

# 정보보호 전문 인력 양성을 위한 교육과정 모델에 관한 연구 (A study on a curriculum for information protection specialty manpower training)

이문구(Moon-ku Lee)<sup>1)</sup>

## 요 약

인터넷의 보급과, 산업 및 생활 전반에 걸쳐 전산화가 이루어지면서 사생활 보호 및 정보보호에 대한 요구가 증가하고 있지만 정보보호 산업분야의 전문 인력의 부족으로 많은 어려움이 있다. 때문에 본 논문에서는 정보보호 전문 인력 양성을 위한 교육과정을 제안하였다. 제안하는 교육과정은 필수 1,2 와 선택 1,2로 분류하였다. 정보보호 응용분야를 9개의 도메인으로 세분화 하여 시행되어야 할 교육과정을 링 구조로 제시하였다. 정보보호 응용분야의 9개 도메인에 따른 현장 실무 프로젝트와 연계된 교육 과정과 졸업 후 전공심화를 위한 강좌가 도메인별로 이루어져서 정보보호 심화과정을 지속적으로 진행한다.

## ABSTRACT

The spreading of internet, combined with the computerization of industry and the life whole has created an increased demand on the private life protection and information protection, but due to the lack of specialty manpower on the information protection industry field there are many difficulties. Therefore, in this paper a curriculum for an information protection specialty manpower training is proposed. The proposed curriculum indispensability 1,2 and classified with a selection 1,2. The information protection application field into 9 segments of domains, and to carry out the curriculum in a ring structure. The curriculum based on the information security field's 9 domains and related field practical business, and the course offered after graduation to deepen the specialty, need to be carried out by each domain in order to continuously carry out the information security deepening process.

논문접수 : 2004. 8. 16.

심사완료 : 2004. 9. 11.

---

1) 정회원 : 김포대학 컴퓨터 계열 조교수

## I. 서론

컴퓨터와 통신기술등의 급속한 발달은 인터넷의 보급과 사용화에 따라 인터넷을 통한 다양한 정보 서비스가 널리 이루어지고 있다. 전자상거래가 활성화 되고, 산업 및 생활 전반에 걸쳐 전산화가 이루어지면서 사생활 보호 및 정보보호에 대한 요구가 증가하고 있지만 정보보호 산업분야의 전문 인력의 부족으로 많은 어려움이 있다. 때문에 본 논문에서는 실제 정보보호 전문 인력의 수급현황과 정보보호인력의 필요성을 살펴보았다. 그리고 정보보호 전문 인력을 양성하기 위한 교육과정 모델을 제안하기 위하여 정보보호 목표가 교육과정의 설치와 내용에 반영될 수 있도록 NSA가 인증하는 정보보호 인력양성을 위한 연구개발 및 교육분야를 참조하였다. 그리고 지속적인 보안교육이 이루어지기 위하여 졸업 후 전문, 심화 교육과정을 외국의 사례를 제시하였다. 우리의 교육여건을 감안하여 본 논문에서 제안하는 정보보호 전문인력양성을 위한 교육과정모델은 정보보호 분야를 8개의 도메인으로 세분화 하고 각 보안 분야의 전문가가 되기 위하여 전공 기초교과목과 전공 심화 교과목을 링 구조로 제시하였다. 각 심화 단계가 이수되면 반드시 산업계와 학계가 함께 의무적으로 연동이 되어 학생들이 졸업 전 관련 분야의 업무를 실무 프로젝트로 실행하여 졸업 작품과 현장실습의 대체교과목이 되어야겠다.

본 논문의 구성은 다음과 같다. 2장에서는 정보보호 산업에서 전문 인력의 수급현황과 필요성을 살펴보도록 하고, 3장에서는 정보보호 전문인력 양성방안을 외국대학의 교육과정을 사례로 살펴보았다. 그리고 4장에서는 본 논문에서 제안하는 정보보호 산업의 전문 인력에 대한 양성방안을 정보보호의 8개 도메인으로 나누어 각 단계별 교육과정을 링 구조로 모델을 제안하였다. 마지막으로 5장은 결론부분으로 구성된다.

## II. 정보보호 산업의 전문인력 수급현황

### 1. 정보보호 산업의 필요인력 현황

정보보호 산업의 규모가 커지고 정보보호 산업 인력에 대한 수요도 급증하고 있지만 아직까지는 전문이력의 공급이 충분히 이루어지지 못하고 있는 현실이다. 정보보호사회 속에서 다양한 인터넷 이용을 통해 정보의 인프라 구축과 사이버 공간의 활용 등 순기능적인 장점이 있는 반면에 사생활 침해, 해킹, 바이러스에 의한 컴퓨터범죄, 스팸메일, 지적 소유권침해, 음란물, 폭력물들의 범람 등 사회가 더욱 정보화 될수록 정보의 역기능 현상 또한 증가하고 있다. 때문에, 이러한 역기능에 대처할 정보보호 전문 인력이 필요하게 되었다.

현재 정보보호분야 종사자는 [표 1]과 같이 2003년도 2,500여명 정도 부족하며, 2007년도에는 7,000여명으로 확대되어 전체적으로는 20,000여명이 부족할 것으로 예상된다[3].

[표 1] 정보보호 인력 수급 전망

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

이처럼 정보보호 인력 수급의 불균형이 지속적으로 확대됨에 따라 인력 공급을 양적으로 확대할 수 있는 대책이 필요한 것은 물론이며, 정보보호 부분은 일반적으로 타 IT 분야의 인력보다 높은 수준의 인력을 필요로 하고 있고, 알고리즘 및 프로토콜 등의 핵심기술개발에는 고급수준의 전문 인력의 집중양성이 필요한 현실이다.

### 2. 정보보안 전문 인력의 필요성

정보보호 전문 인력의 급증하는 수요에 비하여 그 양적, 질적인 공급이 상당히 미흡한 현실이다. 본 장에서는 정보보호 전문 인력의 필요성에 대하여 다음과 같이 분류하여 기술하고자한다.

첫째, 정보화 사회의 급속한 발달로 정보의 시간적, 공간적 제약이 최소화되는 가운데 그 순기능적인 도움이 우리 생활에 밀접한 연관을 갖고 있

지만 반면에 정보화의 역기능역시 급속히 활성화 되어가고 있는 현실이다. 그렇기 때문에 정보화의 역기능에 대처할 수 있는 원격접속 보안관리, 네트워크의 가용성 유지, 네트워크 및 시스템공격과 악용에 대처 할 수 있으며, 악성코드에 대한 대처를 위한 정보보호 전문가 양성이 필요하다.

둘째, 정보보호분야도 보안을 위한 소프트웨어의 개발과 보안 시스템개발의 국산화가 이루어 저야하므로 정보보호 전문 인력 양성은 정보화 사회의 주요 과제이다.

셋째, 보안에 대한 인식을 위한 지속적인 훈련과 교육을 위한 정보보호 전문 인력의 양성이 필요하다.

넷째, 지속적인 통제와 보호를 위한 모니터링과 감사 기능을 위하여 정보보호 전문가가 필요하다.

다섯째, 컴퓨터 범죄의 발생시 책임에 따른 효율적인 정책을 시행할 수 있는 정보보안 관련 법규의 마련과 조사 및 윤리강령 등의 제정을 위한 정보보호 전문가의 양성이 필요하다. 이처럼 정보보호 전문 인력의 양성은 국가적 정보보호발전과 유지를 위한 필수적인 사항이므로 국가는 물론 민간차원에서도 정보보호 인력양성의 양적인 양성은 물론 질적인 양성방안에 대한 제시가 있어야겠다.

### III. 정보보호 전문인력 양성방안

#### 1. 정보보호 교육의 목적

NSA 등에서는 국가 안보에 미치는 중요성을 인식하여 정보보호 인력 양성에 막대한 투자를 하고 있어, NSA가 인증하는 교육 프로그램을 미국 전역에 걸쳐 7개 대학에서 실시하고 있다. NSTISSC의 훈련 기준을 바탕으로 99년 5월 7개 대학을 CAEIAE(Center of Academic Excellence in Information Assurance Education)로 선정하여 미국 정부 보증의 정보보호 전문 인력을 양성하게 되었다[1],[5].

다양한 분야에 걸쳐 정보보호문제에 대한 접근을 제기하고 있으며, 이는 다음과 같은 연구, 개발 및 교육 분야를 포함한다.

- 컴퓨터 및 네트워크 보안
- 통신 보안(communication security)

- 정보 시스템 보안  
(information system assurance)
- 이동 코드(애플릿 등)상에서의 보안 및 신뢰  
(security and trust in mobile code(applets, etc))
- 전자시대 상에서의 프라이버시 윤리  
(the ethics of privacy in an electronic world)
- 정보보호에 관한 공공정책  
(public policy regarding information security)
- 정보관리 및 정책 개발  
(information management and policy development)
- 정보사용, 남용에 관한 사회적, 법적, 윤리적 관점  
(social, legal and ethical aspects of information use abuse)
- 정보보호 경제학(electronic commerce security)
- 해킹 심리학(the psychology of hacking)
- 컴퓨팅 시스템과 네트워크에 대한 위험관리(risk management for computing systems and networks)
- INFOSEC 전문가들의 인지 및 훈련방법  
(awareness and training methods for infosec professionals)
- 컴퓨터 범죄 수사 및 대응  
(computer crime investigation and response)
- 정보전 이슈들(information warfare issues)

영국 정보보호 교육과정은 주로 다음과 같은 정보보호 목표를 교육과정 설치와 내용의 목표로 하고 있다.

- Confidentiality (비밀성)
  - Integrity (무결성)
  - Availability (유용성)
  - Accountability (책임성)
  - Reliability (신뢰성)
  - Functionality versus Assurance  
(기능성, 보증성)
  - Security threats(보안 위협)
  - Risk analysis(위험성 분석)
  - Providing security)(보안설비)
  - Focus of control(통제의 초점)
  - Location of security controls(보안제어구조)
- 다음과 같은 IT 시스템의 5계층에서 보안을 요구한다고 분류 할 수 있다.
- Application programs(응용 프로그램)

-Services : DBMS 또는 분류된 파일 시스템에 의해 제공된 서비스

- Operating system : 파일운영, 프린터 운영을 수행하는 운영체제 시스템

- Kernel (of Operating System) : 프로세서 및 메모리 접근을 중재하는 커널

- Hardware : 프로세서 및 메모리

. Other security controls(그 밖의 보안 통제)

. Assurance versus complexity (보증성과 복잡성)

. Bypassing security controls(보안제어침투)

. Security management (보안관리)

. Security policies (보안정책)

이와 같은 정보보호 교육의 목적에 따라 미국 등에서는 많은 연구가 수행되고 있다. 우리나라에서는 2000년부터 관련연구들이 처음 시도되는 실정이다[1],[3],[4].

2. 정보보호 교육과정 운영 현황

외국의 경우 정보보호분야의 교과과정을 도입하여 가장 활발하게 교육을 하는 캐나다, 호주, 미국의 대표적인 대학의 경우를 조사하였다.

2.1 캐나다

1) Algonquin College (Ottawa)

정규 4년제 대학의 정보보호관련 학과에서 교과과정을 운영하는 것이 아니라 1년 단위의 정보보호 자격증 프로그램의 일환으로 [표 2]와 같은 교육과정을 제공하고 있다. 이 프로그램을 등록할 자격은 2년제 대학 졸업생 또는 동등한 자로 정하며 이 프로그램은 졸업생들의 경험이나 배경에 따라 정보보호 전문가나 관리자로서 정보 시스템 보안 분야에서 일할 수 있는 기술과 능력을 제공한다[7].

[표 2] Algonquin College (Ottawa)

Course #	교과목	시수
Level: 1	NETWORK SECURITY FUNDAMENTALS	80.0
	INTEGRATED/ENVIRONMENTAL SECURITY	64.0
	ETHICS AND LEGAL/REGULATORY ISSUES	48.0
	COMMUNICATIONS SECURITY	48.0
	INFORMATION SECURITY FUNDAMENTALS	64.0
	INFORMATION ENCRYPTION AND PRODUCTIMPLEMENTATION	48.0

Course #	교과목	시수
Level: 2	COMPUTER SECURITY POLICY	32.0
	THREAT RISK MANAGEMENT	48.0
	INFORMATION SYSTEM SECURITY DESIGN	74.0
	OPERATING SYSTEMS AND APPLICATIONPROGRAM SECURITY	74.0
	BUSINESS CONTINUITY PLANNING	32.0
	INVESTIGATIONS	32.0

2) Georgian College (Barrie)

사이버 공간에 대해 학위 후 48주 연수 프로그램으로서 사이버 범죄로부터 조직과 개인을 방어하고 보호하는데 필요한 지식, 기술, 윤리를 제공한다. 이 프로그램은 학부 (2 또는 4년제) 졸업생이나 그와 동등한 경험을 가진 자를 위한 것이다. 이 프로그램의 진행은 1년 3학기제로 졸업자격은 1년 3학기제로 졸업자격은 [표 3]에 있는 10개의 필수과목과 2개의 선택과목(정보보호 관리자 지망생은 선택과목 아래 2개, 컴퓨터 보안 전문가 지망생은 선택과목의 위쪽 2개)과 인턴십을 패스해야 한다[6].

[표 3] Georgian College (Barrie) 프로그램

범주	과목	시수
필수	Contingency Planning & Disaster Recovery	42
	Security Architecture & Models	42
	Telecommunications & Network Security	42
	Application & System Development Security	42
	Controlling System Access	42
	Cryptography	42
	Ethics, Legal Issues and Investigations	42
	Physical & Operations Security	42
	범주	과목
필수	Security Management	42
	Cyberspace Security Trends and Issues	42
선택	Applied Network Security	42
	Advanced Network Security	42
	Risk Management and Analysis	42
	Managing Security Projects	42
인턴십	Internship	640

2.2 호주

QUT(Queensland University of Technology Brisbane)에 설치된 ISRC (Information Security

Research Center)는 학부와 대학원에 정보보호 프로그램을 발전시켜 오고 있다. 학부과정에 정보보호 전공이 설치되지는 않았지만 데이터통신 전공에 다음의 교과목들이 개설되고 있다.

- Data Security, - Introduction,
- Network Security for E-Commerce

2.3 미국

1) North Carolina State University

North Carolina State University는 Computer Science 학위(석사) 프로그램에 정보보증 심화 과정을 제공하고 있다[표 4].

[표 4] North Carolina State University 프로그램

구분	교과목	비고
필수	Introduction to Computer Security	
	Information System Security	
선택	E-commerce Technology	Project Course (1과목 선택)
	(Inter)Networking Technology & Projects	
	Data Mining	
선택	Applications of Algebra	비 기술적 심화과정 (1과목 선택)
	Advanced Military Science Leadership and Systems Management	
	U.S. National Security Policy	

IV. 제안하는 정보보호전문인력 양성 교육과정

1. 정보보호 전문인력 양성을 위한 교육과정

정보보호 산업분야의 전문 인력을 양성하기 위하여 현재 각 공 교육기관은 물론 사설 교육기관에서도 장기 혹은 단기적으로 강좌가 이루어지고 있지만 현실적으로 전문화된 전문 인력의 양성에 대한 대학의 표준 교육과정이 이루어지지 않은 시점이다. 때문에 본 논문에서 제안하는 정보보호 전문인력 양성을 위한 교육과정을 다음 [표 5]와 같이 분류하였다.

[표 5] 정보보호 전문인력 양성을 위한 교육과정

범주	과목	비고
필수1	보안입문	보안 기본과정
	암호학	
	통신 및 네트워크보안	
	시스템 및 운영체제보안	
필수2	접근통제 및 데이터베이스보안	보안 심화과정
	법, 수사, 윤리강령	
	물리적 및 운영적 보안	
	보안관리	
선택1	사업연속계획, 재해복구	기술적 심화과정
	고급 네트워크보안	
	응용프로그램 시스템개발보안	
	접근통제시스템과방법론	
선택2	보안시스템설계 및 구축	비기술적 심화과정
	보안관리 수행	
	보안정책 및 관리	
	위험관리와 분석	
	사이버 보안관리 및 정책	

먼저, 필수과정을 필수 1의 보안기본과정과 필수 2의 보안심화과정으로 분류하여 보안 기본과정에서는 보안에 관련한 기본 지식이 전혀 결여된 경우 이수해야 될 과정이고, 보안심화과정은 보안에 관련한 프로젝트를 수행하기위한 기본이 갖춰진 경우 이수해야 할 과정으로 분류하였다. 또한, 선택과정도 2단계로 나누어 이수하도록 하며, 선택 1과정은 기술적 심화과정의 단계로서 실제로 보안시스템을 설계하고 구축하여 프로젝트를 완성하고자하는 경우 이수해야 할 단계이며, 선택 2단계는 비 기술적 심화과정의 단계로 분류하였다. 각 단계의 시수의 학기별, 또는 분기별 과정에 따라 적절히 배분하는 것이 바람직하다고 고려하여 [표 5]에서는 제시하지 않았다.

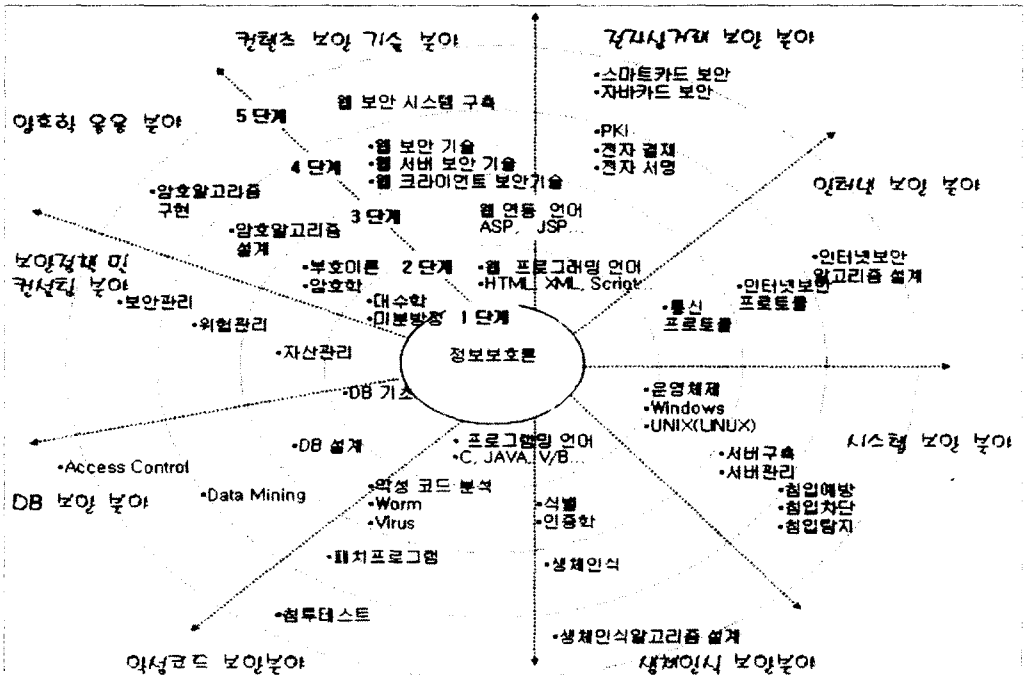
2. 정보보호 응용분야 교육과정

정보보호 전문인력은 다양한 응용분야에 종사하게 된다. [그림 1]은 정보보호의 다양한 응용분야에 종사하게 될 전문인력이 각 응용분야에서 종사하게 된다면 기본적으로 이수해야 할 과정을 9개 도메인 별로 분류하였다.

정보보호의 응용분야의 9개 도메인은 암호학 응용 분야, 컨텐츠 보안기술 분야, 전자상거래 보안 분야, 인터넷보안 분야, 데이터베이스 보안 분야, 생체인식 보안 분야, 시스템 보안 분야, 네트워크 보안 분야, 보안정책 및 컨설팅분야 등으로 분류 하였다.

각 보안 응용분야는 링 구조로 표현하였으며, 교육 과정이수는 단계별로 세분화가 되도록 하지만, 중복되는 과목은 절삭의 과정에 의하여 실행되어야 한다. 가장 안쪽의 링은 보안 전문 인력이 이수해야 할 기본적인 교육과정이고 다음단계의 링은 해당되는 보안응용분야에서 단계별로 이수해야 할 기초 교육과정과 전문교육과정 등으로 이루어진다. 전공기초 과정으로는 정보보호 분야에 대한 기초적인 이론적 지식기반 과 실무

능력을 배양하도록 교육과정을 제안하였다. 가장 안쪽의 링(ring)에는 정보보호 응용분야의 인력으로서 갖추어야 될 기본적인 정보보호이론 이수하여 보안의 기본 이론을 이해하도록 한다. 다음 2 단계부터 3, 4 단계 까지는 보안과 직접적인 관련이 있는 과목이라기보다는 전문 응용분야를 위한 기본 이수과정이라고 할 수 있다. 2단계의 링은 보안교육을 위한 전공 기초 교육과정을 이수하도록 설정하였으며, 정보보호의 분야에 따라서 중복되는 분야가 있을 수 있으므로 학생들은 선택과목으로 이수가 가능하도록 한다. 프로그래밍 언어를 시스템프로그래밍 혹은 클라이언트-서버 프로그래밍 또는 웹 프로그래밍 언어 등으로 분류하여 교육이 가능하도록 한다. 전산관련 기초교과목인 데이터베이스, 운영체제, 자료구조 등의 과목들이 전공 기초 과정에서 이수되어야 하겠다. 다음 3단계 링은 보안 관련분야와 연



[그림 1] 정보보호 응용분야 분류와 교육과정

응용을 위한 기술적인 요소를 함께 접근할 수 있는 계된 전공과목을 이수하도록 한다. 4단계 링 구조

에서는 보안관련 전문 응용분야의 인력양성을 위하여 이수해야 되는 정보보안 필수 교육과정이다. 과목이 해야 하는 과목을 필수적으로 수강하도록 한다. 예를 들면, 시스템 보안 분야를 전공심화과정으로 이수하고자 한다면, 운영체제를 윈도우즈와 유닉스 계열을 기반으로 하는 서버에서 각 시스템의 보안관리, 침해사고 대응, 해킹 예방, 시스템 분석 그리고 지속적인 모니터링과 감사 기능을 갖추도록 운영체제에 대한 관리자과정을 이수하고, 서버구축 및 관리 그리고 침입 예방, 차단, 탐지 시스템 등을 구현할 수 있도록 하는 것이 바람직하다. 이러한 교육과정은 반드시 산업체 현장교육과 연계되어 실무교육이 함께 병행되기를 권고한다. 졸업반 학생들이 산업체의 프로젝트를 의뢰받아서 6개월 혹은 1년간의 과제 수행을 진행하도록 하여 산업체에서 요구하는 전문인력 양성과정이 산업체와 학계의 의무조항이 되도록 정부의 지원이 필요하다. 그리고 지속적인 전문 자격증 취득 및 학습이 이루어지도록 졸업 후 학점인정과정 혹은 사이버 강좌 등의 개설로 지속적인 보안 교육이 이루어 져야겠다.

## V. 결론

정보보호 인력의 수급현황은 양적으로 뿐만 아니라 질적으로도 부족한 현실이다. 때문에 정보보호 전문 인력을 양성하기위한 교육과정을 개발하기위하여 국제표준으로 제시된 정보보호 목표에 맞는 정보보호 교육과정을 살펴보았다. 본 논문에서 제안하는 정보보호 전문인력 양성을 위한 교육과정은 필수 1, 2 단계와 선택 1,2단계의 기본 교육과정을 제시하였다. 그리고 그에 준하여 정보보호 응용분야의 전문 인력 양성을 위하여 9개의 도메인으로 세분화 하여 각 단계별로 시행되어야 할 선행 교육과정을 단계적으로 제시하였다. 제안한 9개 도메인으로 구성된 정보보호 분야에 따른 교육과정은 현장 실무 프로젝트와 연계된 교육이 이루어져서 산업체에서 요구하는 전문 인력이 졸업과 동시에 현장에 투입될 수 있도록 교육과정을 진행하여야 하며, 졸업 이후에도 지속적인 보안 교육을 위하여 도메인별로 학점인정 기관 혹은 자격증 취득 강좌 등으로 개설이 되어 진행되기를 기대한다.

## < 참고 문헌 >

- [1] 김 철(2001), 대학의 정보보호 교육과정 개발 연구, 정보보호 학회지, 제11권 3호.
- [2] 이경애, 김 철,(1999), "NIST SP 800-16소개", 한국통신정보보호학회 종합학술대회 논문집 Vol. 9, No. 1, pp 219-227
- [3] 이형우, 이민섭(2003), 정보보호 인력양성 방안에 관한 연구, 정보보호 학회지 제13권 2호.
- [4] Krutz, Vines (2003) The CISSP Prep-Guide Gold Edition.
- [5] Mark Willson(1998), "NIST Special Pub. 800-16", US Dept of Commerce, NIST.
- [6] <http://www.georcoll.on.ca/>
- [7] <http://www.algonquinc.on.ca>

이 문 구 (Moon-ku Lee)



1984년 숭실대학교  
전자계산학 (학사)  
1993년 이화여자대학교  
대학원 전산교육학 (석사)  
2000년 숭실대학교 대학원  
컴퓨터공학 (박사)  
2000년 3월 - 현재  
김포대학 컴퓨터계열 조교수

관심분야 :

컴퓨터 교육과 교수법 및 교육과정

네트워크 프로그래밍

인터넷 보안, 시스템 보안, 암호화 알고리즘

전자상거래 보안, 침입탐지 및 차단시스템