정보보호 인력양성을 위한 효율적인 정보보호관리체계의 융합 관리 방안

이근호
백석대학교 정보통신학부

A Measures to Converge Manage an Efficient Information Security Management System for Information Security Experts Manpower

Keun-Ho Lee
Division of Information & Communication, Baekseok University

요 약 IT기술의 발전으로 인하여 각종 새로운 서비스모델을 통한 다양한 서비스가 제공이 되고 있다. 이러한 새로운 서비스의 제공으로 인한 새로운 보안위협이 증가하고 있는 상황이다. 국가적으로도 보안위협으로부터 안전한 자산을 보호하기 위한 각종 정보보호 인력 양성프로그램이 운영이 되고 있다. 제도적으로도 정보보호관리체계를 통하여 새로운 서비스와 기존 서비스에 대한 안전성을 검증하면서 기관 인증을 해주고 있다. 사회적으로도 정보보호에 대한 인식이 확산되어 많은 대학이 정보보호 인력 양성을 위한 과정을 운영중이다. 아울러 정보보호 인력양성을 위한 정보보호동아리에 대한 관리도 함께 병행하고 있다. 본 연구에서는 각 대학의 정보보호 인력 양성시 필요한 정보보호관리체계(ISMS)에 대한 교과과정의 운영과 정보보호동아리의 효율적인 융합관리 방안을 제안하고자 한다. 정보보호 인력의 양성을 통하여 안전성을 좀더 보완하는 융합형 정보보안 전문 과정으로 IT기반의 사회의 안전에 기여가 예상된다.

• **주제어** : 정보보호, 정보보호관리체계, 융합, 관리, 안전

Abstract The development in IT technology has brought about various services that are on offer based on a new service model. But such new services have increased security risks. The government is operating a program to foster experts in information security to protect assets from the threat of such risks, too. Society's awareness on the importance of information security has also grown, leading to various courses to train such personnel, including membership clubs for the fostering of such specialists. This study seeks to suggest a method that efficiently manages the convergence of running a curriculum on ISMS(information security management systems) and a club that focuses on information protection. Such converged information security courses are expected to contribute to a safer IT-based society.

• **Key Words** : Information Security, ISMS, Convergence; Management, Safety

1. 서론

최근 IT의 급속한 발전은 다양한 융.복합 환경으로 급속한 변화가 이루어지고 있다. 특히 IoT(Internet of Things) 사물인터넷으로 인한 다양한 서비스 모델이 제

본 논문은 2014년도 백석대학교 대학 연구비에 의하여 수행된 것임
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2014년 8월 25일 수정일 2014년 11월 10일 게재확정일 2014년 11월 15일

공이 되고 있다. 이러한 IT와 IoT의 발전으로 인하여 개인정보와 기업정보 등 중요 정보자산에 대한 위협과 취약점이 어느 때 보다도 매우 심각하게 대두되고 있다. 정보보안의 취약점과 위협을 최소화하기 위한 제도들이 만들어지고 있으며, 그중에 대표적인 제도가 정보보호관리체계(ISMS:Information Security Management System)이다. ISMS는 정보보안에 대한 적절한 위험관리 활동의 필요성에 의해서 제도화되었다. 이를 위해 조직에서 정보자산을 보호하고 조직 역량을 강화하기 위한 수단으로 정보보호관리 프로세스 개선활동의 하나로 ISMS 구축과 함께 인증을 받고 있다. 기업의 정보자산의 가치는 조직 발전에 중요한 요소이며, 이러한 중요 정보자산에 대한 체계적이며 종합적인 정보보호 관리체계 운용만이 조직의 정보자산의 손실을 최소화하고 경쟁우위를 확보하여 기업의 신뢰도와 조직의 가치를 높이는 수단이 된다. 최근에는 이러한 조직의 비즈니스 연속성 확보뿐만 아니라 다양한 사이버공격과 같이 매우 지능화되고 있는 침해사고에 대응하기 위한 정보보호 조직을 구축하고, 정보보호 업무배치를 하여 회사의 중요자산을 확보하고자 하는 노력들을 많이 진행하고 있다. 이런 사이버 공격과 정보중요 자산에 능동적이고 선제적으로 대응하여 정보보호 침해사고에 대한 사전적 예방을 위한 노력으로 국내.외적으로 정보보호 관리체계 도입을 제도화 하고 있다. 현재 국내.외에서 적용하고 있는 정보보호 관리체계로는 ISO27001(Information security management systems Requirements), NIST SP800-39(Managing Risk from Information Systems An Organizational Perspective), KISA ISMS(Korea Internet & Security Agency Information Security Management System), PIMS(Personal Information Management System,), G-ISMS (Government-Information Security Management System), ISCS(Information SecurityCheck Service), CIIP(Critical Information Infrastructure Protection) 등에 대해 제도적으로 시행해 오고 있다. 이러한 제도는 정보보호 특성상 성과나 효과를 나타낼 수 있는 성과 지표의 표기가 어렵다[1].

이러한 정보자산을 안전하게 보호하기 위한 과정으로 실시되고 있는 정보보호관리체계와 IT의 발전으로 인한 정보보호의 중요성의 대두로 인하여 많은 대학들이 정보보호관련 전공을 개설하고 있다. 정보보호관련 전공에서도 정보보호관리체계의 효율적인 실무 역량을 강화하기 위하여 교과과정으로 운영하는 곳이 생겨나고 있다.

따라서 본 연구에서는 정보보호 관리체계에 대한 정확한 이해를 통하여, 정보보호 전공의 학생들이 어떻게 정보보호관리체계를 학습하여 실무에서의 역량을 강화할 지에 대한 내용을 살펴보고자 한다. 이러한 정보보호 관리체계를 통하여 정보보호에 관심 있는 학생들과 정보보호 동아리의 학생들을 효율적으로 관리하고 있는 방안을 제안하여, 국내 정보보호 인력의 확산을 통한 정보보호 전문인력 양성을 통한 중요 정보자산의 안전성을 확보할 수 있는 방안을 제안하고자 한다.

2. 관련 연구

2.1 정보보호관리 체계(ISMS)

조직의 중요 정보자산에 대한 안전성 확보와 신뢰성을 향상시키기 위한 절차적 과정을 체계화고, 문서화하여 지속적으로 정보자산에 대한 관리와 운영을 통하여 정보 자산에 대한 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정에 대한 지속적인 정보보호 개선활동을 정보보호관리체계 (ISMS)라고 한다. ISMS 제도는 통제항목 104개로 관리과정 5개 통제분야 12개 항목, 보호대책 13개 통제분야 92개 항목으로 구성이 되어 있다. 관리적 통제항목은 정보보호 정책 수립 및 범위 설정, 경영진 책임 및 조직 구성, 위험관리, 정보보호대책 구현, 사후관리로 구성되어 있다. 정보보호대책 통제항목은 정보보호정책, 정보보호 조직, 외부자 보안, 정보자산 분류, 정보보호 교육, 인적 보안, 물리적 보안, 시스템 개발보안, 암호통제, 접근통제, 운영보안, 침해사고 관리, IT재해복구의 항목으로 구성이 되어 있다. ISMS 의무대상자의 서비스 범위는 다음과 같다. 기간통신, 부가통신으로 나누어 진다. 기간통신의 경우 주요정보통신서비스제공자로서 초고속인터넷 서비스, 초고속 가입자망 서비스, 기타 초고속 통신 서비스, 무선데이터접속 서비스로 ISP 관련 대상자 영역으로 구분한다. 부가통신의 경우 직접정보통신시설 사업자, 쇼핑몰, 유선방송으로 구분이 된다. 직접정보통신 시설 사업자의 경우 서버호스팅, 스토리지호스팅, 코로케이션, 네트워크 제공서비스 등 이며, 쇼핑몰의 경우 인터넷접속 기반서비스, 카드조회, 지불중계, 컴퓨터 예약 서비스, 전자문서 교환, 네트워크 제공서비스, 인터넷 포털 서비스, 인터넷 전자상거래, 신문/방송, 음악/교육, 인터넷 게임, 기타 인터넷 정보제공 서비

스를 포함하고 있다. 유선방송의 경우는 cable-So 등을 포함하고 있다[2].

2.2 국내 정보보호전공 교육과정

IT기술의 발전에 따른 정보보호 인력에 대한 필요성이 많이 대두되고 있어, 많은 대학에서 정보보호 관련 전공을 개설하여 운영하고 있다. 정보보호학과 인력 현황에 따르면 2013년 12월 기준 한국인터넷진흥원 2012 국내 지식정보보안산업 실태조사 자료를 기반으로 살펴보면, 20여개 대학에서 정보보호관련 전공을 운영하고 있다. 정보보호관련 학과별 공통기반 기술을 위한 교육을 위한 교과과목의 편성을 살펴보면, 단순한 IT기술 기반의 정보보호교육과 함께 시대적 흐름에 맞도록 융합관련 분야의 정보보호 관련 과목을 개설하고 있다. 경일대 사이버보안학의 경우 사이버범죄학, 고려사이버대의 경우 정보관리보안학의 범죄학개론과 광주대 사이버보안학의 경우 경찰학개론과 경찰윤리, 경찰보안관리와 보안영어 등을 개설하여 단순한 정보보안의 분야에만 국한하지 않고, 범죄학과 심리학 등 다양한 학문과의 연계를 위한 교육 과정을 운영하고 있다[2].

정보보호관리체계에 대한 교과과정에 대한 반영이 많이 없지만, 많은 정보보호 전공에서 관련 교과 과정을 운영하고자 하는 계획들을 많이 수립하고 있다. 본 연구자가 있는 백석대학교의 경우 2015학년 정보보호전공의 경우 정보보호관리체계 과목을 신설하여 실무에서 적용할 수 있는 정보보호관리 방법에 대한 내용을 진행 예정이다. 많은 기업에서 ISMS 인증을 위하여 조직을 개편하고, 그에 맞는 인증을 위해서 정보보호 인력의 필요성이 대두되고 있다. 그에 따른 실무적인 교육과정의 개설이 필요한 시점이다.

3. 융합관리 방안

관련연구에서 살펴 본 것처럼 ISMS에 대한 법적인 제도를 통하여 많은 곳에서 ISMS인증을 위한 노력을 기울이고 있다. 이에 적합합 교육과정의 개설을 통하여 정보보호관리체계가 좀더 효율적으로 적용될 수 있도록 대학의 교육과정의 설계가 필요해 보인다. 관련연구 2.2에서 살펴본 것처럼 많은 정보보호 전공에서 단순한 정보보안의 기술적인 부분뿐만이 아닌 융합적 학문으로서 범위를 확장해가고 있으며 그에 맞는 정보보호 교육을 진행 예정이다. 본 연구에서는 이러한 융합적 교육 과정을 위한 교육 과정의 설계와 실제로 대학과정에서 참여하고 있는 정보보호 동아리에 대한 융합관리 방안을 제안하여 정보보호 인력의 양성을 좀 더 효율화하고자 한다.

3.1 융합관리를 통한 정보보호 동아리 운영

IT의 발전에 따라 많은 사람들이 스마트 기기를 통한 다양한 서비스를 이용하고 있다. 그에 따른 다양한 보안 위협요소도 도출되고 있다. 따라서 보안이나 해킹관련 관심도 상당히 대두되고 있다. 특히 청소년들과 대학생들 사이에서도 정보보안에 대한 관심은 상당히 높아지고 있다. 전국의 대학에서도 정보보호 관련 동아리가 많이 생겨나고 있다. 따라서 한국인터넷진흥원에서는 전국 대학정보보호동아리 연학회(KUCIS:Korea University Clubs of Information Security)를 운영하고 있다. 매년 40여개 정보보호동아리르 선발하여 정보보호 교육, 세미나를 통하여 전문기술을 함양하도록 지원하고 있다. 또한 동아리간 기술 교류 및 경진을 통한 기량 향상을 위해 대항한 방법을 제공해주고 있다. 아울러 산.학연계를 통한 현장체험 및 지역봉사활동 등의 내용으로 정보보호 동아리를 관리하고 있다. 많은 정보보호 동아리가 지도교수의 지도 내지는 선배들의 지도를 통하여 활성화가

〈Table 1〉 evaluation of KUCIS

	Items
Configuration	① Configuration of Information security club ② License of information security (3years) - award of information security & information technology ③ employee (3years)
record of last year	① Conference of iofomation security - seminar, workshop of information security & technology ② research & project of information security & technology - paper, patent, book
plan	① plan of project

되어 가고 있다. 정보보호동아리 평가항목을 인용하여 각 활동 방안에 대하여 제안하고자 한다.

– 동아리 구성자격

동아리 구성자격에서는 최소 10인 이상을 권장하고 있다. 정보보호 관련전공자나 정보통신 관련 전공자들과 함께 융합의 필요성을 위하여 경찰학이나 범죄학과 관련된 학생들의 구성원도 필요하다. 융합에 대한 학문적 성과를 위하여 다양한 구성원으로 구성이 필요하다. 대부분은 정보보안에 대한 관심과 열정이 있는 사람들 위주로 편성이 되어야 한다. 최근 3년간 동아리 회원에 대한 정보보호 관련 수상경력 및 자격증 보유율의 평가를 위해서는 동아리 차원에서 자격증관련 세미나와 스터디 그룹을 통하여 동아리 회원들의 기본적인 정보보안 역량을 강화시켜야 한다. KUCIS에서 권장하고 있는 정보보안기사, CISSP, CCNA 등 네트워크나 정보보호 관련 자격이 필요하다. 학생들 자체적인 세미나의 진행이 어려울 수 있기 때문에 지도교수나 전공 관련 교수의 도움을 통하여 진행이 필요하다.

최근 3년간 동아리 회원의 취업에 대한 내용을 위해서는 구성원들이 가능하면 정보보안 업체로의 취업과 정보통신 분야로의 취업을 통해서 관련 역량을 확인할 수 있도록 해야 한다. 대부분 정보보호에 관심을 가지고 있는 사람들로서 대부분 정보보호 관련 업체로의 취업을 준비하고 있다.

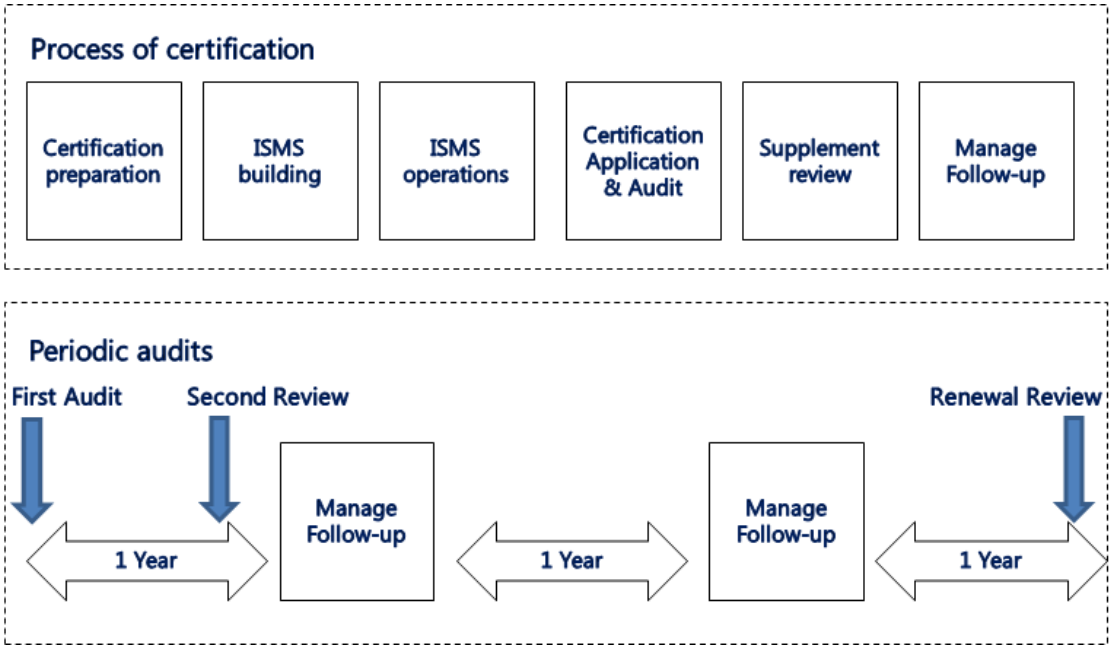
– 전년도 활동실적

정보보호관련 대내외 학술활동의 경우 세미나와 워크숍 개최, 발표 시연 등의 실적이 필요하다. 이러한 실적을 위해서는 동아리 구성원이나 지도교수의 지도아래 학교의 지원을 통해서 준비하는 것이 필요하다. 특히 정보보호 전공내에서는 관련 전공 세미나와 외부 전문가 초청 세미나 등을 많이 진행하고 있기 때문에 관련 세미나와 함께 병행하여 활동하는 것이 필요하다.

정보보호과련 연구활동에서는 프로젝트에 대한 진행을 통해서 정보보호 관련 이슈를 도출하고 도출된 문제를 해결할 수 있는 방안들을 통해 해결점을 찾는 프로젝트를 진행하는 것이 필요하다. 각 대학별로 소규모 단위의 프로젝트와 다양한 경진대회를 진행하고 있으므로 그러한 대회에 참여하여 실적을 통하여 정보보호 관련 프로젝트를 참여하는 것이 필요하다.

3.2 정보보호관리체계 교과 운영

정보보호관리체계 교과목을 운영시 고려해야할 부분



[Fig. 1] Process of Certification & Periodic audits

은 실제 정보보호 담당자로서의 역할을 충실히 수행할 수 있는 역량을 학습하도록 강의 내용은 인증프로세스 이해, 인증 준비단계, ISMS 구축단계, ISMS 운영 단계, 인증신청 및 심사단계, 사후단계에 준비 방법을 이해해야한다.

- ISMS 인증 프로세스 이해

인증신청기관 입장에서의 인증 프로세스를 이해해야 한다. 각 단계별로 진행되는 내용에 대한 전반적인 내용의 소개가 필요하다. 그림 1와 같이 인증 절차는 인증준비단계, ISMS구축, ISMS 운영, 인증신청 및 심사단계, 심사결과 보완조치 단계, 사후관리 단계로 구성이 된다. 아울러 인증 심사주기는 최초심사후 1년이 경과되어 사후심사가 2년간 진행이 되고 향후에는 갱신 심사를 받아야 한다. 교과과정에서는 최초심사 준비에 대한 세부적인 내용을 학습해야 한다. 최초심사의 경우 대부분 인증 신청 기관에서 준비에 상당한 부분이 미흡하므로 관련 절차에 따른 실적과 정보보호 관리체계를 운영하여야 한다.

- 인증 준비단계

인증준비단계는 실제적으로 심사를 준비하기 위한 실제적인 부분으로서 관련 구비 서류들을 모두 준비해야한다. 정보보호컨설턴트, 경영진, 추진팀을 구성하여 체계적인 준비를 해야 한다. 정보보호관리과정 5개의 12개 통제항목과 정보보호대책 13개의 92개 통제항목을 준비해야한다. 이부분에 대한 수업 진행시 세부적인 각 분야에 대한 소개와 통제항목에 대한 자세한 내용들을 살펴보아야 한다. 세부통제항목 별로 진행헤 대한 부분은 정보보호 교과 과정을 통해서 학습했던 내용들을 대부분 알고 있어야만 가능하므로 실무적인 운영방법 등에 대한 자세한 내용들을 학습해야 한다. 심사 인증 범위는 전 조직을 대상으로 정보보호관리체계를 수립하도록 하는 것을 권고하고 있다. 인증 범위가 아닌 부분을 통해서 취약점의 발견이 되어 심각한 문제를 초래할 수 있기 때문에 가능한 많은 범위를 설정하는 것이 필요하다.

- ISMS 구축단계

구축단계에서는 정보보호정책을 수립하고, 관리체계의 범위를 설정하며, 위험관리, 구현, 사후관리를 통한 정보보호 관리체계 관리 과정을 수립해야 한다. 구축시 고려해야할 부분은 정보보호관리체계 구축에 대한 문서화 과정이 필요하다. 관리적, 기술적, 물리적인 정보보호 관리체계를 구축해야 한다. 관리적 관점에서는 경영진의 결정을 반영한 상위 정보보호 규정 수립시 해당 기록을 유지하고, 기술적 관점에서는 침입차단시스템과 침입탐지시스템 등의 최소한의 보안 장비에 대한 도입이 필요하다. 물리적 관점에서는 보호구역 설정 후 해당 구역에 대한 통제권한의 할당이 필요하다.

- ISMS 운영 단계

운영단계에서는 앞에서 준비한 내용을 기반으로 실제적으로 운영하여 정보보호 관리체계가 제대로 적용이 되고 있는지를 확인하는 과정이다. 각 통제분야에 대한 내용을 확인후에 실제 최소 3개월 관리 운영을 해야 한다. 인증에 필요한 기본적인 문서들은 다음과 같다. 정보보호정책서, 위험분석.평가보고서, 정보보호계획서, 정보보호대책명세서, 정보보호관리체계 내부감사결과보고서, 주요정보통신설비 목록과 시스템 구성도, 정보보호관리체계와 관련이 있는 주요 문서 목록으로 각종 지침서가 필요하다.

- 인증신청 및 심사단계

인증신청 및 심사단계는 실제적인 인증 준비가 끝난 상황에서 인증 신청을 진행한다. 인증신청 공문을 심사기관에 접수한다. 인증기관에서는 인증심사 계획을 통보하고 심사위원을 선정하여 심사기간에 심사를 실시한다. 심사가 완료되면 인증신청기관에서는 보완조치를 통하여 내역서를 인증기관에 제출하면 보완조치 여부를 확인 후 인증서를 발급하게 된다.

- 사후단계

사후관리에서는 정보보호관리체계의 운영과정에서 결함사항이 발생여부를 점검하고, 인증서 사용 및 홍보에 있어서 인증범위를 적절하게 활용하고 있는지 여부를 점검한다. 지난 심사의 결함보고서를 통하여 보안의 위험이 감소되었는지 확인한다.

4. 결론

본 논문에서는 중요 정보자산을 안전하게 보호하기 위한 과정으로 실시되고 있는 정보보호관리체계와 IT의 발전으로 인한 정보보호의 중요성의 대두로 인하여 많은

대학들이 정보보호관련 전공을 개설에 따른 융합형 관리 모델의 필요성에 대해서 살펴보았다. 정보보호관련 전공에서도 정보보호관리체계의 효율적인 실무 역량을 강화하기 위하여 교과과정으로 운영이 필요하다. 따라서 본 연구를 통해서 정보보호 관리체계에 대한 정확한 이해를 위한 관련연구와 절차적 방법을 살펴보았다. 정보보호 전공의 학생들이 어떻게 정보보호관리체계를 학습하여 실무에서의 역량을 강화할 지에 대한 내용을 살펴보고, 이러한 정보보호 관리체계를 통하여 정보보호에 관심 있는 학생들과 정보보호 동아리의 학생들을 효율적으로 관리하고 있는 방안을 제안하여, 국내 정보보호 인력의 확산을 통한 정보보호 전문인력을 양성하여 중요 정보자산을 안전하게 지킬 수 있는 방안을 제안하였다.

References

[1] SangSoo Jang, BongNam Noh, SangJoon Lee, “The Effects of the Operation of an Information Security Management System on the Performance of Information Security“, Journal of Korea Institute of Information Science and Engineers”, Vol. 40, No. 1, pp. 58-69, 2013.

[2] Young-Sik Bae, “A study of Effect of Information Security Management System [ISMS] Certification on Organization Performance”, Journal of the Kroea Academia-Industrial Cooperation Society, Vol. 13, No. 9. pp. 4224-4233, 2012.

[3] Jinkeun Hong, “Analysis of Academic Curriculum of Information Security Major in Domestic University and Convergence Education Policy”, Journal of Digital Convergence, Vol. 12, No. 1, pp. 599-605, 2014.

[4] The National Assembly of the Republic of Korea, Act on Promotion of Information and Communications Network Utilization and Information Protection, ect, 2008.

[5] ISO/IEC27002, Information technology - Security techniques - Code of practice for information security management, 2005.

[6] Implementing the ISO/IEC 27001 Information Security Management System Standard, ISACA, 2007.

[7] Information Security Governance Guidance for Information Security Managers, ITGI, 2008.

[8] Jody Westby and Julia Allen, Governing for Enterprise Security(GES) Implementation Guide, CMU/SEI, 2007.

[9] The Graduate School of Konkuk University, A study of a Model for Financial Information Security on Applies Information Security Management, 2010.

[10] KCC, KISA, Information Security Management System (ISMS) certification best casebook, 2010

[11] KISA, Improvement of the Information Security Management System Certification Scheme by Incorporating Information Security Governance Concepts, 2009.

저자소개

이 근 호(Keun-Ho Lee) **[종신회원]**

- 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호