직무별 특성을 고려한 대학 정보보호 학과의 교육분야 선정 및 운영에 관한 연구

임원규* · 신 혁** · 안성진***

요 약

사이버 공격의 지능화, 조직화로 몇몇 소수의 정보보호 전문가만으로 사이버 위협에 대응할 수 없는 시대가 되었다. 이에 따라 대학의 정보보호 관련학과가 2013년에 비해 17%나 증가했다. 하지만 대학의 교육은 실제 산업현장에 필요한 인력을 양성하는데 한계를 노출하고 있다. 본 연구에서는 이를 개선하기 위해 정보보호 직무체계 및 분야별 필요 교육내용에 대한 연구를 조사하였다. 이후 이를 바탕으로 대학에서 학습되어야하는 정보보호 분야를 도출하였다. 그리고 도출된 분야의 교육과정을 운영하기 위한 방안으로 교육내용 선정 및 인증에 대한 방안을 제시하고 있다. 본 연구를 국가정보보호백서에서 조사되는 정보보호 인력 현황과 연계해 대학 정보보호 관련학과의 분야를 조절할 수 있을 것으로 기대된다. 그리고 실 현장의 수요를 반영한 인력을 배출할 수 있는 정보보호 인력 중장기 계획의 기초 연구로 활용되고자 한다.

A Study on Selecting and Operating Educational Department in Cyber Security Major by Analyzing Workforce Framework

Won Gyu Lim* · Hyuk Shin** · Seong Jin Ahn***

ABSTRACT

Because intelligent and organized cyber attack, It is difficult to respond to cyber threats with only a small number of information security experts. Accordingly, information security department compared to 2013 it increased by 17%. But there was a problem that cannot train appropriate students for companies. This research examined the Workforce Framework and Knowledge Units for improving this situation. Based on this, educational department in cyber security major was selected to be learning at the university. And it proposed a plan for a managing course to operate. And the result will be utilized as fundamental research of human resources medium- and long-term demand and supply planning in cyber security department.

Key words : Cyber Security, Workforce Framework, Curriculum

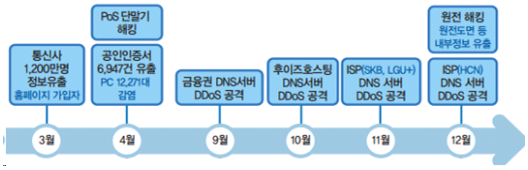
접수일(2015년 6월 3일), 수정일(1차: 2015년 6월 20일), 게재확정일(2015년 6월 29일)

* 성균관대학교/컴퓨터교육학과
** 한국산업기술보호협회
*** 성균관대학교/컴퓨터교육학과 (교신저자)

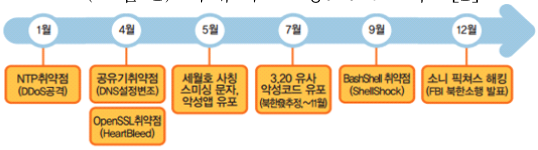
1. 서 론

다양한 IT 기기와 인터넷 등의 발전으로 정보화 시대가 도래 하였다. 이에 따른 역기능으로 사이버공격 또한 점차 지능화, 조직화 되어 보다 큰 손실을 초래하고 있다. 사이버 공격에 대한 위험으로 인해 기업들은 망분리 및 다양한 보안 솔루션을 도입하여 사고에 대응하고 있지만 보안 사고는 여전한 실정이다.

2015년도 국내 정보보호 백서를 보면 13, 14년도의 3/20 사이버테러, 6/25 사이버공격과 같은 대규모 공격을 발생하지 않았지만 고위험의 취약점과 다양한 형태의 침해사고가 발생한 것으로 확인 된다.[1]



(그림 1) 국내 주요 정보보호 사고[1]



(그림 2) 취약점 및 악성코드 이슈[1]

그리고 노턴의 2013 사이버범죄 보고서를 보면 사이버범죄의 피해자는 감소했지만 피해액은 증가한 것으로 조사되고 있다.[2] 이런 현상은 특정 대상을 지정한 공격이 증가하고 있기 때문일 것이다. 이런 현상에 대응하기 위해서는 단순한 기술적인 보안대책을 넘어 보다 종합적인 대책이 필요할 것이다.

이러한 종합대책의 가장 기본이 되는 항목이 정보보호 인력의 양성일 것이다. 이를 뒷받침하듯 정부는 2013년 미래창조과학부의 사버안보종합대책을 통해 최정예 정보보호 전문인력 5,000명 양성, 정보보호 전문인력 체계적 양성을 위한 방안[3] 을 제시하였다.

이에 필요한 분야에 적합한 정보보호 전문인력을 양성하기 위해서는 실 기업환경에서의 정보보호 직무체계가 필요하고 체계별 교육분야를 선정해 교육되어야 할 것이다.

이에 관련해 미국의 NICE에서 제시된 Workforce Framework, KISA의 정보보호 진로 가이드, 정보보호백서의 정보보호 인력분류 등이 정보보호 인력양성을 위해 필요한 전문분야일 것이다.

그리고 해당 분류별 교육내용에 관한 연구 및 사례로 미국의 CAE IA/CD(National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD))와 KISA의 정보보호 진로 가이드에 제시된 교육훈련 로드맵 등이 있다.

그리고 현재 국내의 정보보호 정규교육과정은 8개의 전문대학, 36개의 대학교, 32개의 대학원에서 76개의 학과가 운영중이고 2013년 대비 17% 증가한 것으로 조사되어 있다.[1] 이렇게 교육기관은 증가하고 있지만 정보보호 관련 학과의 교육내용은 정보보호 개발 분야에 집중되어 있어 컴퓨터공학과와의 차별성이 부족하는 것이 문제점으로 도출되어 있다.[4]

본 연구에서는 국내 정보보호 관련 학과의 양성되어야하는 교육분야를 선정하고 운영하는 방안에 대하여 제시 할 것이다.

2. 관련연구

2.1 미국의 정보보호 인력 분류 및 인증 사례

2.1.1 NICE의 Workforce Framework

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[5]. 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.

또한 각 기업별로 상이한 정보보호 직무에 대한 표

준을 제시하고 해당분야 종사자에 대한 교육을 표준화하기 위해 Workforce Framework을 발표하였다.

정보보호 분야의 직무체계로 제시된 Workforce Framework의 7개 Categories와 31개의 세부 직무로 분류되어 있다.

<표 1> NICE에서 제시된 정보보호 직무체계[6]

Categories (직무군)	Specialty areas (세부직무)
Securely Provision (정보보호 제품 및 시스템 개발)	Information Assurance Compliance (정보시스템 인증)
	Software Assurance and Security Engineering (소프트웨어 개발 및 정보보호 공학 기술)
	System Development (시스템 개발)
	System Requirements Planning (시스템 요구분석)
	Systems Security Architecture (보안 시스템 구조)
	Technology Research and Development (최신동향 연구 및 개발)
	Test and Evaluation(테스트 및 평가)
Protect and Defend (사전 침투 방어)	Computer Network Defense Analysis (네트워크 위협분석)
	Computer Network Defense Infrastructure Support (기반시설 네트워크 방어)
	Incident Response (사고대응)
	Vulnerability Assessment and Management (취약점 분석 및 관리)
Oversight and Development (감독 및 총괄)	Education and Training (교육 및 훈련)
	Information Systems Security Operations (Information Systems Security Officer) (정보시스템 보안 운영)
	Legal Advice and Advocacy (법률 자문)
	Security Program Management (Chief Information Security Officer) (최고정보보호 관리자)
	Strategic Planning and Policy Development (정보보호 전략 기획 및 정책 수립)
Operate and Maintain (관리)	Customer Service and Technical Support (고객 관리 및 지원)
	Data Administration
	Knowledge Management (지식 경영)
	Network Services (네트워크 서비스)
	System Administration (시스템 관리)
	Systems Security Analysis (시스템 보안 관리)
Investigate (사후 조사)	Digital Forensics (디지털 포렌식)
	Investigation (사이버 수사)
Collect and Operate (수집 및 해독)	Collection Operations (데이터 수집 관리)
	Cyber Operations (사이버 범죄 및 테러 관련 증거 수집)
	Cyber Operations Planning (사이버 운영 계획)
Analyze (진단 및 평가)	All Source Intelligence (정보종합 분석)
	Threat Analysis (위협 분석)
	Exploitation Analysis (공격 분석)
	Targets (신지식 적용)

2.1.2 미국의 교육지원 프로그램 CAE IA/CD

NSA에서 NICE를 지원하기위한 교육프로그램으로 CAE(National Centers of Academic Excellence (CAE) in Cyber Operations Program)를 공표, 운영 중이다. 이는 정보보호 전문인력 풀을 확보하고 국가 보안을 지원하기 위한 프로그램이다. 이 프로그램은 미국 국가의 허가를 받은 2년제, 4년제 대학 수준의 기관이 NSA/DHS에 의해 교육과정을 인증 받아 지정되는 것이다[7].

해당 교육내용은 2년, 4년과정의 기본 교육내용과 옵션 교육내용으로 분류해 제시되고 있다. 아래의 <표 2>, <표 3>, <표 4>는 각 과정에서 교육되어야 할 KUs(Knowledge Units)이고 <표 5>에 제시된 세부내용은 각 교육내용의 정의와 주제, 결과물들을 나타낸 것이다.[8]

<표 2> CAE IA/CD에 제시된 2년 과정 기본교육내용(CORE KUs for 2 year programs), 일부

순 서	Knowledge Units
1	Basic Data Analysis (데이터 분석 기초)
2	Basic Scripting or Introductory Programming (4 yr core) (프로그래밍 입문)
3	Cyber Defense (사이버 방어)
4	Cyber Threats (사이버 위협)
5	Fundamental Security Design Principles (보안설계 원칙)

<표 3> CAE IA/CD에 제시된 4년 이상 과정 기본교육내용(CORE KUs for 4 year + programs)

순 서	Knowledge Units (2년 과정의 KU 포함)

1	Databases (데이터베이스)
2	Network Defense (네트워크 보안)
3	Networking Technology and Protocols (네트워크 일반)
4	Operating Systems Concepts (운영체제 개론)
5	Probability and Statistics (확률과 통계)
6	Programming (프로그래밍)

<표 4> CAE IA/CD에 제시된 선택 교육내용 (Optional KUs), 일부

순 서	Knowledge Units
1	Advanced Cryptography (암호학 심화)
2	Forensic Accounting (법회계학)
3	Algorithms (알고리즘)
4	Analog Telecommunications (아날로그 통신)
5	Cloud Computing (크라우드 컴퓨팅)

<표 5> KU 세부내용(ex, IT System Components)

정의	The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.
교육 주제	Workstations Servers Network Storage Devices Routers / Switches / Gateways Guards / CDSes / VPNs / Firewalls IDSes, IPSes Mobile Devices Peripheral Devices / Security Peripherals
결과	Students will be able to describe the hardware components of modern computing environments and their individual functions.

2.2 국내의 정보보호 인력 분류 및 교육 현황

2.2.1 국내 정보보호 인력 분류 현황

미래부와 KISA(한국인터넷진흥원)에서 제시된 정보보호 진로가이드는 NICE에서 제시된 Framework를 기반으로 정보보호 인력의 분류를 제시하고 있다. 아래 <표 6>에서 내용을 확인 할 수 있다.[9]

<표 6> 정보보호 진로가이드의 직업분류

분야	직업
보안제품 개발자 (Security System Developer)	SW분석/설계전문가
	SW개발자
	보안제품 기술자
	SW테스트기술자(품질관리자)
	보안제품 기술영업
침해사고 대응 전문가 (Incident Handling Specialist)	사이버 보안 관제사
	취약성 분석 전문가
	모의 해킹 전문가
보안 컨설턴트 (Security Consultant)	정보시스템 감리사
	정보시스템 보안감사
	보안제품 인증 전문가
	보안관리 인증 전문가
	보안기술 컨설턴트
	사이버 보안 관제사
디지털포렌식 전문가 (Digital Forensic Specialist)	사이버 범죄 수사관
악성코드 분석 전문가 (Malicious Code Analysis Specialist)	암호/해독전문가
최고 보안 관리자 (보안전략전문가) (Chief Security Manager (Security Strategy Specialist))	보안관리 기획자
	준법 감시자
	보안 교육 전문가 (변화관리전문가)
	보안전문검사/변호사
	개인정보보호 전문가
	보안전문교수/기자
	국제 보안 전문가
보안관리자 (Securty Manager)	지식 관리자
	DB보안 관리자
	정보시스템(네트워크) 관리자
	보안시스템 관리자
	개인정보보호 관리자

국내의 정보보호 백서에서도 정보보안 산업의 인력 수준 현황을 조사하기 위해 인력을 분류한 내용이 있다. 아래 <표 7>에서 해당 분류를 확인 할 수 있다.[1]

<표 7> 2015 정보보호 백서에 제시된 인력 분류

구분	세부분류
정보보안 연구 및 개발직	암호 및 인증 기술
	시스템 및 네트워크 기술
	응용기술 및 서비스

정보보안 관리직	정보시스템관리
	정보보안컨설팅
	정보보안관제
정보보안 영업직	정보보안마케팅
기타 정보보안 관련직	정보시스템 감리 및 인증
	정보보안교육
	기타

3. 정보보호 학과의 교육분야 선정

3.1 연구절차

본 연구에서는 대학의 정보보호 학과 교육의 분야 선정을 위해 위의 관련연구에서 제시한 NICE의 Workforce Framework의 7개 분류, KISA의 정보보호 진로가이드에 제시된 7가지 분류 그리고 정보보호백서에서 인력의 관리시 사용한 분류를 이용해 필요 분야를 선정 할 것이다.

각 분류에서 대학교육과정으로 합당하지 않은 영역 제거 ⇒ 3가지 분류의 공통적으로 포함된 영역 삭제 ⇒ 도출된 분류에 포함 가능한 세부영역 재 분배

이후 교육분야의 교육내용 선정 및 인증 방안에 대해 논의 할 것이다.

3.2 정보보호학과의 교육분야 도출

NICE의 Workforce Framework에 제시된 Collect and Operate, Analyze의 경우 매우 전문적인 분야로 세부 직무 및 필요 기술들이 제시되지 않고 있다. 따라서 대학 이상의 과정에서 다루어져야하는 과정으로 교육 분야에서 제외하였다. 그리고 KISA의 정보보호 진로 가이드의 악성코드분석 전문가와 보안컨설팅, 최고보안관리자 과정의 경우 각각 보안제품개발과정과 보안관리자과정 등의 심화 과정으로 분류 대학 교육분야에서는 제외 하였다. 이를 고려하여 4개의 교육분야를 도출하였다.

<표 8> 대학의 정보보호 교육분야 선정

교육분야	직무 분야 및 세부직무
보안제품개발자 (Securely Provision)	SW분석/설계전문가
	SW개발자
	보안제품 기술자
	SW테스트기술자 (품질관리자)
	보안제품 기술영업
	암호 및 인증 기술
	시스템 및 네트워크 기술
	응용기술 및 서비스
	Information Assurance Compliance (정보시스템인증)
	Software Assurance and Security Engineering (소프트웨어개발 및 정보보호 공학기술)
	System Development (시스템개발)
	System Requirements Planning (시스템 요구분석)
	Systems Security Architecture (보안시스템구조)
	Technology Research and Development (최신동향 연구 및 개발)
	Test and Evaluation (테스트 및 평가)
침해사고대응 전문가 (Protect and Defend)	사이버보안관제사 (보안 관제요원)
	취약성 분석 전문가
	모의 해킹 전문가
	Computer Network Defense Analysis (네트워크위협분석)
	Computer Network Defense Infrastructure Support (기반시설 네트워크 방어)
	Incident Response (사고대응)
	Vulnerability Assessment and Management (취약점 분석 및 관리)
보안관리자 (Operate and Maintain)	지식 관리자
	DB 보안 관리자
	정보시스템(네트워크)관리자
	보안시스템 관리자
	개인정보보호 관리자
	정보시스템관리
	정보보안컨설팅
	정보보안관제
	Customer Service and Technical Support (고객관리 및 지원)
	Data Administration
	Knowledge Management (지식경영)
	Network Services (네트워크 서비스)
	System Administration(시스템관리)
	Systems Security Analysis (시스템보안관리)
디지털포렌식 전문가 (Investigate)	사이버 범죄 수사관
	Digital Forensics (디지털 포렌식)
	Investigation (사이버수사)

위 <표 8>에서 관련연구를 종합하여 대학의 정보보호 관련 교육분야를 도출하였다. 이는 기 제시된 정보보호 관련 직무체계 및 정보보호 진로가이드를 기반으로 도출된 것으로 정보유출관련의 산업보안 및 침해사고대응 부분의 보안관제 부분 등 향후 연구를 통해 지속적으로 개선되어야 할 것이다.

4. 정보보호 교육분야의 운영방안

이번 장에서는 도출된 분야의 운영방안에 대하여 제시할 것이다. 우선 도출된 분야별 세부 교육내용이 선정되어야할 것이다. 이것은 KISA의 정보보호진로가이드에 제시된 교육훈련 로드맵을 예시로 아래 <표 9>에서 확인 할 수 있다. 교육내용의 선정의 경우는 각 대학의 교육 목표에 따른 고유영역으로 각 대학에서 선정하여 운영하여야 한다.

<표 9> 정보보호 진로가이드 제시 교육훈련 로드맵

교육분야	교과내용
보안제품 개발자	전자상거래보안, 융합보안, 기반시설보안, 모바일보안, 컴퓨터보안, 전자금융보안, 데이터베이스보안, 클라우드보안, 웹보안, 디지털콘텐츠보안, 시스템보안, 역공학기법, 네트워크보안, 암호학, 정보보호개론, 전자서명, 정보보호시스템 설계 및 개발, 해킹과 바이러스
침해사고대응전문가	사이버테러와 정보전, 보안취약점분석, 국가사이버안보학, 해킹과 바이러스, 사이버위기관리, 역공학기법, 정보시스템보안감사, 사이버범죄, 정보보호개론, 정보보호 법과 윤리
보안관리자	전자상거래보안, 개인정보보호, 산업보안, 국가사이버안보학, 융합보안, 클라우드보안, 기반시설보안, 모바일보안, 데이터베이스보안, 전자금융보안, 네트워크보안, 사이버테러와 정보전, 웹보안, 디지털콘텐츠보안, 컴퓨터보안, 정보보호진단 및 컨설팅, 사이버위기관리, 정보시스템보안감사, 정보보호관리체계, 사이버범죄, 시스템보안, 전자서명, 보안취약점분석, 해킹과 바이러스, 정보보호시스템 운영관리, 정보보호정책, 정보보호 법과 윤리, 정보보호개론
디지털포렌식전문가	디지털포렌식, 암호학, 정보보호 법과 윤리, 사이버 수사, 사이버 범죄, 정보보호개론

교육과정 운영 중 이를 인증하는 방안으로 CAE IA/CD에서 사용중인 방안을 제안한다. 이 방안은 교육주제(Topic)을 제시해 운영 중인 교육과정이 얼마나 주제에 적합하게 구성되었는지를 평가하는 방식이다. 아래 <표 10>에 CAE IA/CD에서 제시된 교육주제를 확인 할 수 있다.

<표 10> 교육인증 방안

교육내용	교육주제
Basic Data Analysis	Summary Statistics
	Graphing / Charts
	Spreadsheet Functions
	Problem solving
Basic Scripting	Basic Security - Bounds checking, input validation
	Program Commands
	Program Control Structures
	Variable Declaration
	Debugging
	Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)
	Basic Boolean logic/operations. - AND / OR / XOR / NOT

그리고 교육기관에 대한 인증 기준으로 교육기관간의 협력, 융합교육으로서의 커리큘럼, 정보보호의 실무적 노력, 학생의 정보보호 연구를 위한 인센티브, 현 교수진의 정보보호 활동 및 연구실적, 정보보호 자원, 교육기관의 정보보호 프로그램 운영, 정보보호 교육센터 설립 및 운영, 정보보호 관련 교수진 수 및 강좌수를 제시하고 있다.

5. 결 론

사이버 공격이 더욱 지능화, 고도화되어 몇몇 소수의 정보보호 전문가만으로 사이버 위협을 담당할 수는 없는 시대가 되었다. 이런 환경에서 보다 중요시 되는 것이 정보보호 전문가의 양성, 기존 전문가의 수준 향상 등의 정보보호 관련 교육일 것이다.

이에 본 연구는 국내외 정보보호 인력의 체계를 조사한 연구와 분야별 학습필요 내용, 국내 대학 정보보호 관련학과에 대한 연구를 조사 분석하였다. 이를 토대로 적합한 정보보호 전문인력을 양성하기 위해 대학에서 학습되고 배출되어야하는 정보보호의 전문분야

를 도출하였다. 그리고 해당 전문분야의 교육내용을 구성하고 인증하는 방안을 통해 운영방안을 제시하였다.

도출된 정보보호 전문분야는 정보보호백서에서 조사되는 정보보호 인력 현황과 연계해 인력의 수 조절이 가능할 것이다. 그리고 중장기적인 계획을 반영 필요 기술 또는 분야의 인력을 양성하는데 도움이 될 것으로 기대된다. 이를 위해 도출된 전문분야는 지속적으로 수정 보안되어야 할 것이다. 그리고 운영 방안의 경우 선행연구에서 도출된 내용을 제시한 것으로 향후 연구를 통해 현 국내의 실정을 반영한 교육내용 및 인증방안이 추가 도출되어야 할 것이다. 이 방안의 도출을 통해 각 대학들이 교육과정에 포함할 수 있는 교육내용의 제시하고 이를 이용한 교육과정 도출 모델을 구성할 수 있을 것이다. 이를 통해 대학의 정보보호 학과의 교육내용이 표준화 될 수 있을 것을 기대할 수 있다.

추가적으로 본 연구에서 선정된 교육분야별 필요 역량을 조사하여 대학교육 또는 고용을 위한 고등교육 시 반영할 수 있는 방안이 향후 제시되어야 할 것이다. 그리고 본 연구에서 도출된 내용은 전문가 또는 실 업무 담당자를 통한 검증을 통한 확인이 필요 할 것이다.

참고문헌

[1] 국가정보원, 미래창조과학부 등 "2015 국가 정보보호 백서" 2015

[2] 시만텍 "2013 노턴보고서 사이버 범죄 보고서" 2013

[3] 미래창조과학부 "사이버안보종합대책" 보도자료 2013.07

[4] 임원규 외 "국내 정보보호학과의 교육과정 분석을 통한 개선방안 연구"2014

[5] 김동우 외 2명 "국내 정보보호 교육체계 연구" 2013.03

[6] NICE "THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK, http://csrc.nist.gov/nice/framework. national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing" 2014

[7] 양정모 외 5명 "대학의 정보보호 관련학과 교육과정분석과 모델개발에 관한 연구" 2003.06

[8] NSA, DHS "CAE Knowledge Units" 2014

[9] 한국인터넷진흥원 "kisa_academy_security_guide_book" 2014

[10] 장항배 "정보보호 직업별 교육 훈련 로드맵 구축" 2013

[저 자 소 개]

임 원 규 (Won-gyu Lim)

2008년 서울산업대학교 산업정보시스템공학과 학사
2011년 서울산업대학교 IT정책전문대학원 산업정보시스템공학과 석사
2011년 ~ 현재 성균관대학교 대학원 컴퓨터교육학과 박사과정

email : wglim@skku.edu

신 혁 (Hyuk Shin)

1987년 건국대학교 전자공학사 공학사
1995년 건국대학교 산업공학과 공학석사
2006년 Kansas State University 경영학과 MBA

email : hyukshin@kaits.or.kr

안 성 진 (Seong-jin Ahn)

1988년 성균관대학교 정보공학과 학사
1990년 성균관대학교 정보공학과 석사
1998년 성균관대학교 정보공학과 박사
1990년 ~ 1995년 KIST/SERI 연구원
1996년 정보통신기술사
1999년 ~ 현재 성균관대학교 컴퓨터교육과 교수

email : sjahn@skku.edu