문지
Vol. 10, No. 12, pp. 3725-3730, 2009

국내 정보보호 교육 훈련 프로그램 분석

홍진근[1*]
[1]백석대학교 정보통신학부

Analysis of Education Training Program of Information Security Man Power in Domestic

Jin-Keun Hong[1*]
[1]**Division of Information Communication, Baekseok University**

요 약 7.7 DDoS 해킹 대란은 정보보호의 현주소와 함께 대응체계의 중요성에 대한 인식을 제고하는 기회가 되었다. 정보보호 대응방안 가운데 가장 핵심적인 요소는 정보보호 인력 수급 문제이다. 본 논문은 국내 및 국외 정보보호 프로그램을 살펴보고, 국내 대학의 주요 교과과정과 보호 분류표로부터, 국내 정보보호 인력 양성을 위해 필요한 정보보호 교육 훈련 프로그램을 분석하였다.

Abstract A serious disturbance of the 7.7 DDoS hacking gets a chance of raised awareness for importance of response countermeasure with current status of information security. The critical factor out of countermeasure of information security is the supply of information human power. In this paper, we review program of information security of domestic and foreign, from major courses of domestic university, and category of government about information security, and analyze security education training awareness program of human power in the information security area.

Key Words : Information security program, security training

1. 서론

정보보호 교육 훈련 프로그램 및 인증 프로그램과 관련하여, 미국의 주요 보안 실무자들은 ISA (ISACA협회), CISSP(ISC2협회), GIAC 인증, CCNA/CCNP(Cisco) 등과 관련된 자격증을 주요 자격증으로 선호하고 있다. 매년 발간되는 국가정보보호 백서[1]는 국가정보보호 정책 등을 골자로 정보보호 교육현황, 인력 배출현황, 산업 환경에 대한 유익한 자료를 제공하고 있다. 정보보호 교육 연구와 관련하여, 전효정 등은 정보보호 분야 직무별 필요 지식 및 기술 분석에 대한 연구를 수행한바 있다.

한국인터넷진흥원(구. 한국정보보호진흥원)은 정보보호 실태조사 및 정보보호 산업시장 및 동향 조사에 대한 연구가 수행된 바 있었다. 하재철 등은 공학교육인증을 위한 정보보호학 심화프로그램을 리뷰한 바 있다[3]. 김지숙 등은 국기기관의 정보보호 수준평가에 관한가 있었으며, 김태성 등[5]은 교육통계연보를 이용한 정보보호 교육기관 현황에 대한 분석이 제안된 바 있다. 유혜원 등[6]이 제시한 국내 정보보호 분야 지식 및 기술 수용에 대한 연구에서는 정보보호 분야의 지식 및 기술 분류를 12개로 분류하고, 71개의 기술을 도출하였다. 김태성 등[7]이 제안한 AHP를 이용한 정보보호 인력 양성 정책 분석에서도 국가과학기술위원회의 국가과학기술지도를 기준으로 정보보호기술을 정의하고, 정보보호 인력 양성 계층도를 제시하고 있다. 우리는 실제 대부분의 정보보호 전문가들이 지적하듯이, 정보보호 인력 양성을 위한 기술 도메인의 확대와 로드맵 수립이 시급히 선결되어야 하는 함을 강조하고 싶다. 이러한 환경을 고려하여 본 논문에서는 정보보호 교육과 관련한 주요 추진현황을 살펴보고, 이로부터 현실적인 정보보호 교육 프로그램을 분석한 후, 방안을 제안하고자 한다. 본 논문의 구성은 2장에서 국내 정보보호 프로그램 추진현황을 살펴보았고, 3장에서 국

*교신저자 : 홍진근(jkhong@bu.ac.kr)
접수일 09년 10월 29일 수정일 09년 12월 11일 게재확정일 09년 12월 16일

외 정보보호 프로그램 현황을 분석하였으며, 4장에서 정보보호 인력 양성 방안 제안, 5장에서 결론을 맺었다.

2. 국내 정보보호 프로그램 추진 현황

2.1 정부 정보보호 교육 프로그램

정부기관이나 연구소를 중심으로 한 교육 프로그램이나, 중소기업과 연계된 개인정보보호 교육, 캠페인 등과 함께, 교육 수행을 위한 정규교육 과정, 정규대학인력의 배출현황(정보보호백서에서는 일부자료가 누락되어 있음), 민간교육기관이나 비정규대학의 교육현황이 제시된 바 있다[1].

2.2 국내 정보보호 교육 프로그램 비교분석

1) 국내 2년제/4년제 정보보호 교육 프로그램

[표 1] 정보보호분야별 학부 교육 교과목 현황

분야	교과목
암호&보안이론 (정보보호일반)	정보보호학개론, 암호학을 위한 대수학, 암호론, 암호기술, 정보보호기술, 최신정보보호기술, 대수학
통신/네트워크/ 응용서비스보안	DB보안, 정보보호 소프트웨어, 시스템 보안, 정보보안 및 해킹, 전자상거래보안, 인증시스템, 네트워크 보안, 바이러스와 백신, 보안프로토콜, 암호프로그래밍, 저작권보호시스템, 홈네트워크 , 정보보호시스템 설계, 스마트카드보안, 정보보호응용, 운영체제보안, 해킹 및 바이러스, 네트워크보안, 통신보안
법, 평가 인증, 정책, 관리	정보보호법과 사이버윤리, 정보보호관리체계, 정보보호 산업기술동향, 정보보호평가관리인증, 정보보호법과윤리, 서비스 보안 및 정책, 보안관리

국내 정보보호 관련 전공에서는 표1에서 제시된 바와 같이, 크게 암호 및 보안이론 분야, 통신/네트워크/응용서비스 분야, 법/평가/인증/정책/관리 분야로 나누어 교육이 이루어지고 있다.

제시된 교과목은 국내 및 국외 환경에 직접적인 정보보호 환경 반영에 일대일로 현실성을 가지고 적용된 것보다 대부분 대학 전공의 세부 특성, 관련 교수의 세부전공 특성에 따라 개설되어 운영되고 있는 것으로 파악되며, 정보보호 전공 트랙별 표준 가이드라인(요구시간, 요구과목, 이론 및 실습)이나 교과목 명칭의 일관성/통일성이 정리되어야 할 것으로 사료된다.

2) 국내 대학원 정보보호 교육 프로그램

표2에서는 대학원별 교과목 현황을 제시한 것이다. 대학원 교과과정을 살펴보면, 암호보안기술분야, 응용서비스분야, 포렌식 전문교과, 법/컨설팅/관리분야로 나누어 분류할 수 있다. 대학원 교육은 특정 전문 교과(포렌식과 같은)가 일부 구성되나 대부분이 학부교육의 심화교육 수준으로 구성되어야 진행되고 있다. 대부분 해당 대학의 전공특성에 따라 적합하게 구성 및 운영되고 있다고 판단할지 모르나, 제시된 교과목을 살펴볼 때, 비전문가라 할지라도 커리큐럼 구성이 표준화되고, 체계적인 구성(용어 표준화, 교과 내용 및 수준, 특성화된 트랙 구성 등 고려) 또한 필요함을 알 수 있다.

[표 2] 정보보호분야별 대학원 교과목 현황

분야	교과목
암호&보안기술 (정보보호일반)	암호수학개론, 고등암호수학, 양자정보이론, 암호기술분석, 정보보호개론, 침입탐지이론, 보안 기술 아키텍처, 프라이버시보호, 기초암호, 컴퓨터보안, 유한체이론, 실용암호, OS보안, 개인정보보호특론, 현대암호학, 키관리, 부채널공격방법론, 블록/스트림/공개키암호, 전자서명, 영지식증명 양자암호, 역공학기법, 암호알고리즘의 안전성 분석, 정보보안공학, 시큐어운영체제, 금융정보보호론, 계산대수학응용, 이산대수학특론, 응용대수학특론, 대수적수론, 그리드컴퓨팅보안, 침입대응통합기술
응용서비스보안	DB보안, 정보보안기술 응용, 정보보호 특강, 네트워크/시스템보안, 전자상거래 보안, 보안세미나, 보안시스템 운영실습, 유비쿼터스 보안, 유비쿼터스보안 구조/응용, 무선 및 이동통신 보안, 컴퓨터보안체제, 정보은닉, 양자계산및정보보호, 전산망보안, 정보보호시스템설계, 인터넷시스템보안, 컴퓨터바이러스, 생체인증, 멀티미디어컨텐츠보호, 모바일정보보안, 포렌식어카운팅, 악성코드보안토큰, 스마트카드기술, 고속 암호처리 기술, 복합 인증 및 서명, 사이버공격기법, AAA 서버 기술구현, 암호알고리즘의 하드웨어구현, 전자화폐, 암호프로세스설계, 암호화프로그래밍, 암호화프로세서설계, 자바프로그래밍및보안, 전자지불, 그룹서명, 비밀공유기법, 액세스제어및익명성제어기술, 시멘틱보안, 실시간시스템 , 분산시스템 보안, 임베디드실시간시스템

[표 2] 정보보호분야별 대학원 교과목 현황(계속)

분야	교과목
포렌식	사이버포렌식, 윈도우 포렌식, 파일시스템(윈도우, 리눅스) 포렌식, 네트워크/데이터베이스 포렌식, 모바일 포렌식, 시스템 포렌식, 소스 포렌식, 안티포렌식, 포렌식 툴 활용, 조사실습, 포렌식과 증거법, 포렌식과 법정대응, 포렌식과 소송절차, 포렌식실습, 네트워크 보안, 사이버보안, 정보시스템 보안, 시큐리티 인지니어링/아키텍쳐
관리, 법, 컨설팅	정보보안 정책과 컨설팅정보, 성능평가, 보안감리, 정보보호관리, 고급사이버법률, 정보보호시스템평가방법론, 국가정보학, 사이버법률 특론, 정보보호정책 특론, 정보경영특론, 정보보호컨설팅정보전, 사이버 범죄론, 개인정보보호법, 콘텐츠, 방송통신법, 저작권법, 국가안전관리론, 정보시스템 운용관리특론

3) 국내 학부 정보보호 교육 프로그램 분석

국내 학부에서 정보보호 인력 양성 및 심화된 보안 교과과정을 편성 운영함에 있어서 다음과 같은 한계점이 발견된다. 첫째 대부분의 정보보호 관련 전공 교과과정은 보안 교과목과 일반 IT 과목이 융합된 인력 양성에 초점이 맞추어져 있고, 유사전공(정보보호 복수전공자나 부전공자)의 인력 양성에서는 정보보호 교과목이 선택과목 수준으로 이해되고 있는 실정이다. 둘째 산업체에서 정보보호 인력 요구(취업)가 대부분 신입보다는 경력 위주의 현실적인 정책을 추진함에 따라 대부분의 정보보호 인력들은 정보보호 이외의 분야 취업 준비로 인해 심화된 정보보호 인력 양성에 걸림돌로 작용되고 있다는 점이다. 셋째 일반 IT 전공자의 경우 산업체와 대학간의 인턴 프로그램 등 다양한 혜택 및 집중화 프로그램이 추진되고 있으나, 정보보호 전공은 기업의 보안 문제 등과 같은 정보보호 특성상의 이유로 인턴십 프로그램, 기타 연계 프로그램 추진이 제한적이다. 상기와 같은 이유로 인해 정보보호 전공에서 보다 심화된 정보보호 교과과정 편성이 현실적인 어려움에 부딪히고 있다. 또한 국내 정보보호 교과 구성은 대학 교수진의 구성에 따라 교과과정 불균형 현상이 초래되는 것을 발견할 수 있다. 대부분의 구성이 3개의 도메인으로 구성되는데, 수학 및 관련 분야, 컴퓨터 전공 관련분야, 전자/정보통신 분야, 법/컨설팅/평가 인증 분야이다. 실제 국가에서 분류하고 있는 정보보호 분야 범위나 현실적으로 국내외 산업구조에서 요구되고 있는 산업(수익성)에 대한 비교분석이 미흡한 상태에서, 크게 3개 영역의 도메인을 중심으로 대학 교수의 전공에 따라 학습시키고 있는 것으로 파악되고 있다. 우리는 교과과정 구성에 있어서 보다 폭넓은 보안 도메인으로 확대가 필요하며, 대학별 교수특성과 환경에 따라 특성화의 필요성을 강조하고 싶다. 현실적으로 정보보호 전공 학부생을 지원하는 정부의 지원 프로그램은 전무하다고 볼 수 있다.

4) 국내 대학원 정보보호 교육 프로그램 분석

대학원 정보보호 교육과정은 특성화된 트랙별 프로그램 추진이 예상되나, 일부 대학원을 제외하고는 보편적으로 학부 교과과정에서 제한적으로 심화된 수준의 프로그램이 구성 운영되고 있는 것으로 파악된다. 우리는 도메인별 차별성이 요구되는 교과과정 편성의 필요성이나 트랙별 교육과정에 대한 표준 가이드라인을 수립이 선결되어야 한다고 주장하고 싶다.

5) 국내 공공/민간기관의 정보보호 교과과정은 민간기관 교육의 경우 자격증 중심, 시스템/네트워크/해킹 교육에 초점이 맞추어져 있다. 공공기관 교육의 경우 시스템/네트워크/해킹 기본 교육이나 전문 교육에 초점이 맞추어져 있으며, 다양한 도메인에 대한 교육에 고민해야 할 것으로 판단된다.

6) 정부의 정보보호 분류표

정부는 정보보호 분류를 네트워크 침입대응솔루션(패킷 차단 게이트웨이, NAT, 개인방화벽, 웹방화벽, 네트워크침입탐지, 통합연동, 네트워크침입방지, 악성코드 분석, 네트워크 공격유도, DDoS Sensor, 보안터널링, IPSec, PPTP, L2TP, MPLS, VPN 인증/암호용 키관리, 통합연동, 패킷분석 및 차단 , 프로토콜별 공격 코드 탐지, 고성능 대용량 트래픽 처리, 자체 방어 및 신속한 패턴 update, 사용자 및 사용자 PC 인증 및 무결성 점검, 네트워크 접근제어 보안정책 관리, 상황인지 기반 네트워크 접근제어, 취약 클라이언트 보안 강화, 응용서비스 계층 추적, 도메인 협력 기반의 IP 계층 추적, 도메인 비협력 기반의 IP 계층 추적, MAC 계층 기반 추적, IP/MAC/무선랜 위조주소 탐지)을 포함한, 호스트 침입대응, 암호알고리즘 및 안전성평가, 인증및접근제어, 보안전용칩셋, 유무선접속보안, RFID/USN보안, IT보안관리, 개인정보보호, 지식콘텐츠보안, 응용서비스보안, 재난관제, 보안모니터링, 금융보안, 바이오인식, 운송보안(자동차/항공), 로봇보안, 주력산업융합보안 등으로 분류하고 있다. 아쉬운 점은 정부가 분류하고 있는 항목을 중심으로 현재 실시되고 있는 인력 양성 프로그램이나 대학 정규 교과목을 살펴볼 때 재구성이 필요함을 발견할 수 있다는 점이다.

3. 국외 정보보호 프로그램 현황

미 정부는 다양한 정보보호 프로그램이 추진하고 있는 실정이다. 국토안보 보안 교육센터에서 추진하는 PSTP (Physical Security Training Program)에서는 접근통제를 포함한 10개의 클래스에 대한 교육이 이루어진다. 이 교육 클래스에서는 접근통제, 폐쇄된 회로 TV시스템, 업무 연속성 계획, 대량파괴 무기, 침입탐지시스템, 운영보안, 경계 조명, 보안 설계, 보안 법적 고려, 특정 이벤트의 보안 장비, 실무적인 방어 실습, 무기/폭발 탐지, 폭탄과 폭발, 컴퓨터 보안, 국내 테러리즘, 경계 병력, 잠금과 잠금장치, 경계보안, 위험 평가, 보안 정보 자원, 보안 조사 프로세스, 특정 이벤트 보안 계획, 물리적 보안 이론과 범죄, 작업장 폭력 등의 프로그램이 추진되고 있다. 미 국토안보부 교육센터의 CIPTP(Critical Infra structure

Protection Training Program)는 국가의 핵심적인 인프라 구조나 핵심 자원 보호를 목표로 국가적인 우선순위, 목표, 요구사항을 수립하기 위한 프로그램으로 CIP 개요, CIP 법과 정책, 위협 평가 프로세스, 물리적 보안, 주요 인프라구조(CI) 및 핵심 자원(KR)의 독립성과 종속성, 컴퓨터 보안(취약성과 대응책), 사례연구, 파트너십 모델과 정보 공유, 취약성 평가 계획을 주제로 교육이 이루어지고 있다. CEPT(Covert Electronic Tracking Program)에서는 전자 추적장비의 법적 사용, 디지털 증거의 보호 유지 관리, GPS, 장비의 사전설치 계획, 이동체의 다양한 모델과 타입에 따른 설치 계획, 목표 이동체에 공급전력 사용과 배터리 기술, 확장된 배터리 팩 기술, 관리자 보호를 위한 보안 팀 조직, GPS 추적 소프트웨어 운영, 어스 구글과 윈도우 라이브 로컬 프로그램 사용하는 온라인 추적 소프트웨어 사용을 위한 어플리케이션, 범죄 사례 사전 조사를 위한 GPS 정보 분석 등이 교육된다. DEASTP (Digital Evidence Acquisition Specialist Training Program)는 전자의 법과 증거, 컴퓨터 POST/부트 프로세스, 명령 프롬프트 오퍼레이션, 포렌식 하드웨어, 데이터 인식, 최종 디지털 증거 인식 실무 등의 프로그램이 진행된다. NIH(National Institutes of Health) 기관의 보안 교육 훈련 프로그램에서는 NIH 보안 프로그램, IT 리소스 사용, 정보관리, 로컬 및 원격 접근, 인터넷 안전성, 물리적 보안과 백업 UPS, 워크스테이션 기초 등을 훈련하고 있다. SCP (Security Certified Program)은 보안 인식, SCNS(Security Certified Network Specialist), SCNP(Security Certified Network Professional), SCNA(Security Certified Network Architect)에 대한 자격 인증을 실시한다. 미국 버지니아 주정부 차원에서 온라인 보안 인식 훈련이 제공되는 사례나, 2009년 프로세스 통제시스템의 사이버 보안 교육 훈련 프로그램, 호주 정부에 의해 추진되는 PSCC(Protective Security) 훈련 센터에 의한 보안 방어 실무/인증, 개인보안 인증, 고급 개인 보안 인증, 보안위험 관리, 정보/통신 보안, 보안방어관리 디플로마, 정부 조사 인증, 물리보안, 상급/실무 보안 방어 세미나, 인식 등의 프로그램이 추진되고 있다. 미 SANS(SysAdim, Audit, Network, Security) GIAC(Global Information Assurance Certifi cation) 인증은 미국 뿐아니라 국외에서도 선호되는 자격인증이다. 이 자격증은 NSA를 포함한 미 정부기관이 신뢰하는 인증이며 컴퓨터, 정보, 소프트웨어 보안의 핵심 영역에서 활동하는 사람에게 요구되는 필수 지식, 기술 보유에 대한 인증이다. SANS 교육은 크게 보안 코스, 개발자 코스, 관리코스, 감사 코스, 법, 특별 코스 등으로 구성되어 운영된다. 우리는 SANS 교육 프로그램과 정부의 보호 분류표로부터 현재의 정부기관/민간기관 및 대학기관의 주요 정보보호 교과과정의 재구성, 로드맵 수립이 필요함을 강조하고 싶다. 이러한 관점에서 미국에서 수행되는 대표적인 정보보호 프로그램인 SANS 프로그램을 아래에 제시한다.

[표 3] SANS 개발자 코스의 주요 과목

교과목
PCI 컴플라이언스를 위한 보안 코딩, 실제 웹 어플리케이션 침투테스팅, 웹 어플리케이션 침투 테스팅과 Java/JEE의 보안코딩: 방어가능한, .NET 보안코딩: 방어가능한, 웹 어플리케이션 보안 소개, 웹 어플리케이션 보안 방어 에센셜, Java/JEE 안전한 보안코딩, MS SDLC 소개, PHP 보안코딩: 방어 가능한 어플리케이션 개발, C 보안코딩: 방어가능한, 웹 어플리케이션의 안전한 코드 리뷰, 소프트웨어 보안 인식

[표 4] SANS 관리자 코스의 주요 과목

교과목
보안 인식 프로그램을 수립하는 법, 관리자를 위한 안전한 웹 서비스, SANS® +S™ 교육훈련 프로그램(CISSP® 인증 시험), SANS 관리자를 위한 보안 리더십 에센셜™, SANS 27000 구현과 관리, 보안 전문가와 관리자를 위한 프로젝트 관리 및 효과적인 통신, 관리자를 위한 해킹, 보안정책과 인식, 핵심적인 인프라 보호정보보호 정책의 기본, SANS 리더십과 관리 능력, IT에서 윤리, 시스템과 어플리케이션 보안의 실무 개요, IT서비스 관리 에센셜(IT 보안전문가를 위한), 비즈니스 실행을 위한 정보보호

[표 5] SANS 보안코스의 주요 과목

교과목
IPv6, 보안에센셜 훈련, 해킹/익스플로잇/사고대응 훈련, 컴퓨터 포렌식/조사/응답, 넷 침투테스팅/윤리적해킹, 심층 침입탐지, 무선 윤리적 해킹/침투테스팅/방어, 윈도우보안, 심층 경계보안, 정보보호 개론, 오라클 보안, 역공학(멀웨어 분석도구 및 기법), 유닉스/리눅스 보안, 최첨단 해킹, 침투테스터를 위한 메타플로잇, 고급 파일시스템복구 및 메모리포렌식, 고급정보 감시정찰, 무선보안, 정보보호 처리를 위한 심층윈도우 명령 라인, 심층 FAT 파일시스템, 컴퓨터 네트워크 보안 인식, 네트워크 보안 기초 및 위협, 해킹된 무선 라우터를 네트워크 보안프로젝트, SANS교육훈련(Comp TIA Security+ Cert ification (4 days) 코스), 네트워크 세그먼트를 위한 전략, 시스템 관리자를 위한 보안 구조, 심층 로그 관리, 보안/포렌식/트러블슈팅, GSEC 시험준비와 리뷰, 네트워크 포렌식, 컴퓨터 포렌식 에센셜, 네트워크 침투테스팅: 레포트, 익스플로잇, 명령쉘의 인터넷 상 개인 프라이버시 보호, 윈도우 포렌식, 역공학 멀웨어-부가적인 도구와 기법, 침투 테스터와 보안 연구자를 위한 익스플로잇, 멀웨어 역공학: 멀웨어 에센셜, DB 활동 모니터링 시스템, 고급 보안 에센셜-엔터프라이즈 방어, 모바일포렌식, 가상화 보안과 운용, 이해 가능한 패킷, IPv6 에센셜, VoIP보안, 심층 방어의 핵심적인 20개 보안 통제, 핵심적인 20개의 보안 통제 (계획, 구현, 감사), 드라이브와 데이터 복구 포렌식

[표 6] SANS 감사 코스의 주요 과목

교과목
네트워크/경계/시스템 감사, IT 보안 감사와 통제 에센셜, 최소 기준: PCI/DSS 1.2, SANS® +S™ 교육훈련(ISACA® CISA® 인증시험), Java 품질 보증/보안 테스팅, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) 위험평가 방법론, IT 보안 감사 에센셜, 웹 기반 어플리케이션과 고급 시스템 감사

[표 7] SANS 법 코스의 주요 과목

교과목
정보기술과 정보보호 법적 이슈, 정보기술에서 법적 이슈, 비즈니스 법과 컴퓨터 보안, 데이터 보안과 다른 기술계약, 떠오르는 위협에 대한 법 적용, IT 컴플라이언스 법(조사)

4. 정보보호 인력 양성 방안 제안

4.1 정부기관 내 교육 기능 및 인증 기능 강화

1) 교육 기능을 강화하자. 국내 NIS/사이버안전센터, 인터넷진흥원(구. KISA) 등을 포함한 정부 정보보호 관련 기관의 교육 기능을 강화하자(국내 자격증 인증 기능 강화 및 국외 인증 연계 프로그램의 추진, SIS 인증의 강화, 정보보호 도메인별로 자격증 인증 프로그램의 다양화 필요).

[표 8] SANS 특별 코스의 주요 과목

교과목
침투테스팅 서밋: 침투테스팅과 윤리적해킹, DIACAP(DoD Information Assurance Certification and Accreditation Process) + 인증 : In-Depth, (ISC)2® Certified Secure Software Lifecycle Professional (CSSLPCM) CBK® 교육 훈련 프로그램, Vendor Solutions Expo, SCADA (Supervisory Control & Data Acquisition,원격감시제어 데이터수집시스템) & 프로세스 통제 보안 서밋, 어플리케이션 보안 서밋 - Consensus Audit Guidelines (CAG) 자동화 도구, 중역을 위한 정보보안 통찰력 프로그램, 데이터 노출 예방과 암호에 관한 서밋, 가상화 보안에 관한 서밋

2) SANS 등과 같은 국외 기관 훈련교육의 연계 프로그램에 대한 추진이 필요하다.

3) 현재 진행되는 교육 프로그램의 다양화 및 다변화가 필요하다. 첫째 정부기관 주도의 자격증 교육의 확대 및 다변화(보안 관리를 포함한 전체 보안 도메인에 대한 이해와 이를 기반으로 다양화, 다변화된 교육 방안 마련이 요구)가 필요하다. 둘째 다양화되고 다변화되는 교육은 집중화 및 구체화를 필요로 한다(앞서 제시된 SANS 프로그램 참조). 현재 국내 대학원의 경우 특정 테마를 주제로 집중 및 구체화 프로그램이 일부 추진되고 있는 사례가 있다.

4.2 대학 지원 프로그램

1) 학사 운영 지원 프로그램과 관련하여, 일반 대학의 교과과정에 IT 교과목이 일반교양 필수 과목으로 편성 운영되고 있으나, 정보보호 중요성을 고려하여 교양 필수 교과목으로 편성될 수 있는 제도적 관리가 필요하다. 또한 사법대학이나 교직을 이수하는 과목에 정보보호 관련 교육을 필수 교과목으로 편성을 유도하는 것도 고려할 수 있다.

2) 전공/전공연계 학부생을 중심으로 인력 양성 지원 정책이 필요하다. 정부나 지자체와 대학간 전공연계에 대한 정보보호 관련 대학 인턴십 프로그램 지원이 요구된다. 현재 다른 전공분야에서는 추진되고 있는 정책이나 정보보호 분야에서는 제한되어 있다. 군무원 및 군 전산병, 통신병 등 부서나 분야에 정보보호 인력을 배치시키는 활성화 정책이 요구된다.

3) 인력 양성을 위한 재정적인 지원이 필요하다. IT를 포함한 다른 전공에 대한 재정적인 지원이 이루어지고 있는 현실에서 정보보호 관련 정부의 재정지원 프로그램은 절실하다. 공통교과 구성을 위한 교육 및 기자재 지원 프로그램이 필요하다. 정보보호 교육을 위한 실제적인 테스트베드를 구축하고, 이 환경을 대학별 공동 이용/운용하거나, 정보보호 인증제 프로그램 지원사업(예, Next 공학인증제 지원사업)을 통해 정보보호 권장교과목 선별, 로드맵 구성하며, 학부 및 석박사 과정이 연계되도록 구성하는 표준화된 교과과정 수립이 필요하다.

4) 교육기관을 정부기관과 클러스터 묶어 인력 양성 도입이 필요하다. 정보보호 대학 전공을 지역별, 특성별, 테마별로 클러스터를 구성하여 인력을 양성하는 지원책이 필요하며, 대학원 중심의 연구기능 강화가 아닌 학부 중심의 대학생에게 실질적인 혜택이 주어지는 현실적인 지원책 마련이 필요하다. 또한 클러스터의 핵심은 대학이 아닌 지자체 기관/출연기관(테크노파크 등과 같은)의 교육센터에서 주관하고, 지원되는 재정으로 테마별(관리, 해킹, 법, 웹보안, 포렌식 등) 주요 인력 양성(학점교류/인정, 수료시 취업 연계)을 추진할 수 있도록 구성한다. 또한 이 프로그램에 참여하는 대학 인력은 일정 비율(전공 학생수 대비)로 배분하여 참여하도록 한다. 추가적으로 교육 기관을 중심으로 자격증 양성 과정을 추진하여 효율성을 높이도록 유도한다.

4.3 정부/기업 지원 프로그램

1) 정부기관, 연구소 발행 간행물의 교육기관 관련 전공 및 관리자에 배포/보급하자. 전문적인 기술요령/보고서 자료를 정보보호 전공 교육자나 관리자에게 배포 보급을 통하여 효율적인 교육이 가능하다.

2) 정보보호 관련 정부기관, 연구소 중심의 교육 프로

그램/행사를 지원하자. 교육 기관 교육 대상자가 정보보호 교육에 참여할 때 무료 또는 실비 교육이 가능하도록 지원한다. 이 프로그램은 관련 전공교수/조교 등에 대한 실무 심화교육, 신설 교과목 교육 확대에 기여할 수 있다. 또한 교육 프로그램의 정비 및 체계화, 표준 로드맵 수립(기관별, 센터별로 분산되어 있는 교육 내용이나 수준 점검)이 필요하다.

3) 중소기업과 연계된 교육 프로그램을 추진하자. 현재 대부분의 중소기업이 정보보호 관련 교육은 기본 교육수준에 머물러 있다. 그러나 최근 많은 중소기업들의 정보화 지수가 증가하고 있다. 일반 중소기업의 정보화 시스템 구축 보급률이 높게 나타나고 있으나, 여전히 정보보호 인식은 낮다. 중소기업 지원 프로젝트에 정보보호 관리자 편성을 유도하고 과제 개발 중이거나 사후 관리 체계에 정보보호 관리 대책 수립이 요구된다.

4) 정부의 국책사업/과제 추진과정에서 기업의 보안 담당자가 참여하도록 하자. 정부가 지원하는 사업에 지원하는 중소기업은 나름대로 정보보호 대책을 마련하여 추진할 수 있도록 한다. 민간 업체는 정부사업에 지원할 때 정보보호 담당자 선정 및 전담부서를 배치할 때 가점을 부여하는 정책을 추진하고, 정보보호 자격증 소지자가 관련 과제에 참여하도록 유도한다. 현재 대부분의 중소기업은 경영기획 관리 인원이 정보화 업무를 겸직하는 수준에 머물러 있다.

5) 국가 정보보호 전담부서 운영을 확대하자. 정부나 지자체 유관부서에서는 정보보호 전문가 설치를 유도하고(관련 자격증 소지자), 정보보호 전문인력이 관련부서에 응시할 경우 가점을 부여하는 방안을 고려하는 것이 필요하다.

6) 민간 정보보호 컨설팅 업체 지원 프로그램 실시하자. 국내 주요 정보보호 업체에 대한 정부의 재정 지원 프로그램을 정보보호 관련 전공자 인턴쉽 프로그램(대학별 일정비율로 인턴쉽 수용이 가능하도록 유도)이나 연계 프로그램(실무능력 배양, 기술 자격증 취득 유도)과 공동으로 추진하게 한다.

4. 결론

본 논문에서는 정보보호 인력 양상방안을 제안함에 있어 종래의 국내에서 실시되고 있는 정보보호 주요 현황을 정부기관, 민간기관, 대학기관으로부터 살펴보았으며, 국외 주요 보안 프로그램의 현황을 검토하였다. 정부의 주요 보호 분류표와 국외 주요 프로그램의 커리큐럼, 국내 정보보호 주요 류표와을 연결하여 검토할 때, 보다 효율적인 정보보호 인력을 양성하기 위해서는 표준 가이드라인, 로드맵과 함께 적절한 지원 방안 정책이 마련되어야 함을 알 수 있었다.

참고문헌

[1] 국가정보보호백서 2009-2006.

[2] 전국대학의 정보보호 전공 웹사이트(교과과정)

[3] 정원일, 하재철, “공학교육인증을 위한 정보보호학 심화프로그램,” 정보보호학회지, 제19권 제1호, 2009.2

[4] 김지숙, 최명길, “국기기관의 정보보호수준평가에 관한 연구,” 한국정보보호학회지, 제18권, 제6호, 2008. 12, pp.6-10.

[5] 김태성, 김민정, 김종하, “정규교육기관을 통한 정보보호인력 양성에 대한 연구,” 한국정보보호학회지, 제14권, 제4호, 2004. 8, pp.78-91.

[6] 유혜원, 김태성, 전효정, “정보보호 분야 지식 및 기술 수요,” 정보보호학회지, 제19권, 제1호, 2009. 2, pp.23-28.

[7] 김태성, 전효정, “AHP를 이용한 정보보호 인력 양성정책 분석,” 한국통신학회논문지, 제31권 5B호, 2006.

[8] 전효정, 유혜원, 김태성, “정보보호 분야 직무별 필요지식 및 기술 분석,” 한국경영정보학회지, Vol.10n No.2, 2008. 8.

[9] 정보통신연구진흥원, 정보보호 실태조사, 2005.

[10] 김태성, 김길환, 박현민, 임대은, “정보보호 인력 교육훈련 프로그램 운영전략,” 한국경영학회 통합학술대회 2007.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2008년 12월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안