

# 정보보호 전문인력 양성을 위한 전문대학 정보보안과의 운영방안에 관한 연구

A Study on the Operational Plan of Information Security Department in Colleges for Educating Information Security Personnel

김경호  
 김천과학대학 컴퓨터정보계열

Kyung-Ho Kim (khkim@kcs.ac.kr)  
 Div. of Computer Information, Kimcheon Science College

김명숙  
 충남대학교 경영학과

Myeong-Suk Kim (kmsjws@hanmail.net)  
 Dept. of Business Administration, Chungnam National University

중심어 : 정보보안, 교육목표, 교과과정

Keyword : Information Security, Educational Goal, Curriculum

## 요 약

본 논문의 목적은 전문대학 정보보안과의 운영방안을 제안한다. 이러한 목적을 달성하기 위해 첫째, 정보보호 전문인력 양성의 필요성을 살펴보고, 둘째, 국내 전문대학 중 정보보안과를 운영하고 있는 7개 전문대학의 현황 및 교과과정을 분석하고, 셋째, 전문대학 정보보안과가 직면하고 있는 문제점을 극복하기 위한 운영방안에 대해 제안한다.

## Abstract

The purpose of this study is to suggest an operational plan for the information security department of colleges. First, the necessity for educating information security personnel was examined. Second, the institutes for educating information security personnel were investigated and the curriculum for information security of the college in Korea were examined. Finally, the challenges were examined and the solutions were suggested.

## 1. 서론

정보보호의 문제는 개인의 문제를 뛰어넘어 기업조직, 국가의 경쟁력 문제로 대두되고 있다. 현재 많은 논란이 되고 있는 교육행정정보시스템(NEIS)의 경우도 학생 각 개인의 프라이버시가 보장될 수 없다는 것이고, 2003년 1월 25일 14시 10분경부터 시작된 웬바이러스에 의한 인터넷 마비사건은 매우 짧은 시간에 트래픽이 폭발적으로 증가하여 인터넷서비스사업자(ISP)의 일부 도메인네임서버(DNS)가 일시적으로 마비되었고, 인터넷서비스 전반에 걸쳐 접속 지연 및 불가 상태가 발생한 것으로 분석되었다[12]. 이번 사고의 범위는 한국, 미국, 일본을 포함하여 전세계적으로 대규모로 발생한 것으로

추정된다. 그러나 만약 국가적 차원에서 정보보호에 대한 대책을 수립하지 못한다면 “1.25 인터넷 마비사고”는 앞으로 다가올 인터넷 대란의 서곡에 불과할 것이다. 이와 같은 무차별적인 해킹과 사이버 테러에 대응하기 위해서는 무엇보다 정보보호 전문인력 양성이 매우 절실하다고 볼 수 있다. 국내 대학과 전문대학의 경우 최근 2~3년 동안 꾸준히 학과를 신설하고 있으나 정보보안 실습환경의 부족, 정보보안 전담교수의 부족, 그리고 표준화된 교과과정이 수립되지 못하여 정보보호 전문인력 양성이라는 교육목표를 달성하지 못하여 정보보호 전문인력 양성이라는 교육목표를 달성하기에는 어려움이 있다. 이에 본 연구에서는 정보보호 인력양성기관중 하나인 국내 전문대학의 효율적인 운영방안을 논의하고자 한다. 이를

접수번호 : #040406-002

\*교신저자 : 김경호, e-mail : khkim@kcs.ac.kr

접수일자 : 2004년 4월 6일, 심사완료일 : 2004년 6월 7일

위해 먼저 정보보호 전문인력 양성의 필요성과 전문대학 정보 보안과 운영실태에 대해 알아본 후, 전문대학 정보보안과가 직면하고 있는 여러 가지 문제점을 극복할 수 있는 운영방안을 제시할 것이다.

## II. 정보보호 전문인력 양성의 필요성

### 1. 인터넷의 폭발적인 발전에 따른 위험성 증대

정보통신기술의 급속한 발전에 따라 표 1과 같이 인터넷 이용자 수가 급증하면서 산업 및 사회적 환경이 인터넷을 기반으로 하는 구조로 빠르게 변화하고 성장해 가는 만큼 컴퓨터 정보시스템 침해에 따른 사회적 혼란이 초래될 가능성도 그만큼 커지고 있다고 할 수 있다. 2003년 1월 25일 국내의 인터넷 마비 사태가 일례라 할 수 있을 것이다. 이러한 상황에서 혼란을 방지하기 위해서는 정보시스템을 안정적으로 보호하기 위한 정보보호 기술이 절실하게 요구되는 시점이라 할 수 있다.

표 1. 인터넷 이용자수 증가추이

(단위 : 천명)

년도	1999년	2000년	2001년	2002년	2003년6월
이용자수	10,860	19,040	24,380	26,270	28,610

자료원 : 한국인터넷정보센터, 2004년

### 2. 정보보호 침해 및 피해의 급증

정보통신기술의 발전과 함께 해킹기술과 도구 및 바이러스 기술 역시 발전하면서 컴퓨터 정보시스템에 대한 침해가 급증하고 있다. 한국정보보호진흥원 침해사고대응팀(CERTCC)에 따르면 해킹 피해건수가 매년 최근 5년 동안 1.5~3배씩 증가하고 있다. 표 2에서 보는 바와 같이 2003년에는 총 26,179건의 해킹 피해가 국내에서 발생했는데 이는 지난 98년의 572건과 비교하면 5년만에 무려 45.7배나 증가한 수치다. 또한 해커의 유형이 자신의 연구를 목적으로 시스템을 탐구하는 학구형 해커에서 시스템에 침입 후 자료를 파괴하는 파괴형 해커로 또는 타인의 비밀이나 신상 정보를 절취하는 스파이형 해커로 변하고 있다. 이에 따라 호기심 차원에서 이루어지던 침해가 이제는 범죄화 수준으로까지 발전하면서 그 피해액 역시 급증하고 있는 실정이다. 표 3에서 보는 바와 같이 2002년 CSI/FBI 컴퓨터범죄 및 보안 서베이<sup>1)</sup> 결과에 의하면 사이

버 공격으로 인한 미국의 경제적 손실 규모는 약 30%이상 계속하여 증가하고 있는 것으로 나타났다. 또 전체 조사대상 중 연도별로 약 35%~44%만이 피해규모를 산정, 실제 피해규모는 2배 이상일 것으로 추정되어 2002년의 경우 10억 달러가 넘을 것으로 추정된다<sup>12)</sup>.

표 2. 연도별 해킹 피해 신고 건수

년도	1999년	2000년	2001년	2002년	2003년
건수	572	1,943	5,333	15,192	26,179

자료원 : 한국정보보호진흥원, 2003년 해킹바이러스 동향

### 3. 정보보호산업 발전에 따른 인력수요 급증

정보통신기술의 발전은 정보보호기술의 발전과 상호보완적 관계에 있다고 할 수 있다. 정보시스템의 침해로 인한 부작용을 최소화하여 정보통신 기반사회를 안정적으로 발전시키기 위해서는 정보시스템을 보호하기 위한 기술의 개발을 필요로 하며, 이는 정보보호기술과 정보보호산업 시장의 발전을 촉진시키게 된다. 결론적으로 정보통신기술 분야는 앞으로도 계속 발전할 것이며, 이는 필연적으로 상호보완적 관계에 있는 정보보호기술 분야의 끊임없는 발전과 성장을 가져오게 될 것이다.

세계 정보보호시장은 1999년 77억 달러 수준에서 2001년 135억 달러로 시장규모 측면에서 2배에 가까운 성장을 하고 있으며, 연평균 30% 정도 성장하여 2004년도에는 280억불에 달할 것으로 예측된다. 국내 정보보호산업은 '99년에 400억 원 정도였던 시장규모가 2002년에 3,964억 원, 2003년에 5,165억 원에 달했고, 올해에는 7,051억 원에 이를 것으로 전망됨에 따라 정보보호산업이 새로운 고부가가치 산업으로 각광받고 있다. 한국정보보호산업협회에서 100개 정보보호업체를 대상으로 조사한 결과에서는 현재 2,672명의 정보보호 관련기술인력이 있지만 올해 안으로 3,363명의 인력이 더 필요한 것으로 추정하고 있다. 향후 5년간 기술관련 종사자의 수요는 2005년에 4,110명, 그리고 2007년에는 그 수요가 4,780명에 이를 전망으로 연평균 12.3%에 이르는 증가세를 보일 것으로 조사되었다. 또한 정보통신부의 중장기 정보보호 기본

1) 미국의 CSI(Computer Security Institute)와 FBI가 주관이 되어 미국의 기업, 정부기관, 금융기관, 의료기관 및 대학의 컴퓨터 보안 실무자를 대상으로, 1996년 이후 매년 실시해온 컴퓨터 범죄 및 정보보안 실태에 관한 설문조사이며, 2002년 까지 7번째 조사결과를 발표하였다.

계획에 따르면 정보보호산업은 향후 5년 동안 약 22,000여명 정도의 공급부족으로 인한 심각한 수급 불일치 현상이 지속될 것이라는 전망이 나오고 있다[10]. 이와 같이 정보보호산업의 빠른 성장으로 인하여 정보보호산업인력에 대한 시장 수요도 현재 급격히 증가하고 있지만 이러한 급격한 수요증가를 충족시키는 수준의 원활한 공급을 하지 못하고 있는 실정이다.

표 3. CSI·FBI : 사이버공격으로 인한 손실액

구분	조사·응답자	피해규모
2000년	249명	266 백만 달러
2001년	186명	378 백만 달러
2002년	503명	456 백만 달러

자료원 : 한국통신연구진흥원, 국내 정보보호 현황과 발전방향, 2003년

특히 정보보호산업체가 대부분 창업 3년 미만의 중소기업체로서 신규인력을 충원해 교육시절 역력이 없어 경력이 있는 전문가를 요구하는 것도 정보보호 산업인력부족의 큰 요인으로 지적되고 있다. 2000년 말에 정보보호산업체를 대상으로 한 설문조사에서 기술개발과 제품생산의 가장 큰 애로요인으로 전문인력의 부족을 꼽았을 정도로 정보보호 산업인력의 부족은 업체들의 큰 어려움 중의 하나라고 볼 수 있다[8].

전체 정보산업에서 적절한 정보보호 인력규모를 추정하기는 쉽지 않지만 미국의 몇몇 전문가들은 대체로 정보보호인력은 전체 정보화인력의 10% 정도가 적당하다고 보고 있다. 국내의 경우 2005년에 정보산업 종사인력이 150~160만 명에 이를 것으로 추정되는 가운데 2005년에 15~16만 명의 정보보호 전문인력을 확보하기는 현실적으로 불가능하다[6]. 또한 정보보호산업 경쟁력 분석 결과에 의하면 경쟁력 확보에 가장 큰 장애요인으로 시장 확보 (3.68점/5점 만점), 영업 인력의 양적 부족(3.33점/5점 만점), 기술개발 인력의 양적 부족(3.29점/5점 만점) 등의 순서로 나타나고 있어 정보보호업계의 인력 부족현상은 향후 매출이 증가하면서 더욱 심한 경쟁력 저해요인으로 작용할 전망이다[5]. 따라서 정보보호산업이 직면하고 있는 가장 큰 문제는 이러한 인력수급 불일치 현상을 조절하고 극복하느냐 하는 것이다.

### III. 전문대학 정보보안과 운영실태

#### 1. 국내 전문대학의 정보보안과 개설 현황

국내 전문대학의 정보보안관련과 개설 현황에 관한 정보는 한국전문대학교육협의회(<http://www.kcce.or.kr>)와 각 대학의 홈페이지를 검색하여 파악하였다. 파악된 전문대학의 경우 각 해당학과 홈페이지를 방문하여 교육목표나 과정을 분석하여 정보보안관련학과라고 보기에에는 무리가 있는 일부 학과는 본 연구에 포함하지 않고 최종적으로 표 4의 7개 전문대학만을 조사대상으로 선정하였다[2].

표 4. 정보보안관련과 설치 전문대학

대 학 명	학과(계열)	세부 전공
김천과학대학	컴퓨터정보계열(3년)	정보보안전공
동명대학	정보·디자인학부(3년)	인터넷보안과
광주보건대학	정보계열	컴퓨터보안과
대덕대학	컴퓨터인터넷정보계열	정보보안·해킹전공
동부산대학	웹모바일보안과	웹보안전공
송원대학	컴퓨터보안과	
한국재활복지대학	정보보안과	

#### 2. 국내 전문대학 정보보안과의 인력 현황

각 조사기관마다 조금씩 차이는 있지만 KISA에 의하면 정보보호 인력수요는 2003년부터 2007년까지 14,000여 명이 되는 반면에 정보보호 인력공급은 정규 교과과정을 중심으로 10,000여 명의 신규 인력을 배출할 전망이다, 이 중 대학원 이상의 인력 규모는 3,000여 명 정도가 될 것으로 전망된다. 따라서 정보보호분야는 2003년부터 2007년까지 5년 동안 약 4,000명의 공급부족 현상이 발생할 것으로 예상된다[7]. 이와 같이 매년 1,000여 명 정도의 공급부족 현상을 약 19개 대학(정보보호관련학과가 개설된 대학)과 7개 전문대학에서 공급하는 인력으로는 정보보호산업체가 요구하는 수요를 충분히 만족시켜 주지 못하고 있다. 일부 대학은 계열단위로 인원을 모집하여 정확히 파악하기 어렵지만 7개 전문대학에서 매년 배출하는 정보보호 인력은 약 200명 정도 되는 것으로 추정되어진다. 따라서 이러한 인력부족을 보완하기 위하여 지금까지는 정보보호업체나 협회를 중심으로 한 컨소시엄 형태의 교육기관에서 운영하는 단기간의 교육을 벗어나 장기적으로 정보보호산업 분야의 국가경쟁력을 확보하기 위해서는 대학차원에서 체계적인 교육과정을 이용하여 인력을 양성할 필요가 있다.

### 3. 국내 전문대학 정보보안과의 교과과정 현황

학과의 정체성을 확보한 대부분의 학과에서는 무엇을 교육해야 할 것이냐에 대한 공통적인 견해가 있다. 그러나 정보보안과의 경우 최근에 신설되었고 그 응용기술의 변화가 빠르다는 점 때문에 교과과정에 대한 공감대를 형성한다는 것이 쉽지 않다. 따라서 각 전문대학이 학과가 설정한 교육목표를 달성하기 위해 전공과목을 학문영역별로 어떻게 배분해야 할 것인가에 대한 통일된 분류기준이 없는 실정이다[2]. 정보통신부의 “정보보호 기술개발 5개년 계획”에서는 정보보호기술의 분류 기준을 기술적 특성과 응용분야를 고려하여 공통기반 기술, 시스템·네트워크 보호기술, 응용서비스 보호기술의 3계층 구조로 구분하고 있다. 공통기반 기술은 정보보호제품 전반에 적용되는 암호 알고리즘, 암호 프로토콜, 키관리 및 인증기술 등을 포함하고, 시스템·네트워크 보호기술은 정보통신시스템을 구성하는 서버, 네트워크 및 PC 등 유무선 단말 시스템에 대한 보호기술을 포함하며, 응용서비스 보호기술은 정보통신기술을 활용한 전자상거래 등 응용 서비스(콘텐츠보호, 전자지불 등)의 안전 신뢰성 향상을 위한 보호기술을 포함한다[10]. 또한 국내 보안분야의 대표적인 자격증인 정보보호전문가(SIS : Specialist of Information Security)의 경우 ‘시스템분야’, ‘네트워크분야’, ‘어플리케이션분야’, ‘정보보호 일반분야’로 분류하고 있다. 이에 본 연구에서는 두 기관에서 공통적으로 내포하고 있는 기준을 토대로 정보보안 전공과목은 정보보안기초분야, 정보보안전공분야, 그리고 정보보안공통분야로 분류하고 정보보안기초분야와 정보보안전공분야의 경우에는 다시 시스템보안분야, 네트워크보안분야, 어플리케이션보안분야로 세분화하였다[2]. 이를 바탕으로 각 전문대학 현행 교과과정에 대한 분석은 표 5 ~ 표 11과 같고, 통합적 분석에 따르면 7개 전문대학에서 운영하는 전공과목 전체의 수는 203개 과목이고, 각 대학은 평균적으로 25과목의 전공과목을 운영하고 있다. 또한 교과목 분류기준에 의하면 정보보안기초분야의 교과목 수는 114개(56%), 정보보안전공분야의 교과목 수는 56개(28%), 그리고 전산학개론, 정보처리실습, 졸업 프로젝트 등 기타분야의 교과목 수는 33개(16%)이다. 각 분야별 평균 교과목 수는 정보보안기초분야의 교과목 수는 14과목, 정보보안전공분야의 교과목 수는 4과목, 정보보안공통분야의 교과목 수는 3과목, 나머지 기타분야의 교과목은 4과목을 개설하는 것으로 나타났다.

또한 교과목 개설의 중요도 측면에서는 정보보안기초분야의 경우 데이터베이스, 정보통신개론, 네트워크서버관리, 비주얼 프로그래밍, 운영체제, 컴퓨터구조, 프로그래밍언어, 자료구조,

C언어, 인터넷프로그래밍, 멀티미디어개론, TCP/IP실습, 무선인터넷, 네트워크프로그래밍, 컴퓨터네트워크 등의 순서로 교과목 개설의 중요도가 나타났으며, 정보보안전공분야에서는 네트워크보안, 침입탐지시스템, Windows보안, 해킹바이러스실습, 해킹분석기법 등의 순서로 교과목 개설의 중요도가 나타났고, 정보보안공통분야에서는 정보보호개론, 암호학개론, 보안실무프로젝트 등의 순서로 교과목 개설의 중요도가 나타났다.

### 4. 정보보안실습실 및 교원확보 현황

정보보안과에서 개설한 ‘침입탐지시스템’, ‘역추적기술’, ‘해킹과 크래킹’, ‘VPN’, ‘보안 컨설팅실습’ 등과 같은 교과목을 교육하기 위해서는 단순한 형태의 컴퓨터실습실로는 어려움이 많은데 전문대학의 현실로는 수억의 비용을 투입해서 정보보안실습실을 만들기는 어려운 실정이다. 실제로 교육인적자원부로부터 정보보안특성화계열로 선정된 K대학과 D대학의 경우에만 정보보안관제센터와 모의해킹실습실과 같은 정보보안실습실을 구축하였을 뿐 나머지 대학의 경우에는 적극적인 투자를 하지 못한 상황에 있다. 이러한 시설투자에 대한 부담이 정보보안과 신설을 가로막는 큰 장애요인이 되고 있다. 또한 정보보안분야의 이론과 기술이 최근에 발생한 이유로 기존 컴퓨터관련학과의 전임교원이 정보보안과 관련된 이론과 기술을 습득하기에는 많은 어려움이 있다. 실제로 기존의 컴퓨터관련 학과에서 정보보안과로 변경하거나 신설하는 경우 기존 전임교수들이 정보보안과의 교수가 된다. 이런 경우 학과목의 개설이 교육목표 달성이라는 거시적 접근에 의하여 개설되어 지는 것이 아니라 전임교수들의 학문적 배경 또는 개인적인 사정을 고려하거나, 강의하기가 어려운 과목은 개설을 기피함에 따라 교과과정을 잘못 구성하는 경우도 있다. 이러한 경우에는 왜곡된 교과과정을 학생들에게 강요하는 오류를 범하게 된다. 따라서 대학 경영층이 비용의 논리로 접근한다면 학과의 신설이나 효율적인 운영이 매우 어려울 것으로 판단된다.

### IV. 정보보호 전문인력 양성을 위한 전문대학 정보보안과의 운영방안

정보보호 전문인력을 체계적으로 양성하기 위해서는 대학은 먼저 정보보호분야에 대한 교육목표 설정, 교과과정 확립, 정보보안실습실 구축과 교원확보 등과 같은 작업을 선행하여야 한다.

### 1. 교육목표 설정

많은 전문대학 정보보안과의 경우 학과의 교육목표를 '정보보호 전문인력 양성'에 두고 있지만 정보보호 기술의 생명주기가 매우 짧고, 매우 역동적으로 변화하는 데다가 정보보호 산업이 타산업과의 동태적인 상관관계 속에서 성장하고 있는 산업이기 때문에 정보보호 전문인력에 대한 정의조차 아직까지 명확하게 제시하지 못하고 있는 실정이다[4].

표 5. 김천과학대학 컴퓨터정보계열 정보보안전공 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	UNIX 실습	정보통신론	멀티미디어세계
	컴퓨터구조	정보통신네트워크	C 언어
	운영체제	네트워크프로그래밍	비주얼언어
		근거리통신망설계	자료구조
		스크립트프로그래밍	시스템분석설계
		데이터베이스	
		데이터베이스실습	
정보보안 전공분야	서버보안	네트워크보안	컨텐츠보안
	해킹분석 및 방지	침입차단 및 탐지	바이러스보안기술
	해킹분석 및 방지실습	역추적기술	
		역추적기술실습	
VPN			
정보보안 공통분야	정보보호개론, 통합보안관제, 통합보안관제 실습		

현재 가장 널리 활용되는 정보보호 전문인력에 대한 정의는 다음과 같다. 미국의 국립표준연구소(National Institute of Standards and Technology : NIST)에 의하면 정보보호 전문인력이란 '정보보호에 관한 고도의 지식과 기술수준을 가지고 미래지향적으로 정보보호 업무를 수행할 수 있는 능력을 가진 인력'이라고 정의하고 있다[13]. 또한 김태성 외(2003)는 정보보호 전문인력은 '정보보호에 대한 마인드와 지식을 보유하고 정보보호업무를 수행할 수 있는 능력을 가진 인력'으로 정의하고 있다[4].

표 6. 동부선대학 인터넷 보안과 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	운영체제	인터넷프로그래밍	C 언어
	컴퓨터구조	정보통신개론	시스템분석설계
	서버운영	네트워크프로그래밍	데이터베이스구축
			실무프로그래밍
컴퓨터그래픽			
정보보안 전공분야	취약점분석 II		보안프로그래밍 II
	해킹기법분석	침입탐지	
	바이러스백신 분석		
정보보안 공통분야	정보보안개론, 암호알고리즘		

표 7. 송원대학 컴퓨터보안과 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	Windows기초	웹프로그래밍언어 II	C언어
	Linux기초	Windows네트워크	Shell프로그래밍
	Unix기초	Linux네트워크	
		Unix네트워크	
		라우터네트워크	
		TCP/IP	
정보보안 전공분야	Windows보안 II		
	Linux보안 II		
	Unix보안 II		
정보보안 공통분야	정보보호개론, 암호화 기술		

이에 본 연구에서는 정보보안과의 교육목표를 '실무 중심의 교육을 통해 정보보호 기술에 대한 전문지식을 보유하고 정보보호 관련직무를 수행할 수 있는 인력'을 양성하는 것으로 설정한다[2].

## 2. 교과과정 확립 및 개선

전문대학 교과과정 분석에 따르면 각 대학마다 개설하고 있는 교과목의 경우에 교과목 명칭과 교육내용이 표준화되어 있지 못하고 있음을 알 수 있었다.

표 8. 광주보건대학 정보기술계열 컴퓨터보안과 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	운영체제	컴퓨터네트워크	비주얼베이직실습
	전산기구조	정보통신	어셈블리실습
		이동컴퓨팅	C언어실습
	인터넷프로그래밍실습	자료구조	
	LAN설계	데이터베이스	
	네트워크구성론	시스템분석설계	
	TCP/IP실습	C++프로그래밍실습	
	정보통신법규	파일처리론	
	네트워크관리		
	네트워크프로그래밍		
	클라이언트/서버 기술		
	클라이언트/서버 응용실습		
	정보보안 전공분야	컴퓨터보안	
해킹과 크래킹			
정보보안 공통분야	정보보안, 암호체계, 보안시스템구축실무프로젝트		

물론 각 학과마다 독특한 영역을 가지고 교과과정을 개발하여 운영할 수 있지만 이러한 교과과정들이 각 학과의 특성에 지나치게 치우쳐 정보보안과가 가져야 할 공통적인 특성을 무시해서는 곤란하다.

이는 교과과정을 수립한 해당 교수들이 아직 무엇을 교육해야 하는지에 대한 공감대가 형성되지 못하고 있기 때문에 판단된다. 따라서 각 학과가 수립한 교육목표에 따라 교과과정이 고려되어야 하지만 어느 정도의 공통성을 가지고 그 범위 안에서 변형되어야 할 것이다. 그러한 점에서 정보보안과 교과 과정에 대한 연구는 더욱 필요하다.

교과과정 현황에 따르면 정보보안기초분야와 정보보안전공 및 정보보안공통분야의 전공과목 배분의 비율에서 지나치게 정보보안기초분야에 편중되어 있음을 알 수 있다. 이는 정보

보안기초분야와 정보보안전공 및 정보보안공통분야의 교과목을 균형있게 재배분할 필요성이 있음을 암시하고 있다. 따라서 전문대학의 짧은 수업연한으로는 모든 정보보안분야의 내용을 이수하기가 어려운 실정이므로 학과의 교육목표나 상황에 맞추어 시스템보안 또는 네트워크보안으로 집중교육하여 특화할 필요성이 있다[2].

표 9. 한국재활복지대학 정보보안과 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	운영체제 II	데이터통신	프로그래밍C++
	전산기구조	네트워크이해	프로그래밍실습
		인터넷프로그래밍	자료구조
	무선인터넷	프로그래밍응용 II	
	네트워크프로젝트	데이터베이스프로젝트	
		트	트
		데이터베이스	
	전자상거래시스템		
멀티미디어이해			
정보보안 전공분야	해킹 및 바이러스처리	무선보안	
	시스템 및 네트워크보안관리 II		
정보보안 공통분야	정보보호개론, 보안프로젝트		

김철(2001)의 연구에 의하면 4년제 대학의 경우 학과의 교육목표를 달성하기 위해서는 정보보호학과 정보보호교과목으로 16과목정도는 이수해야 한다고 한다[3]. 전문대학의 경우 수업연한의 차이는 있기 하지만 7과목 정도의 전공과목을 이수하여 '정보보호 전문인력' 양성이라는 교육목표를 달성하기에는 어려움이 있다. 따라서 정보보안기초분야의 교과목을 정보보안전공분야의 교과목으로 균형있게 재배분할 필요성이 있다.

## 3. 정보보안실습실 구축 및 교원확보 강화

산업계는 교육의 유용성과 현장성 강화에 대한 요구가 높으면서도, 실제로 학생들에게 현장실습 기회를 제공하는데는 매우 소극적이다. 또한 대학과 산업체간에 연구개발된 지식이나 기술을 상호 확산·공유할 수 있는 시스템을 제대로 마련되어 있지 못한 것도 현실이다. 이러한 현실에서 대학은 현장실습을 외부의 산업체에서 나가서 받아야 한다고 하는 기존의 고

정관념에서 벗어나 대학 스스로 그러한 환경을 만들어 교육목표를 달성하는 것이 바람직하다.

표 10. 대덕대학 컴퓨터인터넷정보계열 정보보안·해킹전공 교과목

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야		정보통신과인터넷	데이터베이스기초
		자바프로그래밍	프로그래밍실습
		네트워크서버 관리	프로그래밍언어
		컴퓨터네트워크	비주얼프로그래밍 기초
			비주얼프로그래밍 응용
자료구조			
정보보안 전공분야	운영체제보안	인터넷보안	전자상거래보안
		네트워크보안	
정보보안 공통분야	정보보호개론, 암호의 이해, 정보보호법 및 표준		

그 대안의 하나로 대학내에서 현장실습이 가능하도록 하는 학교기업(SBE: school-based enterprise) 형태의 교육시스템이다. 이러한 시스템을 도입한 K대학의 경우 정보보안관제센터를 통해 인근 12개 고교를 중심으로 침입탐지관제서비스를 실제로 행하고 있으면, 이를 통해 대상 고교에 해킹과 바이러스가 침입되고 있는지에 대한 로그분석을 학생들이 실습하고 있다. 이와 같은 시스템을 통해 학생들은 대학 내에서 현장실무를 직접 경험할 수 있게 될 것이고, 기업 또한 실무능력을 갖춘 인력을 공급받을 수 있는 기회가 될 것이다. 이 외에도 D대학의 경우 모의해킹실습실(Free Hacking Zone)을 구축하여 해킹과 관련된 실습을 실시하고 있으며, 4년제 대학의 경우에는 K대학교가 2003년 2월 26일에 통합보안관제센터를 개원하여 해킹, 바이러스 정보 및 예방교육을 실시하고 있다. 향후 많은 대학은 대학경영진의 적극적인 지원과 이해를 바탕으로 이와 같은 교육시스템을 통해 보다 질 높은 정보보호 인력이 양성되어야 할 것이다.

또한 대학의 교육과정이 산업체의 요구사항을 적극적으로 반영하지 못한다면 결국 대학에서 배출하는 인력이 산업체에 큰 부담으로 작용할 수밖에 없다. 특히 정보보호 분야와 관련된 전문지식과 기술의 경우에는 대학 내의 기존 전임교수로 소화하기가 현실적으로 매우 어려운 상황이다.

표 11. 동명대학 정보통신계열 교과목 분류

구분	시스템 보안	네트워크 보안	어플리케이션 보안
정보보안 기초분야	운영체제활용	정보통신개론	프로그래밍언어
	컴퓨터구조	컴퓨터네트워크	프로그래밍응용
	윈도우즈시스템관리	TCP/IP실습	데이터베이스실습
	리눅스시스템 관리	라우터실습 I II	데이터베이스관리
		윈도우즈네트워크 관리	
		리눅스네트워크 관리	
		네트워크장애처리 실습	
		무선응용프로토콜실습	
		해킹바이러스 실습	
	윈도우즈보안 실습	침입탐지시스템 실습	
리눅스보안			
정보보안 공통분야	정보보호개론, 보안컨설팅실습		

따라서 대학에서는 정보보호업체와 산학협력을 통해 실무자로서의 강교원으로 활용하는 것이 매우 필요하며, 이를 통해 대학은 산업체에서 요구하는 실용적 지식과 기술을 상당부분 습득할 수 있을 것이다. K대학의 경우에는 정보보안관제센터와 온라인해킹스페이스(Online-Hacking Space)를 구축할 때 정보보안업체와 산학협력을 맺어 정보보안관제센터 운영에 필요한 지식과 기술을 지속적으로 지원 받고, 정보보안전문가를 강의교수로 활용하여 산학협력의 관계를 유지하고 있다. 이와 같이 여러 가지 방안을 통하여 산학협력의 범위와 폭을 확대하는 것이 대학이 직면한 과제라 할 수 있다.

## V. 결론

본 연구에서는 정보보호 전문인력 양성을 위한 전문대학 정보보안과의 운영방안에 대해 살펴보았다. 이를 위해서 먼저 전문대학 정보보안과에 대한 교육목표 설정, 교과과정 분석,

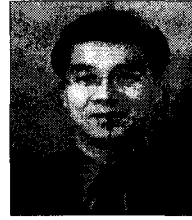
정보보안실습실 구축과 교원 확보 등에 관해 고찰하였다. 먼저 각 학과에서는 교육목표를 명확히 하고 무엇을 가르칠 것인가에 대한 교과과정에 대한 공감대를 형성해야 하며 이를 위해서는 교과과정에 대한 체계적인 분석이 수반되어야 한다. 이와 같은 교육과정을 효율적으로 운영하기 위해서는 정보보안실습실 구축이 필수적이며, 이에 따른 엄청난 비용은 대학 경영진의 적극적인 지원과 이해가 수반되어야 할 것이다. 또한 개설된 교과과목들을 보다 효과적으로 교육하기 위해서는 정보보안 전임교수의 확보 및 산업체 실무자들에 의한 강의가 병행되어야 한다. 이러한 환경이 제대로 구비된다면 대학은 정보보호인력에 대한 양질의 공급을 할 수 있을 것이다.

### 참 고 문 헌

- [1] 길민정, "국내정보보호산업 실태조사", 정보보호뉴스, 4월호, 2002.
- [2] 김경호, "전문대학 정보보안과 교과과정 개발에 관한 연구", 정보보호학회지, 제 13권 제 6호, pp. 3-15, 2003.
- [3] 김철, "대학의 정보보호 교육과정 개발 연구", 정보보호학회지, 제 11권 제 3호, pp. 75-89, 2001.
- [4] 김태성 외 3인, "정보보호인력의 분류체계에 대한 연구", 정보보호학회지, 제 13권 제 3호, pp. 50-60, 2003.
- [5] 박영우 & 길민정, "2001년 국내정보보호산업 실태조사", 한국정보보호진흥원, 2001.
- [6] 송희준, "정보보호산업인력의 적정규모 예측과 수급전략", 정보보호뉴스, 12월호, 2000.
- [7] 이초희 외 2인, "정보보호 인력 양성 정책에 대한 소고", 한국정보기술응용학회, 2002년도 춘계학술대회, 2002.
- [8] 이현, "정보보호산업 전문인력 양성", 정보보호뉴스 10월호, 2000.
- [9] 정보통신부, "정보보호 기술개발 5개년 계획(안)", 2001. 3.
- [10] 정보통신부, 중장기 정보보호 기본계획, 2002. 8.
- [11] 한국정보보호산업협회, "국내정보보호산업 통계 및 시장조사", 2002.
- [12] 황성원, "국내 정보보호 현황과 발전방향", 정보통신연구진흥, Vol. 15, No. 1, 2003, pp. 12-13.
- [13] NIST, Information Technology Security Training Requirement: A Role-and performance-based Model, NIST Special Publishing 800-16, 1998.

김 경 호(Kyung-Ho Kim)

정회원



1986년 2월 : 계명대학교 경영학과  
(경영학사)

1989년 8월 : 계명대학교 경영학과  
(경영학석사)

2001년 8월 : 영남대학교 경영학과  
(경영학박사)

1992년 9월 ~ 현재 : 김천과학대학 컴퓨터정보계열  
조교수

<관심분야> : 정보보호윤리, 인터넷비즈니스, 모바일  
인터넷

김 명 숙(Myeong-Suk Kim)

정회원



1984년 2월 : 효성여자대학교  
경영학과 (경영학사)

1986년 2월 : 효성여자대학교  
경영학과 (경영학석사)

2004년 2월 : 충남대학교 경영학과  
(경영학박사)

현재 : 충남대학교 경영학과 시간강사

<관심분야> : e-비즈니스, 모바일 인터넷, 지식경영