

정보보호 인력양성 방안에 관한 연구

이형우*, 이민섭**

요약

본 연구에서는 대학 및 정보보호 관련 교육기관을 중심으로 활발히 진행되고 있는 정보보호 인력양성 과정 및 체계를 살펴보고 정보보호 산업 현황을 분석하여 정보보호 인력 양성 방안을 살펴보았다. 우선 정보보호 인력의 기준 및 조건을 검토하고 정보보호 인력이 갖추어야 하는 전공 지식 분야를 분류하였다. 특히 정보보호 교육기관에서의 정보보호 관련 전공 및 유사전공을 통해서 수행되는 인력양성 방안을 기초로 산업계에서 필요로 하는 정보보호 인력양성 방안을 고찰해본다.

1. 서론

최근 우리나라에서는 대학 및 대학원의 정보보호 관련 유사 전공학과와 최근 개설되고 있으며 학부 과정에서의 정보보호 전공, 대학원 과정에서의 정보보호 관련 학위과정, 사실 교육기관에 의한 정보보호 인력 양성 및 정보보호 산업체 등에서 정보보호 관련 전문 개발 인력을 양성하고 있다.

특히 현재까지는 주로 특수대학원을 포함한 대학원에 정보보호전공 과정이 개설되어 있어 전문 인력을 양성하고 있으나, 학부 과정에서 정보보호전공 과정이 개설된 곳이 많지 않아서 체계화되고 연계성을 갖는 정보보호 교육 및 인력 양성 방안이 제시될 필요가 있다.

정보보호 교육을 시행하고 있는 국내 대학의 여건을 살펴보면 급변하는 인력 수요에 신속하고 효과적으로 대응이 필요하다고 할 수 있다. 현재 주요 대학에서 정보보호 관련 유사학과를 통해 정보보호 관련 학과목을 개설하고 있으나, 일차적으로 인력양성에 필요한 교수진이 부족하고 개설 교과과정 역시 다양한 형태로 구성되어 개선의 여지가 있다.

이에 정보보호 전공의 운영 방안에 대한 연구나 기업 및 관련 기관에서의 정보보호 교육을 통해 정보보호 인력을 양성하는 방안을 고찰해 보고, 정부

및 산업체와 연계된 측면에서 정보보호 인력 양성 방안에 대해 고찰해 보고자 한다. 물론 단순히 양적인 측면에서의 인력 양성이 아니라, 질적으로도 전문 지식과 소양을 갖춘 정보보호 인력을 양성하는 방안을 고찰하여 앞으로의 정책 방향을 수립하는데 참고가 되었으면 한다.

2장에서는 정보보호 산업 현황을 분석하여 정보보호 인력 양성의 필요성을 제시하고, 3장에서는 정보보호 인력의 기준 및 조건을 제시하고 정보보호 인력이 갖추어야 하는 지식 분야를 고찰하였다. 4장에서는 정보보호 전공 및 유사전공을 통한 인력양성 방안과 연계 전공 및 부전공 등 대학에서의 인력양성 방안 모델을 제시한다. 또한 산업계에서 필요로 하는 정보보호 인력양성 방안을 고찰해 본다. 5장과 6장에서는 정보보호 인력양성과 관련된 향후 전망을 고찰하며 결론을 맺는다.

II. 정보보호 인력 현황

1. 정보보호 산업 현황

최근 들어 해킹과 컴퓨터바이러스 등 사이버상의 불법행위가 급증하면서 정보보호산업이 급성장하고 있다. 국내 정보보호산업은 시장규모가 급격히 증가

* 한신대학교 소프트웨어학과 조교수(hwlee@hanshin.ac.kr)

** 단국대학교 첨단과학부 응용수학전공 교수(msrhee@dankook.ac.kr)

하고 있다. 정보화가 급진전되면서 전자거래가 보편화됨에 따라 정보화사회의 파수꾼역할을 하는 정보보호산업이 새로운 산업으로 각광받고 있다. 현재 정보보호업체를 대표하는 한국정보보호산업협회의 등록 업체 수 역시 급속도로 증가하고 있다.

정보보호산업규모가 급성장하면서 정보보호산업인력에 대한 수요도 급증하고 있으나 아직까지는 인력공급이 충분히 이루어지지 못하고 있다. 특히, 정보보호산업체가 대부분 창업 3년 미만의 중소벤처업체로서 신규인력을 충원해 교육시킬 여력이 없어 경력이 있는 전문가를 요구하는 것도 정보보호 산업인력부족의 큰 요인으로 지적되고 있다. 정보보호산업을 대상으로 한 설문조사에서 기술개발과 제품생산의 가장 큰 애로요인으로 전문인력의 부족을 꼽았을 정도로 정보보호 산업인력의 부족은 업체들의 큰 어려움 중의 하나라고 볼 수 있다[1].

정보화 정책과 편리성에 기인해서 2002년 현재 인터넷 이용자수 2,400만명, 초고속 인터넷 가입자 800만명, 전자상거래 규모 110조원 초과 등 가입 및 이용 기준의 정보화 수준이 세계 최고 수준에 이를 정도로 고도화되었다. 정보화 사회 속에서 다양한 인터넷 이용을 통해서 순기능 및 역기능적인 측면이 나타나게 되었으며 역기능에 대한 정보보호가 필요하게 되었다.

국내 정보보호 산업은 2007년에 1.8조원 규모로 연평균 35%의 성장이 전망이 되면서 정보화의 역기능에 의해서 주요 정보통신 기반에 대한 해킹과 바이러스 등 사이버공격에 대해 국가적인 탐지 및 대응 체계의 구축과 민간부문의 신뢰성 있는 전자거래, 주요 인프라에 대한 효율적·체계적인 정보보호환경 마련이 필요하게 되었다.

현재 정보보호 분야 종사자는 아래 [표 1]과 같이 2003년도 2,500여명 정도 부족하며 2007년도에는 7,000여명으로 확대되어 전체적으로는 20,000여명이 부족할 것으로 예상된다.

[표 1] 정보보호 인력 수급 전망

구분	2003	2004	2005	2006	2007	합계
인력수요	3,876	4,990	6,434	8,283	10,671	34,254
인력공급	1,312	1,688	2,172	2,795	3,596	11,563
수급차	-2,564	-3,302	-4,262	-5,488	-7,075	-22,691

인력수급불균형이 지속적으로 확대됨에 따라 인력공급을 양적으로 확대할 수 있는 대책이 필요하다.

또한 인력수급의 양적인 불일치 외에 인력수준의 불만족 등 질적인 측면(수준, 시점, 분야)에서도 수급 불균형이 나타나고 있다. IT전공자의 재교육, 전환교육, 학제간 전공설치 등을 통해 다양한 수준의 정보보호인력 양성이 필요하다.

결국, 앞으로의 수요에 기반하여 정보보호 인력양성 체계를 정비하고 산업현장의 수요를 반영하여 대학의 교육과정을 조정할 필요가 있으며, IT 인력 전환 등을 탄력적으로 운영하여 효율적인 인력양성을 수행해야 할 것으로 판단된다. 특히 정보보호교육을 위한 교육교재, 교육환경, 강사인력, 교육기관 등 교육환경을 조성하고, 지속적으로 정보보호 인력수급에 관한 통계분석을 실시하여 적절히 대처할 필요가 있다. 정보보호 산업에서 필요로 하는 인력 현황과 전망은 아래 [표 2]와 같다^[6].

[표 2] 정보보호산업 필요인력 현황 및 전망

(단위 : 백만원,명)

	2003	2004	2005	2006	2007
매출규모	646,756	888,160	1,117,606	1,465,964	1,856,936
산업종사인력(A)	5,879	8,074	10,160	13,330	16,881
연구개발인력(B)	3,250	4,264	5,110	6,369	7,581
B/A x 100(%)	55.28	52.81	50.29	47.78	44.91

정보보호인력을 배출하는 기관은 아직까지 부족하다고 할 수 있으며 정보보호진흥원이나 정보통신교육원 등에서 단기 교육과정을 운영하고 있다. 대학에도 정보보호전공을 개설한 학교가 일부에 그치고 있어 대부분의 인력은 정보보호업체들이 자체교육 및 재교육 과정 등을 통해 확보하고 있는 실정이다.

2. 정보보호 인력양성의 필요성

정보보호 시장의 성장 속에서 정보보호 기반의 유지와 발전을 위해서 많은 정보보호 인력이 필요하게 되었다.

첫째, 급속한 정보화 진전에 따라 정보시스템에 대한 의존도가 증가하고, 정보보호 문제가 정부, 기업, 개인 등에 걸친 범국가적 의제로 등장하게 되었고 전반적인 정보화 수준에 비해 정보보호 의식이 매우 낮고 관련 부문 투자도 부족한 현실에 있다. 따라서 정보보호의 중요성을 정보기반 이용자들에게

인식을 시키고, 인식수준을 제고하고, 인식기반을 전 국민적으로 확산시킬 필요가 있게 되었다.

둘째, 정보보호 산업의 급속한 성장에 따른 전문 인력에 대한 수요의 증대에 대해 현행 인력양성 체계로는 충분한 공급을 하지 못하고 있으며 정보보호 산업체 대상의 설문조사에서 기술개발과 제품생산의 가장 큰 어려운 요인으로 전문인력의 부족을 꼽고 있다. 그리고 정보보호 부문은 일반적으로 타 IT부문의 인력보다 높은 수준의 인력을 필요로 하고 있고, 알고리즘 및 프로토콜 등의 핵심기술개발에는 고급 수준의 전문인력의 집중양성이 필요하다.

셋째, 현재 정보보호 부문은 전반적인 IT 부문과 통합화 및 대형시스템화 되어가고, 주요 민간 및 공공시설에 대한 사이버테러 등 사회적 이슈에 민감하게 반응하며 이에 따라, 장기적인 소요인력 분야 및 규모에 대한 수급 분석에 기반하고, 급변하는 시장 수요에 탄력적으로 대처할 수 있는 인력 양성 체계의 확립이 요구되고 있으며 궁극적으로 수요의 양적·질적 성장 및 다양화에 대비할 수 있는 인력 양성 체계의 수립이 요구되고 있다.

따라서 정보보호 인력은 국가 정보보호 발전과 유지를 위한 필수 요인이므로 국가 및 민간 차원의 정보보호 인력양성 방안이 제시되어야 한다.

III. 정보보호 인력

1. 정보보호 인력의 기준 및 조건

정보보호 인력을 양성하는 방안에 대해 고찰하기 이전에, 정보보호 인력의 기준과 조건에 대해 살펴보고자 한다. 이를 통해 정보보호 인력에 대해 정의할 수 있을 것이며, 향후 바람직한 정보보호 인력 양성 방안을 수립할 수 있을 것으로 판단된다.

현재 정보화의 진전으로 전자상거래가 활성화되고 각종 경제활동에서 정보통신시스템에 대한 의존도가 심화되면서 전산망 해킹이나 컴퓨터 바이러스 등 사이버 테러 위협요인도 증가하는 추세이다. 이에 따라 정보보호 전문인력에 대한 기준 및 조건도 변화하고 있다. 정보보호 인력에 대한 기준은 조금씩 변화하고 있다. 특히 IT 기술의 발전으로 인해 필요로 하는 정보보호 인력의 자질 역시 변화하고 있다. 따라서 정보보호 인력을 한 가지 기준에 따라 정의할 수는 없는 것이 사실이다.

시대적인 흐름을 반영하면서도 가장 적절한 형태

의 자격 기준을 제시하고 있는 것 중에 하나는 정보보호 관련 자격증일 것이다. 정보보호 인력의 기준을 파악하기에 가장 적합한 기준은 정보보호 관련 자격증을 부여하는 기준을 통해 판단할 수 있다. 예를 들어 인터넷 보안 전문가인 경우는 사단법인 한국정보통신자격협회에서 운영하고 있는 자격으로서 서버 보호와 복구, 보안 설정과 분석, 해킹 방지 등 서버에 대한 해킹에 효과적으로 대처하고 정보를 보호할 수 있는 인터넷 보안 관련 기술력 보유여부를 요구하는 직무내용으로 이를 측정하고 평가하여 자격을 부여하고 있다. 구체적인 자격등급과 검정기준은 [표 3]과 같다.

[표 3] 인터넷 보안 전문가 자격의 등급과 검정 기준

자격명칭		검정기준
인터넷 보안 전문가	1급	Unix, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해 사고 대응, 해킹예방, 시스템 분석 등의 전문능력을 검정
	2급	Linux, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해 사고 분석 및 대처의 실무능력을 검정

인터넷 보안 전문가 자격증을 이수하기 위해서는 아래 표와 같이 기본적인 교과목을 이수하였으며 인터넷 기반 보안 관련 사항을 이수한 자를 정보보호 인력이라 평가하고 자격을 부여할 최소 기준으로 본다. 또한 시스템 보안 관리, 시스템 침해 분석, 방화벽 구축, 침해 상황 분석, 침해 상태 분석, 침해 과정 분석, 기타 침해 분석, 해결책 및 예방책 제시, 시스템 관리, 사용자 관리, 보안 관리, 서비스 관리, 암호, 코드, 바이러스 분석 등의 과목을 이수한 자를 협의의 의미에서 정보보호 전문인력이 필요로 하는 기본 지식으로 갖춘 자라 할 수 있을 것이다^[2].

구체적으로 정보보호 인력에 대한 자격증을 부여하는 과정에서 시행하는 필기시험의 경우 정보보호 개론, 운영 체제, 네트워크, 보안, 암호와 시스템 언어 등 5과목을 평가한다([표 4] 참조).

국제공인 정보 시스템에서의 정보보호 전문가를 평가하는 기준에서는 정보 시스템 보안과 연관된 지식과 기술을 습득한 보안업무 종사자, 보안 감시자, 보안 컨설턴트, 보안 제공업자, 컴퓨터 범죄수사관, 보안제품 개발자 등 실제로 보안과 관련한 정규직원으로 3년 이상 근무한 경력을 요구하고 있다.

(표 4) 인터넷 보안 전문가 자격의 검정 과목과 검정 내용

검정과목	검정내용
정보보호 개론	정보보호개요, 운영체제 보안, 네트워크 보안, 서비스 보안, 정보보호 제도 및 관련기관, 정보보호 관리 및 해킹동향, 정보보호 윤리 등
운영체제	사용자 관리, 인터넷서비스 관리, 시스템 관리, 보안 관리 등
네트워크	네트워크 개론, 토폴로지/아키텍처, 네트워크 계층, 네트워크 전송매체, 데이터 통신망, TCP/IP 구조/분석, TCP/IP 프로토콜, 라우팅/어드레싱/서브네틱 등
보안	서버보안, 서비스보안, 방화벽, 악성 소프트웨어, 주요 해킹방식 및 대비책
암호, 시스템 언어	암호개론, 암호알고리즘, 암호프로토콜, 코드, 어셈블러, 유닉스 c(셸 스크립트) 등

국제공인 시스템 보안 관리자(SSCP : Systems Security Certified Practitioner) 역시 위협평가, 보안 정책 및 서비스 계획, 개발 및 구성, 보안 환경에서의 검정, 평가, 경영, 도구 접근 제어, 인증, 원격통신 제어, 실행 및 체계 모니터, 리뷰, 긴급사고 복구 수행, 부당 코드 대응, 경영 및 실행 변화에 따른 강화, 긴급 반응, 시스템 복구, 보안 경고, 보안기초 이해, 기술 및 실행 유지, 조직 내·외 중재 등과 같은 직무수행을 기대하게 된다.

한국정보보호진흥원 역시 정보보호 교육사업과 정보보호 학술연구활동을 지원하고 있다. 정보보호 산업체 특화과정(보안운영 전문실무과정, 전자서명 인증관리체계 운영자과정, 개인정보보호 전문교육과정, CC기반 평가준비과정)과 주요 정보통신기반시설의 취약성 분석 등의 업무를 수행할 정보보호 컨설턴트를 양성하기 위한 정보보호 전문업체 교육과정, 정보통신 관련학과 석·박사 과정 대학원생들을 대상으로 대학원생 정보보호 기술교육과정 등을 시행하고 있다.

이상과 같이 정보보호 전문인력의 기준을 판단하기 위해 전문 자격증을 중심으로 살펴봤으며 이를 통해 산업체에서 필요로 하는 정보보호 전문인력의 조건을 판단하여 정보보호 인력의 기준을 반영하고 있다고 할 수 있다.

2. 정보보호 인력이 갖추어야 할 기본 지식 및 분야

일반적으로 정보보호 인력이 갖추어야 할 기본적인 지식에 대해 고찰해 보면 아래와 같다. 사이버 공간을 통한 정보 침해의 양상이 다양화, 지능화되고 새로운 정보통신서비스가 등장함에 따라 정보보호 기술의 발전도 더욱 가속화 될 전망이다. 특히 정보통신망의 고도화로 전송 트래픽이 급증함에 따라 통신망의 부담을 최소화하고 정보의 안전한 전송을 보장할 수 있도록 정보보호 기술의 고속·고비도화가 진전되어야 하며, 통신기술과의 융합도 가속화

될 전망이다.

IMT-2000, 무선 LAN 등을 이용한 무선 인터넷의 보급이 급증하여 유·무선 통합 환경이 보편화 될 것으로 예측됨에 따라서 보안 취약점을 해결할 수 있는 방안이 제시되어야 한다. 또한 인터넷이 IPv4망에서 IPv6망으로 전환되고 궁극적으로는 전체 통신망이 All IP 망으로 단일화됨에 따라서 이에 대한 정보보호 기술 연구도 활발히 진행되고 있다.

전자거래, 전자정부 서비스 등 응용 서비스가 널리 보급됨에 따라서 전자거래의 안전성을 확보할 수 있는 기술과 인증기술 및 언제 어디서나 간편하게 서비스를 제공받을 수 있는 이용성 확보 기술 등이 널리 확대될 것으로 판단된다.

정보보호 패러다임도 방화벽, 침입탐지 시스템 등의 단일 기술을 이용하여 외부의 전자적 침해를 단순히 차단하는 현재의 수동적인 보안 기술에서 새로운 침입에 대한 실시간 탐지와 차단이 가능하고 복구, 역추적, 대응 공격 등을 적극적으로 수행하는 능동형 네트워크 보호 기술로 변화하고 있다.

정보보호 전문인력이 갖추어야 하는 지식 역시 인터넷보안 전문가 과정을 중심으로 판단해 보고자 한다. 인터넷보안 전문가로서 갖추어야 할 요건은 전문 지식과 전문적 기능으로 나눌 수 있는데 먼저 지식에는 보안관련 법률지식, 인증·전자서명, 각종 OS 등이 있으며, 기능에는 보안사고 조사/분석/진단/대응과 보안정책 자료수집/조사/평가/분석/진단/대응이 있다. 예를 들어 인터넷보안 전문가로서 갖추어야 할 지식과 기능은 다음과 같다^[3].

2.1 인터넷보안 전문가로서 갖추어야 할 지식

가) 보안관련 법률지식

- 정보통신망이용촉진 및 정보보호 등에 관한 법률시행령, 공공기관의 개인정보보호에 관한 법률 시행령 등에서의 "정보통신망과 정보시스템

- 의 보호조치"에 관한 부분
- 산업기술기반 조성에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등에서의 "데이터의 부정조작·변조범죄·정보시스템 및 데이터 손상 파괴"에 관한 부분
- 나) 인증, 전자서명
- 공개키의 위·변조 문제 관련 부분
 - 위조 불가, 서명자 인증, 부인방지, 변경불가, 재사용불가 관련 부분
- 다) TCP/IP 구조 및 체계
- OSI(Open Systems Interconnect) Reference Model 각층 개념
 - TCP/IP 프로토콜의 구조 및 문제점 진단, 진단도구, 해결, 주소체계
- 라) SSL, X.25
- 개념 및 프로토콜 구조
- 마) Kernel보안
- 사용자 식별 인증 및 객체 재사용 보호
 - 강제적/임의적 접근 통제 및 감사(audit)
 - 침입탐지(intrusion detection)
- 바) Scanner, Hacking/Cracking
- saint, courtney, nmap, portsentry 정도
- 사) rootkit, Buffer Overflow
- LKM, 등
 - Buffer Overflow 공격유형
- 아) Packet Sniffer, IP Spoofing
- sniffit, tcpdump, netlog 등
- 자) OS의 이해
- Unix, Linux, Wdow98/XP, WindowsNT, Windows2000
- 차) 네트워크 보안
- 네트워크 보안 서비스 및 메커니즘
- 카) DBMS(database management system)
- Oracle, MS SQL, MySQL
- 보안 DBMS를 설계하고 구현하는 접근방법
- 타) 바이러스/백신/트로이목마/웜/논리폭탄/트랩도어/악성자바애플릿/악성 ActiveX
- ## 2.2 인터넷보안 전문가로서 갖추어야 할 기능
- 가) 보안사고 조사/분석/진단/대응
- 각종 로그 조사(방화벽, 라우터로그, syslog, lastlog, accesslog등)
 - 백도어 조사, 분석
 - 활동내역 리스트 작업
 - 복구 및 사전차단 시스템점검, 신고
- 나) 요구사항 작성/분석
- 현재 시스템 파악, 의뢰자 요구사항 분석, 차단 시스템 구축 자료
- 다) 보안기술 적용
- IP 마스크레이팅, IPchain 등
- 라) 시스템서비스 관리
- 사용하는 서비스의 중지 및 각 서비스 패치 등
- 마) 보안시스템 지침서 작성
- 관리, 시스템 감시, 지속적인 업데이트
- 바) C 언어 코드 분석/작성 기능
- 사) 보안정책 자료수집/조사/평가/분석/진단/대응
- 보안비용, 기능성, 외부네트워크와 상호 호환성, 법적문제 등
- ## IV. 정보보호 인력양성 방안
- ### 1. 정보보호 전공/유사전공을 통한 인력양성
- 정보보호 인력이 갖추어야 하는 기본적인 지식 및 전공내용을 대학 현황을 통해 분석하면 다음과 같다. 정보보호 분야는 기본적으로 수학, 컴퓨터과학, 전자공학 등을 기반으로 정보통신, 경영, 법학 등과 연결된 통합학문의 특성이 강하다.
- 불법도청 방지, 변조 및 위조 방지, 무결성 입증, 인증, 방화벽, 침입탐지시스템(IDS) 등의 통신망 보안, 해킹 및 바이러스 방지, 리눅스 등의 OS 보안,

데이터베이스 보안 등의 시스템 보안, IC 카드보안, 저작권보호기술(watermarking 기술)의 콘텐츠 보안과 PKI 서비스, CA 솔루션 제공, 전자상거래 보안 등의 PKI 서비스 분야, 보안정책, 보안관련 법 등이 관련되기 때문에 대학 전공 과정을 통한 체계적인 인력양성이 필요하다. 대학에서의 정보보호 인력 양성을 위해서는 2년 또는 4년간의 전공 교육과정을 이수하게 된다. 구체적으로 수학 분야, 전자 및 통신 분야, 컴퓨터 공학 분야 및 보안 복합 분야 등에 관한 지식을 학습하게 된다.

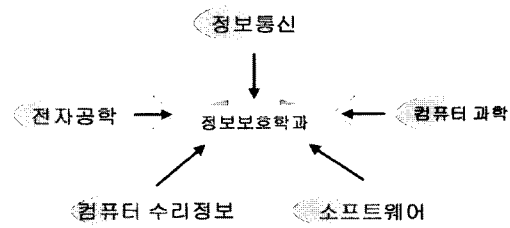
[표 5] 정보보호 전문가의 지식기반

분야	교과목
수학분야	대수학, 이산수학, 정수론, 암호학, 확률/통계학 등
전자 및 통신분야	암호프로토콜, 데이터통신보안, 인터넷보안, 전자상거래보안 등
컴퓨터 공학분야	데이터베이스, 자료구조, 운영체제보안, 컴퓨터 시스템보안, 네트워크 보안 등
보안복합분야	해킹 및 바이러스, 침입탐지기술, 응용 서비스보안 등
기타분야	정보보호법, 평가 및 인증, 프로젝트 등

결국 정보보호 전공에서는 수학 관련 전공, 응용물리학 관련 전공 등을 기초적으로 이수한 후에 전기, 전자 및 통신 기초 이론을 학습한다. 상위 과정에서는 컴퓨터과학 관련 전공과 기타 복합 전공 등에서 필요한 정보보호 교과목을 이수한다면 전공 지식을 갖춘 전문 인력으로 발전할 수 있다. 또한 실습 교과목이 적절히 병행되어 실제적인 정보보호 인력을 양성할 수 있는 토대를 제공할 수 있을 것이다. 한편 정보보호 유사 전공과정을 통해 기초교육을 실행하고 산학 연계를 통해 프로젝트 중심의 실습을 겸비한다면 정보보호 산업분야의 기초 전문인력을 양성할 수 있을 것이다.

이러한 목표를 달성하기 위하여 기존의 전산학 관련 학과에서 정보보호 전공 교과목을 개설하기도 하고, 수학과 전공에서 일부 정보보호 전공을 개설하기도 한다. 물론 정보통신전공, 전기전자공학부의 전자공학전공 등에서도 정보보호에 관련된 기초지식을 습득할 수 있다. 결국 학부 과정에서는 정보보호 전공 이외의 타 전공을 이수하면서 정보보호에 관련된 기초 지식을 습득하는 과정이 구축되고 있다⁽⁸⁾.

학부과정에서의 정보보호 전공 교과 과정을 이수한다면 대학원 과정에서는 좀더 구체적으로 정보보호이론, 정보보호응용 그리고 정보보호정책 등을 학습하게 된다.



<그림 1> 정보보호 관련 전공과의 연계도

정보보호이론 분야는 대수학, 확률론, 계산이론, 정보이론 등 암호기술에 사용되는 원천 이론과 비밀키 암호, 공개키 암호 등 암호 기술의 프리미티브, 키분배, 인증, 영지식 증명 등의 프로토콜을 다루는 정보보호 프로토콜 이론 그리고 양자암호, DNA 컴퓨터 등을 다루는 암호 신기술 등으로 분류된다. 정보보호 응용 분야에는 컴퓨터보안 기술, 네트워크보안 기술, 통신보안 기술, 시스템보안 기술, 보안하드웨어 기술 등이 있고 정보보호정책 분야에는 사이버 법률, 정보경제학, 컨설팅, 전자정부론 등이 있다.

2. 연계 전공/부전공을 통한 인력양성

정보보호 분야의 교육은 다양한 학부과정을 이수한 비전공자와도 연계될 수 있다. 정보보호와 관련된 기초 전공을 바탕으로 정보보호 기술에 대한 이론 습득 및 실험 실습이 이루어지는 경우 전문 인력으로 발전할 수 있다.

구체적으로 정보보호 이외의 전공자를 위한 기초 이론 교육과 정보보호 기술 분야의 심도 있는 이론 교육 및 다양한 정보보호 응용 시스템을 구현할 수 있는 능력을 배양하는 교육이 필요하다.

연계과정 및 부전공 관련 교육과정에서는 크게 선수과목, 기초공통과목, 전공과목을 지정하여 비전공자에게도 정보보호 인력으로서의 기본적인 교과목을 이수할 수 있도록 권장할 필요가 있다.

연계전공 및 부전공 과정을 이수하는 경우 선수과목으로는 우선적으로 암호수학 과목을 이수토록 하여야 한다. 암호수학 과목은 정보보호 기술 분야에서 사용되는 수학의 기본 이론을 가르치게 된다. 그리고 프로그래밍에 익숙하지 않은 전공자들을 위해 자료구조 및 실습을 개설하여 향후 전공과목을 수강하며 실험/실습에 대비할 수 있도록 교육할 필요가 있다. 또한 정보보호에 대한 일반 지식이 없는 경우 정보보호개론을 이수토록 하여 균형적인 발전을 도모한다.

연계전공 또는 부전공을 하는 학생에 대해서 기초 공통과목을 이수토록 하여 좀더 심도 있는 교육과정을 제공할 수 있을 것이다. 즉, 정보보호에 대한 기초 이론을 다루는 정보보호이론과 암호 알고리즘 일반에 대해 다루는 암호알고리즘 그리고 정보보호 프로토콜 일반에 대해 다루는 정보보호 프로토콜 등의 교과목을 이수하게 할 필요가 있다.

현재 여러 대학에서 학제간 연계과정을 확대하고 있다. 정보보호 전공은 타 교과목과 많은 연계성을 갖고 있기 때문에 타 전공 분야와 여러 측면에서 연관성을 갖고 있다. 따라서 학제간 연계과정을 통해 인력 양성이 가능하다. 기초적인 수학, 전자·통신, 컴퓨터 관련분야의 지식을 습득하고 관련 정보보호 분야의 전문지식을 습득한다면 정보보호 분야 기초 전문인력으로 양성될 수 있을 것으로 판단하고 있다.

연계전공 및 부전공에 따라서 아래와 같은 교과목들을 이수해야 할 것이다. 크게 전자공학, 컴퓨터 및 수학 관련 교과목을 이수해야 하는데, 만일 컴퓨터 관련 전공자인 경우에는 전자공학과 수학에 관련된 교과목을 이수토록 권장한다면 여러 가지 전공이 복합된 정보보호 전문 인력으로 발전할 수 있을 것으로 판단된다.

2.1 전자공학과 관련 전공자의 교과목 이수

- 컴퓨터 관련 교과목 : 운영체제, 데이터베이스, 컴퓨터 알고리즘, 전자상거래 보안, 네트워크 보안, 컴퓨터시스템 보안, 컴퓨터 네트워크, 데이터 통신, 인터넷 프로그래밍, 컴퓨터 바이러스
- 수학 관련 교과목 : 이산수학, 확률/통계, 대수학, 정수론, 선형대수학, 암호학
- 정보보호 관련 공통 교과목 : 정보보호론, 정보보호 시스템, 정보보호 프로토콜, 침입 탐지 이론, 정보보호 시스템 설계, 멀티미디어 콘텐츠 보호 기술

2.2 컴퓨터 관련 전공자의 교과목 이수

- 전자공학 관련 교과목 : 디지털통신, 영상통신, 컴퓨터 구조론, 실시간 시스템, 디지털 신호처리, 음성 신호처리, 영상 신호처리, 시스템 기술 언어, 암호회로 설계
- 수학 관련 교과목 : 이산수학, 확률/통계, 대수학, 정수론, 선형대수학, 암호학
- 정보보호 관련 공통 교과목 : 전자공학 전공자와 동일

2.3 수학과 관련 전공자의 교과목 이수

- 전자공학 관련 교과목 : 디지털통신, 영상통신, 컴퓨터 구조론, 실시간 시스템, 디지털 신호처리, 음성 신호처리, 영상 신호처리, 시스템 기술 언어, 암호회로 설계
- 컴퓨터 관련 교과목 : 운영체제, 데이터베이스, 컴퓨터 알고리즘, 전자상거래 보안, 네트워크 보안, 컴퓨터시스템 보안, 컴퓨터 네트워크, 데이터 통신, 인터넷 프로그래밍, 컴퓨터 바이러스
- 정보보호 관련 공통 교과목 : 전자공학 전공자와 동일

위와 같이 전공별로 이수해야할 교과목을 분류하였으나, 본 사항은 권고사항으로서 각 대학의 환경 및 각 개인의 특성에 따라 조금씩 다른 결과를 보일 수 있다. 그러나 전반적으로 연계전공 및 부전공의 종류에 따라서 자신의 주전공을 살리면서 정보보호 전문가로 발전하기 위해서는 관련되는 기본 교과목을 이수해야 할 것이다.

3. 산업계에서 필요로 하는 정보보호 인력양성

산업계에서 필요로 하는 정보보호 인력을 양성하기 위해서는 이론 중심의 교육과 함께 실무 능력을 갖춘 인재를 양성할 수 있도록 적절한 산학협력 과정을 개발해야 한다. 따라서 산업계에서 필요로 하는 인력을 양성하기 위한 방안을 제시해 본다.

3.1 산업계에서 필요로 하는 정보보호 교육

가) 이론과 실습이 겸비된 교육

실전경험이 풍부한 연구요원을 교수요원으로 확충하여 그 경험을 전수토록 한다. 이러한 교육과정 중, 학생들이 정보보호 시스템을 직접 제작해보고, 사용할 수 있는 기회를 부여함으로써, 개인의 실전 기술력을 향상시킨다. 또한 학생들은 현재 상용화되고 있는 정보보호 시스템 기술을 연구하고, 실험할 기회를 갖게 되며, 실습 서버를 구축하여 학생들이 언제나 수업 내용을 점검해 볼 수 있도록 하여, 산업계에서 필요로 하는 실전 능력을 향상시킨다.

나) 정보보호 연구개발과 연계된 교육

이론에 대한 실제 모의 테스트가 가능하도록 센터의 연구개발 항목과 연결하고, 학생들의 자발적인 참여를 유도하여 정보보호 연구과제에 참여하여 수행할 수 있도록 한다. 또한 연구내용을 학생들이 직접 실습

할 수 있도록 하여 최신의 시스템 보안 기술을 습득하게 하고, 향후의 연구 개발 방향을 확립하도록 한다.

다) 실무 중심의 교과과정 개발

운영체제에 대한 개념뿐만 아니라 가능한 위협 요소를 인지시키고, 운영체제를 보호할 수 있는 메커니즘을 학습하도록 한다. 정보보호에 활용할 수 있는 소프트웨어에 대한 지식을 전수하고 프로그래밍할 수 있는 정보보호용 소프트웨어를 직접 제작해 볼 수 기회를 갖게 한다. 위와 같은 강의 과목을 수강함으로써 산업체가 요구하는 보안 전문 인력으로 성장할 수 있도록 한다.

3.2 산업계에서 필요로 하는 인력양성 활동 부분

가) 산학연 공동 연구를 통한 정보보호 전문가 양성

정보보호 관련 교과목을 연구센터의 과제와 접목 시킴으로써 이론교육이 실습과 병행될 수 있도록 한다. 또한 학생들을 연구원으로 참여시켜 과제를 수행하도록 하여 교육과정을 이수하는 과정에서 충분한 실습이 가능하도록 한다. 학생들은 연구과제를 통한 참여뿐 아니라, 협약된 산업체와 교류를 통하여 직접 투입되어 실전 경험을 쌓도록 한다.

나) 사이버 교육을 통한 전문인력 양성

현 교육 체제에서 사이버 교육이 가질 수 있는 장점은 매우 많다. 먼저 산업체에 소속한 대학원생들이 업무환경과 각자가 편리한 시간에 따라 언제, 어디에서도 필요한 강의를 받을 수 있어, 시간과 공간의 제약을 없앨 수 있다는 개인적인 이점 이외에도, 교육과정에 필요한 교과목을 모두 새로이 개설하지 않고 기존의 동일 교육 과정을 협동과정 학생들이 이용할 수 있도록 함으로써 비용과 인력 및 시간의 소모를 줄일 수 있다. 또한 사이버 교육은 평생 교육체제 및 산업체 재교육 시스템에도 이바지할 수 있다. 협동과정의 강의는 교류를 통하여 산업체 인력의 재교육을 위한 콘텐츠로 사용되어질 수 있어, 협동과정의 정보보호 전문 인력이 산업체 인력의 교육을 담당할 수 있도록 하고 있다.

3.3 교내외 협력활동

연구센터에 참여한 산업체 인력에 대하여 정보보호 협동과정과의 연구 및 교류의 기회를 부여하고, 새로운 정보보호 시스템 기술에 대한 공동 학습, 연구 성과를 교류하도록 한다. 또한 산업체 학생의 강

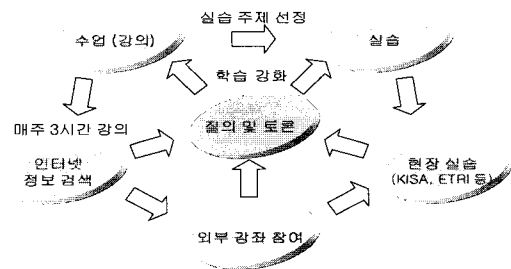
의 학습 및 대학(원)생의 산업체 및 연구소의 강의 학습 기회를 부여하고 산업체 기술을 견학할 수 있는 기회를 부여하고 있다.

또한 학생들은 학내외에 발생하는 침입 및 공격을 지속적으로 감시하고, 지역 산업체와 교류하여 교육과정 중 배운 학습내용을 실전 테스트해볼 수 있는 기회를 갖고, 개인적인 실전능력을 높이도록 하고 있다. 이러한 활동을 통해 지역 산업체에 기업정보 유출의 위험성과 심각성에 따른 정보보호의 필요성에 대한 인식을 높이도록 하고 있다.

라) 실무 중심 정보보호 인력양성

산업계에서 필요로 하는 인력은 실무 능력을 갖춘 인력일 것이다. 따라서 아래와 같은 단계로 인력을 양성하는 것이 바람직하다. 정보보호 인력을 양성하는 과정을 제시하면 아래와 같다^[7].

- 강의시간에 주제별 강의를 수행하고 실습을 유도한다.(실습에 따른 성적 평가)
- 미리 공고된 주제별 질의 및 토론을 수행한다.(토론 참여도 및 주제별 학습 정도를 성적에 반영)
- 산업체에 현장실습을 수행하여 실전능력을 배양한다.(정보보호 산업체와의 산학협동을 수행하고 실습을 수행)
- 정보보호 프로젝트를 실시하여 계획단계부터 구현까지를 수행한다.(정보보호 프로젝트를 위한 실습환경을 구축하여 학생들의 흥미 유발하고 실제 보안 전문가로서의 경험을 축적)



<그림 2> 실무 능력을 배양하기 위한 정보보호 교육 프로그램 (예시)

V. 정보보호 인력양성에 관한 향후 전망

1. 정보보호 인력의 공급 기반 확충

정보보호 기술의 발전을 지속적으로 도모하고 선

진 기술력을 확보하기 위해서는 정보보호 인력에 대한 체계적인 인력 양성 방안을 제시하여야 한다. 구체적으로 전문대학, 대학(원)에 대한 정보보호 전공의 신설 및 증설을 지원하고 정보보호 분야의 학제간 전공 설치 등을 지원하여 정보보호 인력양성의 기반을 강화하는 것이 필요하다.

구체적으로 정보보호전공 설치를 유도하기 위해 정보보호전공을 신설 및 증설하는 대학 중 일부 대학을 우수대학으로 선정하여 실험실습 기자재 등을 지원하는 방안이 있다. 또한 정보보호 기술과 경영학, 법학, 생명공학 등이 결합된 학제간 연계전공 과정을 설치를 지원하여 더욱 복합적으로 발전하는 기술 변화에 적극적으로 대처할 수 있을 것이다.

또한 대학 등에서 정보보호 인력을 양성할 수 있도록 표준 정보보호 교재를 개발 보급하여 인력 양성을 질적으로 뒷받침할 수 있을 것이다. 암호기술, 시스템 보안기술 및 주요 정보보호 기술관련 교재를 개발하고 보급하여 인력 양성을 확대하고, 학회를 중심으로 교과과정을 분석하여 정보보호 인력양성 과정의 내실화를 기할 것이다.

또한 교육과정의 원격화/사이버화 시대에 부응하기 위해 정보보호 교육자료 역시 사이버 환경으로 제공하며 정보의 주요 시책 및 정보보호와 관련된 제반 사항을 시간과 공간에 구애받지 않고 교육할 수 있다. 멀티미디어 정보 시스템의 특성을 활용하여 교육자료를 제공하며 급변하는 정보보호 기술의 발전에 능동적으로 대처할 수 있을 것으로 판단된다.

2. 산업체에서 요구하는 인력양성

정보보호 산업은 급변하고 있으며 IT 전 분야의 기술이 복합적으로 결합된 신기술 분야라고 할 수 있다. 따라서 산업체에서 요구하는 정보보호 인력 역시 고급 지식과 기술을 갖춘 인력을 필요로 한다. 따라서 학부 과정에서의 정보보호 인력을 중심으로 대학원 과정과 연계하며, 특히 정보보호 전문 연구 센터를 통해 산업체와 연계함으로써 기술 발전을 도모하고 결국에는 필요로 하는 인력을 양성할 수 있을 것이다.

현재까지 설립된 4개 ITRC 연구 센터를 중심으로 암호기술, 인증기술, 시스템 보호기술, 네트워크 보호기술에 대해 연구하고 그 결과를 산업계와 공유함으로써 전체적인 기술 발전을 도모할 뿐만 아니라, 고급 정보보호 인력을 지속적으로 배출할 수 있는 토대를 제공할 수 있다. 따라서 앞으로는 더욱

더 지원을 확대하고 센터 설립을 지원하여 결국에는 산업계에서 필요로 하는 정보보호 인력으로 발전할 수 있도록 적극 지원해야 할 것이다.

또한 산업계와 대학간의 현장교육을 강화하여 산학간 교류를 증대하고 정보보호 전문 기업을 선정하여 정보보호 기술 분야의 중요성을 홍보할 필요도 있다. 이와 더불어 IT 전문가들을 적극 활용하는 차원에서 정보보호 산업인력으로 전환될 수 있도록 민간 정보보호 교육기관을 적극 지원해야 한다. 이를 통해 전체적인 정보보호 인력을 확보할 수 있을 뿐만 아니라, 산업현장에서 필요로 하는 인력을 확보할 수 있으며 전문인력 풀을 구성할 수 있을 것이다.

3. 국제 인력교류 확대를 통한 전문인력 양성

국내 대학과 국외 대학간의 공동 연구 및 교류를 확대하고 대학원 과정을 통한 학위 이수 등을 지원하여 정보보호 분야의 국제화를 앞당기고 교류를 증진한다. 정보보호 분야의 우수 대학을 선정하여 외국 대학 및 연구소와 국제 공동연구를 지원하고, 상대적으로 취약한 분야에 대해 해외전문가를 적극 활용하여 전문인력 양성을 적극 지원할 것이다.

국제적으로 우수한 논문을 발표할 수 있도록 지원하고 산업인력이 외국의 전문교육과정에 참여할 경우 경비를 일부 지원하는 방안 등 다양한 지원 방안을 수립하여 정보보호 인력을 양성한다. 또한 국제 암호 및 정보보호 관련 학술 행사를 적극적으로 유치하여 정보 교류와 연구 및 학술 교류를 활성화하도록 지원해야 할 것으로 판단된다.

4. 정보보호 자격제도의 활성화

정보보호 분야의 자격증 제도를 활성화하여 정보보호 인력을 양성할 것이다. 국가가 공인하는 자격증 제도를 정착하여 신뢰성을 향상시키고 산업체에서 필요로 하는 인력을 확보할 수 있도록 적극 지원할 수 있다.

정보통신부 및 한국정보보호진흥원 등과 같은 정보보호 관련 정부기관과 민간 기관이 유기적으로 연계되어 정보보호에 대한 중요성을 널리 인식시키고 정보보호 인력 양성의 필요성을 인식시켜 급변하는 기술 변화에 적극적으로 대처할 수 있는 고급 정보보호 인력을 양성할 필요가 있다. 이를 통해 국가 경쟁력을 확보하고 사이버 기반의 정보통신 환경에

능동적으로 대처할 수 있는 방안이라고 하겠다.

VI. 결 론

정보보호가 정보화를 지속적으로 추진하기 위한 핵심적인 분야라는 인식아래 정보보호 기술강국으로 도약하기 위해 정부에서는 정보보호 관련 기술개발, 산업육성 그리고 인력양성 등 전반적인 분야에 대한 정보보호 기술개발 중장기 계획을 수립하고 있다.

정보보호 인력양성에는 정보보호관련 업체에서 근무하는 산업인력뿐만 아니라 정보보호 전문가, 대학내 인식확산을 위한 각종 활동 지원 등 교육과 홍보를 포함하는 다양한 분야에 걸쳐있는 복합적인 문제에 해당한다.

정보보호인력이 체계적으로 양성되기 위해서는 정규교육과정에 정보보호과정이 반영되어야 하며, 공식적이고 검증된 교육과정을 통해 정보보호 전공 교육과정을 개설해야 한다. 정부에서도 대학내에 정보보호관련 교육과정을 반영하는데 노력하였으며 정보보호분야가 대학교육과정에 반영될 수 있도록 적극 지원하고 있다. 많은 대학들이 정보보호관련 분야로 지원을 받고 있으며 점차적으로 대학에서 정보보호 신규인력이 양성될 것으로 전망된다.

이와 더불어 산업인력양성을 활성화하기 위해서는 민간교육기관의 역할이 가장 크게 필요하다. 정보보호인력의 수요가 급증하면서 정보보호인력양성 전문교육기관도 설립되어 자체교육과정을 운영하고 있다.

정보보호분야의 특성상 복합적인 학문 분야가 결합된 기술 분야이기 때문에 인력양성에 장기간이 소요되며 인력 양성 비용도 타 전공 분야에 비해 상대적으로 무시할 수 없지만, 고도화되는 IT 기술을 선도하기 위해서는 체계적이고도 적극적인 투자가 뒷받침이 된다면 정보보호교육의 활성화를 가져올 수 있을 것으로 본다.

참 고 문 헌

[1] 김 철, "대학의 정보보호 교육 과정 개발 연구", 한국 정보보호학회회지, 제11권, 제3호, 2001. 6

[2] 인터넷 보안 전문가 자격시험 운영 현황, 정보보호교육워크샵, pp. 110-116, 2002. 6. 정보보호학회

[3] 정보보호전문가(SIS) 자격점정제도, 정보보호교육워크샵, pp.117-127, 2002. 6. 정보보호학회

[4] 정보보호 교육방법에 관한 연구, pp. 172-184, 정보보호교육워크샵, 2002. 6. 정보보호학회

[5] 산업체가 바라고 있는 정보보호 인력, pp. 161-171, 정보보호교육워크샵, 2002. 6. 정보보호학회

[6] 민간 정보보호 교육기관의 현황, pp. 66-72, 정보보호교육워크샵, 2002. 6. 정보보호학회

[7] 대학원 정보보호교육 산학연 협동 운영모델, pp. 83-92, 정보보호교육워크샵, 2002. 6. 정보보호학회

[8] 정보보호학과 교과과정의 편성과 운영, pp. 37-46 정보보호교육워크샵, 2002. 6. 정보보호학회

[8] 경북대학교 일반대학원 정보보호학과 (<http://isec.knu.ac.kr/>)

[9] 고려대학교 정보보호대학원 (<http://cist.korea.ac.kr/course.htm>)

[10] 단국대학교 멀티미디어 대학원 정보보호전공 (<http://user.dankook.ac.kr/~multi/>)

[11] 성균관대학교 정보통신 대학원 정보보호학과 (<http://www.skku.ac.kr/~gsic/2002/index.html>)

[12] 순천향대학교 산업정보 대학원 정보보호학과 (<http://elec.sch.ac.kr/dis/room/process.html>)

[13] 전남대학교 정보보호협동과정 (http://altair.chonnam.ac.kr/~webgs/lesson/cooperation_10.htm)

[14] 동국대학교 국제정보 대학원 정보보호학과 (http://iai.dongguk.ac.kr/~iai/ipc_course3)

[15] 한국전자통신대학원대학교 정보보호전공 (http://www.icu.ac.kr/icu/icu_under/main03/html/sub02_02.htm)

<著者紹介>**이 형 우 (Hyung-Woo Lee)**

종신회원

본호의 “국내 4년제 주요대학 정보
보호 관련학과 학부 교육과정 비교
분석 연구” 저자소개 참조

**이 민 섭 (Min-Surp Rhee)**

종신회원

본호의 “국내 4년제 주요대학 정보
보호 관련학과 학부 교육과정 비교
분석 연구” 저자소개 참조