사물인터넷 환경에서 ESG기반 정보보호 교육 모델에 관한 연구

이근호*
백석대학교 컴퓨터공학부 교수

A Study on ESG-based Information Security Education Model in IoT Environment

Keun-Ho Lee*
Professor, Div. of Computer Engineering, BaekSeok University

요 약 사물인터넷 환경에서 ESG를 기반으로 지속가능성을 위한 다양한 노력이 진행되고 있다. ESG는 환경뿐만 아니라 사람과 지역 사회에 영향을 미치는 광범위한 문제를 포함하여 오늘날 비즈니스 운영 및 전략에서 중요하다. 특히 정보 및 데이터 보안 분야의 정보보호 교육은 ESG의 사회적 영역에 속한다. 이는 중요한 정보, 사용자 개인정보보호 및 디지털 권한 보호가 조직의 사회적 책임의 중요한 부분임을 보여주고 있다. 사물인터넷 환경에서 ESG를 기반으로 보안을 강화하기 위해서는 사물인터넷 환경의 특성을 고려한 교육 과정이 필요하다. 본 논문에서는 사물인터넷 환경에서의 ESG 기반의 정보보호 교육모델을 제안하였다. 제안된 교육모델은 사물인터넷 환경의 지속가능성을 위한 ESG를 위한 정보보호 교육 과정으로 설계하였다. 제안된 교육과정 모델을 3개 기관에서 진행해보고 교육 참여자의 설문을 통한 교육과정의 효율성을 확인하였다.

주제어 : 사물인터넷, 정보보호, 교육모델, 보안 위협, 지속가능성

Abstract In the IoT environment, various efforts for sustainability are underway based on ESG. ESG is important in today's business operations and strategies, covering a wide range of issues affecting people and communities as well as the environment. In particular, information security education in the field of information and data security belongs to the social domain of ESG. This shows that protecting sensitive information, user privacy, and digital rights is an important part of an organization's social responsibility. In order to strengthen security based on ESG in the Internet of Things environment, a training course that takes into account the characteristics of the Internet of Things environment is needed. In this paper, we proposed an ESG-based information security education model in the Internet of Things environment. The proposed education model was designed as an information security education course for ESG for sustainability of the Internet of Things environment. The proposed curriculum model was implemented at three institutions and the effectiveness of the curriculum was confirmed through a survey of training participants.

Key Words : IoT, Information Security, Education Model, Security Threats, Sustainability

*이 논문은 2023학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2023년 5월 14일 수정일 2023년 10월 12일 심사완료일 2023년 10월 14일

1. 서론

사물인터넷은 사물과 사물 간의 통신을 통해 정보를 교환하고 제어하는 기술이다. 사물인터넷은 다양한 산업 분야에서 활용되고 있으며, 그 규모는 빠르게 증가하고 있다. ESG는 환경(Environmental), 사회(Social), 지배구조(Governance)의 약자로, 기업의 지속가능성을 위한 비재무적 요소를 의미한다. ESG는 기업의 경영성과, 투자성과, 사회적 영향력 등에 중요한 영향을 미치고 있다. ESG는 기업의 지속가능성을 위한 핵심 요소이고, 기업의 지속가능성은 기업의 장기적인 성장과 발전을 위한 필수 조건이다. ESG 경영을 통해 기업은 환경, 사회, 지배구조 측면에서 긍정적인 영향을 미칠 수 있다. ESG는 기업의 경영성과에도 긍정적인 영향을 주고 있다. ESG 경영을 통해 기업은 정부 규제에 대한 부담을 줄이고, 고객과 투자자의 신뢰를 얻을 수 있다. 또한, ESG 경영은 자원 효율성 향상, 비용 절감, 생산성 향상 등에 도움이 된다. ESG는 최근 전 세계적으로 중요성이 커지고 있으며, 기업, 투자자, 정부 등 다양한 이해 관계자들이 ESG 경영을 요구하고 있다. 이에 따라 ESG 관련 규제와 인증, 투자 등이 확대되고 있다. ESG는 기업의 경쟁력과 지속가능성을 위한 필수 요소이다. 기업은 ESG 경영을 통해 경영성과, 사회적 영향력 등을 향상시킬 수 있다. ESG는 사회적 영향력에도 중요한 영향을 미친다. ESG 경영을 통해 기업은 환경 보호, 사회 공헌, 사회적 책임 등에 기여할 수 있다. 이는 기업의 사회적 이미지를 높이고, 사회적 가치를 창출하는 데 도움이 된다. 사물인터넷의 확산으로 인해 기업의 ESG 경영에 새로운 도전과 기회가 생겨나고 있다. 사물인터넷은 기업의 생산성 향상, 비용 절감, 효율성 개선 등 다양한 측면에서 ESG 경영에 기여할 수 있지만, 한편으로는 새로운 보안 위협을 야기한다. 사물인터넷 환경에서 발생하는 보안 사고는 기업의 ESG 경영에 부정적인 영향을 미칠 수 있다. 예를 들어, 사물인터넷 장비를 통해 개인정보가 유출되면 기업의 이미지와 신뢰도가 하락할 수 있으며, 사물인터넷 장비가 제어를 잃으면 기업의 생산성과 안전에 영향을 미칠 수 있다. 따라서 사물인터넷 환경에서의 침해사고를 예방하고 대응하기 위한 노력은 ESG 경영을 위한 필수 요소이다. 사물인터넷 환경에서의 ESG 기반 침해사고대응 교육과정 모델은 사물인터넷 환경의 보안을 강화하고, 사물인터넷의 침해 사고를 예방하는 데 도움이 될 수 있다. 이 교육과정 모델은 사물인터넷 환경의 특성을 고려하여 한다. 사물인터넷 환경의 보안 위협, 보안사고의 종류, 침해사고대응 절차 등을 교육한다. 이를 통해 사물인터넷 환경의 보안 인식을 높이고, 사물인터넷 보안의 중요성에 대한 인식을 높일 수 있다. 사물인터넷 보안 인식 향상은 기업의 ESG 경영에 다음과 같은 긍정적인 영향을 미칠 수 있다. 환경적 측면에서는 사물인터넷 장비의 보안을 강화하면 에너지 효율성이 향상되고, 환경오염이 감소할 수 있다. 사회적 측면에서는 사물인터넷 장비의 보안을 강화하면 개인 정보 유출을 방지하고, 소비자의 안전을 보호할 수 있다. 지배구조 측면에서는 사물인터넷 장비의 보안을 강화하면 기업의 재무적 손실을 방지하고, 투자자의 신뢰를 높일 수 있다. 사물인터넷 환경에서의 정보보호 교육과정 모델은 기업의 ESG 경영을 위한 중요한 수단이 될 수 있다. 기업은 이 교육과정 모델을 활용하여 사물인터넷 환경의 보안을 강화하고, ESG 경영을 실천할 수 있다[1-6].

사물인터넷 환경에서의 정보보호 교육과정 모델을 ESG 경영에 활용할 수 있다. 교육과정 대상자를 확대하여 사물인터넷 보안 인식을 전사적으로 확산하고, 사물인터넷 환경에서의 보안 사고는 IT 보안 전문가뿐만 아니라, 사물인터넷 장비를 개발 및 제조하는 기업의 개발자, 사물인터넷 장비를 사용하는 기업의 임직원 등 다양한 이해관계자에 의해 발생할 수 있다. 따라서 교육과정 대상자를 확대하여 사물인터넷 보안 인식을 전사적으로 확산하는 것이 중요하다. 교육과정 내용을 ESG 경영과 연계하여 사물인터넷 환경에서의 보안 위협을 ESG 관점에서 이해하고, 사물인터넷 환경에서의 보안 위협은 기업의 ESG 경영에 부정적인 영향을 미칠 수 있다. 따라서 교육과정 내용을 ESG 경영과 연계하여 사물인터넷 환경에서의 보안 위협을 ESG 관점에서 이해하는 것이 중요하다. 교육과정 평가 결과를 활용하여 사물인터넷 환경의 보안을 개선한다. 교육과정 평가 결과를 활용하여 사물인터넷 환경의 보안을 개선하는 노력이 필요하다. 예를 들어, 교육 내용이 실제 업무에 적용될 수 있는지, 교육받은 내용을 바탕으로 사물인터넷 환경의 보안을 개선할 수 있는지에 대한 평가 결과를 바탕으로 교육과정과 실무를 연계하는 노력이 필요하다. 사물인터넷 환경에서의 정보보호 교육과정 모델은 기업의 ESG 경영을 위한 중요한 수단이 될 수 있다. 기업은 이 교육과정 모델을 활용하여 사물인터넷 환경의 보안을 강화하고, ESG 경영을 실천할 수 있다[7-15].

본 연구에서는 ESG 관련 연구를 통하여 기존에 제안하고 있는 사물인터넷 환경에서의 정보보호 교육과정에

대한 내용을 살펴보고, 제안한 교육 내용에서 좀 더 ESG 맞춤형 교육과정에 대한 모델을 제안하고자 한다. FGI를 통한 ESG 관련 정보보호 교육과정 모델을 위하여 3개 기관을 통하여 사례중심으로 교육을 진행해보고 각 기관의 주요 요구사항을 접목한 교육과정 모델을 개선 하고자 한다. 본 교육과정 모델을 위하여 기존에 진행했던 블록체인 기반의 인재양성 사업과 침해사고 대응 교육과정 개발과 적용 경험을 바탕으로 정보보호 교육 모델을 제안하고자 한다.

2. 관련 연구

2.1 ESG

ESG는 환경(Environmental), 사회(Social), 지배구조(Governance)의 약자로, 기업의 지속가능성을 위한 비재무적 요소를 의미한다. ESG는 최근 기업의 경영성과와 투자성과에 중요한 영향을 미치고 있으며, 이에 따라 ESG 관련 연구도 활발히 진행되고 있다. ESG 관련 연구는 크게 두 가지 관점에서 연구되고 있습니다. 첫 번째는 ESG가 기업의 경영성과에 미치는 영향에 대한 연구이다. 이 연구는 ESG 경영이 기업의 수익성, 주가수익률, 기업가치 등에 미치는 영향을 분석한다. 두 번째는 ESG가 투자성과에 미치는 영향에 대한 연구이다. 이 연구는 ESG 투자가 투자자의 수익률, 위험, 성과 리스크 등에 미치는 영향을 분석한다. ESG 중 환경 요소인 기업의 환경성과가 기업의 경영성과에 미치는 영향을 분석한 연구로서 연구 결과, 기업의 환경성과가 높을수록 기업의 수익성, 주가수익률, 기업가치 등이 높게 나타나는 것으로 나타났다. 환경성과가 높은 기업은 정부 규제에 대한 부담이 적고, 사회적 이미지가 좋기 때문에 고객과 투자자로부터 더 많은 신뢰를 얻을 수 있다. 환경성과가 높은 기업은 자원 효율성이 높고, 환경 사고의 위험이 적기 때문에 비용 절감과 생산성 향상에 도움이 된다[1-6].

2.2 사물인터넷 관련 정보보호 교육과정

사물인터넷 관련 정보보호 교육과정의 목표는 사물인터넷의 개념과 특징을 이해하고, 사물인터넷의 보안 위협과 보안사고를 예방하고 대응할 수 있는 능력을 배양한다.

교육대상은 사물인터넷 관련 업무를 담당하는 IT 인력, 사물인터넷 관련 제품과 서비스를 개발하는 개발자, 사물인터넷 관련 시스템을 운영하는 관리자로 하고 일반적인 사물인터넷에 관심이 있는 자로 한다.

교육내용은 사물인터넷의 개념과 특징, 사물인터넷의 보안 위협, 사물인터넷 침해사고의 예방과 대응으로 구성한다. 교육방법은 강의, 실습, 실기 교육 등을 병행하여 진행한다. 교육평가는 교육 내용에 대한 이해도 평가, 교육 후 실습 능력 평가 등을 실시한다. 교육내용 세부설명으로는 사물인터넷의 개념과 특징, 사물인터넷의 정의, 사물인터넷의 구성요소, 사물인터넷의 특징, 사물인터넷의 보안 위협, 물리적 공격, 네트워크 공격, 소프트웨어 공격, 인적 실수로 구성한다. 사물인터넷 침해사고의 예방과 대응으로는 사물인터넷 침해사고의 정의, 사물인터넷 침해사고의 예방, 사물인터넷 침해사고의 대응으로 한다. 교육과정 적용은 사물인터넷 관련 업무를 담당하는 모든 인력에게 적합하다. 교육 내용에 대한 이해도 평가는 교육 후 설문조사 등을 통해 실시할 수 있다. 위의 교육과정은 기업, 대학, 연구소 등에서 활용할 수 있다. 기업은 사물인터넷 관련 업무를 담당하는 인력을 양성하기 위해 이 교육과정을 활용할 수 있다. 대학은 사물인터넷 관련 학과에서 이 교육과정을 활용하여 학생들의 사물인터넷 보안 역량을 강화할 수 있다. 연구소는 사물인터넷 보안 기술을 개발하기 위해 이 교육과정을 활용하여 연구 인력을 양성할 수 있습니다[7-12].

2.3 정보보호 관련 교육과정

정보보호 전공 교육과정은 정보보호 전문가를 양성하기 위한 교육과정이다. 정보보호 전공 교육과정은 정보보호의 기본 개념, 정보보호 기술, 정보보호 정책, 정보보호 법률 등을 교육한다. 또한, 정보보호 전공 교육과정은 정보보호 실무를 경험할 수 있는 기회를 제공한다. 정보보호 전공 교육과정은 일반적으로 다음과 같은 과목을 포함합니다. 컴퓨터 네트워크와 네트워크 보안, 운영 체제와 시스템 보안, 데이터베이스, 프로그래밍, 보안 리스크 관리, 보안 침투 테스트, 보안 감사, 보안 컨설팅, 보안 연구, 보안관재, 어플리케이션 보안 등의 정보보안 관련 기초부터 심화 응용에 이르는 다양한 교육과정에 대한 운영이 진행되고 있다. 정보보호 전공 교육과정은 정보보호 전문가가 되기 위해 필요한 지식과 기술을 제공하고 있으며, 각 교육기관 마다 중점 분야 기반으로 교육과정이 설계되고 교육이 이루어진다[3].

3. ESG기반 정보보호 교육과정 모델 설계

[표1] ESG기반 정보보호 교육과정 모델은 충청남도 중소기업 및 대학생의 정보보호 역량 강화를 목적으로 하였다. 이 프로그램은 필수 정보보안 관행에 대해 참가자를 교육하고, 잠재적인 위험과 위협에 대한 인식을 높이며, 참여 조직의 전반적인 사이버 보안 태세를 강화하기 위한 실용적인 전략을 제공하는 것을 목표로 하고 있다. 전체적인 주제로는 크게 정보보안 기초 교육, 전자정부, 정보보안 실무, 보안관리 분야로 구분하였다. 정보보안 기초 교육과정에서는 4차 산업혁명 시대의 정보보안, 정보보호 개념 이해 및 정립, 정보보안 기술적 이해, 정보보호 및 개인정보보호 관리체계(ISMS-P) 이해로 구성하였다. 전자정부에서는 전자정부 정보보호 거버넌스의 이해 및 정책 개발·수립, 전자정부 IT 인프라의 이해와 보안, 전자정부 네트워크 보안 실무, 전자정부 소프트웨어 플랫폼 보안 실무, 전자정부 내부 보안감사 실무로 구성하도록 하였다. 정보보안 실무에서는 랜섬웨어 대응, 정보시스템 위험진단 기술실무, 클라우드 보안 구축 실무로 구성하였다. 보안 관리에서는 물리보안과 접근통제, 정보시스템 보안성 확보를 위한 위험기반 테스팅, 침해사고 대응을 위한 네트워크 데이터분석 및 포렌식, 웹 해킹 보안 및 취약점 분석으로 구성하였다.

제안 모델에 대한 사례는 충청남도에 위치한 중소기업의 직원 및 의사 결정자, IT 직원, 관리자, 임원 및 정보보안을 담당자, 데이터 처리 담당하는 기타 직원, 대학의 경영학과 학생 및 인공지능학과 학생들 대상으로 사례를 적용해 보았다. 3개 기관에 대한 교육과정 모델의 기본 내용은 정보보안 인식 향상을 위하여 중소기업의 정보보안 인식 수준을 향상하고, 정보 보안과 관련된 위험, 위협 및 취약성에 대한 더 나은 이해 촉진을 내용으로 하고 있다. 정보보호 능력 강화를 통하여 정보보호 능력을 강화하는 데 필요한 지식, 기술 및 도구를 중소기업에 제공하고자 한다. 보안 의식 문화 확산을 위하여 조직의 모든 직원이 정보 보안을 우선시 가치 있게 여기는 환경을 조성하고자 하였다. 적용했던 교육과정 내용은 사례로 보는 ESG환경과 보안 경영, 블록체인과 디지털화폐, 경영에 필요한 산업보안, 랜섬웨어와 정보보호 기술, 침해사고 대응을 위한 네트워크 데이터 분석 및 포렌식, 웹해킹 보안 및 침해사고 대응을 교육하였다.

〈Table1〉 Basic information security professional training

Division	Target	Subject
Information Security Basic Training	All	Information security in the era of the 4th Industrial Revolution
		Understanding and establishing information security concepts
		Information security technical understanding
		Understanding Information Security and Personal Information Protection Management System
E-government	Government Official Small and Medium-sized Business Employee College Student	Understanding and policy development and establishment of e-government information security governance
		Understanding and security of e-government IT infrastructure
		E-government network security practice
		E-government software platform security practice
		Electronic government internal security audit practice
Information Security Practice	Small and medium-sized business employee Information security practitioner College student	Ransomware response
		Information system risk diagnosis technology practice
		Cloud security implementation practice
Security Management	All	Physical security and system access control
		Risk-based testing to ensure information system security
		Network data analysis and forensics to respond to infringement incidents
		Web hacking security and vulnerability analysis

4. ESG기반 정보보호 교육과정 모델 분석

[표2] Focus Group Interview을 통한 3개 교육기관을 대상으로 교육 내용을 진행하고, 각 설문을 통하여 만족도를 조사하였다.

FGI 진행 절차는 FGI 대상자 선정, 설문지 개발, 진행, 결과 분석으로 구성한다. 세부 내용은 다음과 같이 진행한다. FGI 대상자 선정은 사물인터넷 관련 교육 과정을 수강한 경험이 있는 학생과 기업 관계자 등으로 구성하였다. 또한, 교육과정에 대한 다양한 의견을 얻기 위해 다양한 배경의 사람들을 선정하였다. IT관련 전공과 경영관련 전공으로 구분하여 설문을 진행하였다. FGI 설문지는 사물인터넷에서 ESG 관련 정보보호 교육 과정에 대한 교육 과정의 만족도, 교육 과정의 장점과 단점, 교육 과정 개선에 대한 의견 내용을 포함하도록 개발하였다. FGI 진행은 특강을 마치고 나서 ESG관련 교육과정에 대한 설문으로 진행하여 만족도를 확인하여 교육과정에 대한 내용을 확인하도록 하였다. 위와 같은 방법으로 FGI를 진행하면 3개 교육기관의 사물인터넷 관련 ESG 기반의 정보보호 교육 과정에 대한 다양한 의견을 수렴하고, 이를 바탕으로 향후 교육 과정을 개선하도록 하고자 한다. 전체적인 만족도 조사에서는 교육과정에 대한 만족도가 5점 만점 기준으로 4.71로 상당히 ESG 기반 정보보호 교육과정에 대한 만족도를 나타내고 있다. 만족도 조사 내용은 교육내용, 강사, 교육환경 등 교육의 전반적인 사항에 대한 만족도와 교육 내용의 유익성, 교육 참여 목적, 강사의 전문성 등을 만족도로 조사하였다. 경영관련 학과에서의 만족도가 약간 떨어지는 부분은 기술관련 내용에 대한 어려움이 약간 있었던 것으로 판단이 된다. 하지만 ESG경영에서 정보보호가 차지하는 의미를 이해하는 과정으로 학습에 대한 만족감을 나타내고 있다.

5. 결론

ESG는 기업의 경영성과에도 긍정적인 영향을 미치고 있다. ESG 경영에서 정보보호 교육에 대한 교육과정을 설계하여 효율화를 위한 노력이 필요한 시점이다. ESG 경영은 자원 효율성 향상, 비용 절감, 생산성 향상 등에 도움이 된다. ESG는 최근 전 세계적으로 중요성이 커지고 있으며, 기업, 투자자, 정부 등 다양한 이해 관계자들이 ESG 경영을 요구하고 있다. 사물인터넷 기술은 빠르게 발전하고 있으며, 이데 대한 ESG 경영과 관련된 부분으로의 발전이 필요하다. 본 연구에서는 사물인터넷 환경에서 ESG기반으로 정보보호를 위한 교육과정 모델을 제안하였다. 향후 연구에서는 제안된 교육과정 모델의 교육 효과를 검증하고, 교육과정 모델을 지속적으로 체계화하고, ESG 발전을 위한 추가적인 교육 모델제안이 필요하다.

〈Table2〉 Survey results for each course

Target	Number	Total satisfaction	Satisfaction1	Satisfaction2	Satisfaction3	Satisfaction4	Lecture Content
H University MOT Course	116	4.75	4.8	4.74	4.74	4.73	Network data analysis and forensics to respond to infringement incidents
S University, Department of Business Administration	45	4.77	4.78	4.79	4.81	4.66	Blockchain and digital currency
N University Department of Business Administration	68	4.53	4.51	4.53	4.57	4.5	ESG environment and security management
		4.61	4.55	4.58	4.67	4.59	Industrial security required for management
N University Department of Artificial Intelligence	112	4.8	4.7	4.8	4.85	4.8	Ransomware and information protection technology
		4.77	4.78	4.79	4.81	4.66	Response to web hacking and infringement incidents
Sum	341	4.71	4.69	4.71	4.74	4.66	

REFERENCES

[1] Wagner,M. and Schaltegger,S., "The Impact of Corporate Environmental Performance on Financial Performance: Evidence from Panel Data", Journal of Business Ethics, Vol.49, No.1, pp.35-51, 2004.

[2] H.W.Kim. "Intrusion response methods in the Internet of Things (IoT) environment". Journal of the Korea Institute of Information Security and Cryptology, Vol.28, No.4, 739-749, 2018.

[3] K.H.Lee, "A Study on the Infringement Incident Response Curriculum Model in IoT Environment", Journal of Internet of Things and Convergence, Vol.9, No.3, pp.55-60, 2023.

[4] J.H.Lee, "Security threats and response methods in the Internet of Things (IoT) environment". Journal of the Korea Institute of Information Security and Cryptology, Vol.27, No.4, 697-706. 2017.

[5] "The Internet of Things (IoT): A Security Perspective", by Andrew S. Tanenbaum and Maarten van Steen, in "The New Internet", edited by Andrew S. Tanenbaum and Maarten van Steen, 2010.

[6] Y.M.Park, "Training program model for intrusion response in the Internet of Things (IoT) environment". Journal of the Korea Institute of Information Security and Cryptology, Vol.29, No.4, 795-804. 2019.

[7] Ministry of Science and ICT, number of cyber infringement incidents by year (2022.11)

[8] "Security for the Internet of Things", by David A. Wheeler and Richard E. Smith, 2016.

[9] K.H.Lee, "A Study on a Project-based Blockchain Web Developer Education Model Customized for Companies", Journal of Internet of Things and Convergence, Vol.8, No.4, pp.77-83, 2022.

[10] Korea Internet & Security Agency, a study on estimating the economic and social costs of cyber infringement accidents(2021.12)

[11] "Security in the Internet of Things", by Richard E. Smith, in "The Internet of Things: A Systems Perspective", edited by Richard E. Smith, 2015.

[12] N. Asokan, S. Sadeh, and A. Sadeh, "A Survey on Security Issues in the Internet of Things", Proceedings of the 2009 IEEE Security and Privacy Symposium, Vol.23, No.5, pp.71-82, 2009.

[13] M. Conti, S. Dehghantanha, S. Jajodia, and H. Hu,, "Security and Privacy in the Internet of Things", Computer, Vol.49, No.2, pp.84-91, 2016.

[14] S. M. Rahman, M. A. Khan, and S. K. Das, "A Survey on Security and Privacy Challenges in the Internet of Things", IEEE Access, Vol.6, pp.17684-17707, 2018.

[15] J.Park, H.Lee and M.Seo, "The 4th Industrial Revolution and the Future of Advertising and Public Relations Curriculum : Focusing on Academic and Industry Perspectives", Korean Journal of Advertising, 115, pp.120-142. 2019.

이 근 호(Keun Ho Lee) [종신회원]

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

〈관심분야〉
침해사고대응, 융합보안, 개인정보보호, 블록체인