사물인터넷융복합논문지 Vol. 9, No. 3, pp. 55-60, 2023 https://doi.org/10.20465/KIOTS.2023.9.3.055

사물인터넷 환경에서 침해사고대응 교육과정 모델에 관한 연구

이근호*
백석대학교 컴퓨터공학부 교수

A Study on the Infringement Incident Response Curriculum Model in IoT Environment

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

요 약 사물인터넷 환경은 보안 위협에 상당히 취약하며, 침해사고가 발생하면 큰 피해를 줄 수 있다. 사물인터넷 환경의 보안을 강화하기 위해서는 사물인터넷 환경의 특성을 고려한 교육과정이 필요하다. 본 논문에서는 사물인터넷 환경에서의 침해사고대응 교육과정 모델을 제안하고자 한다. 제안된 교육과정 모델은 사물인터넷 환경의 보안 위협, 침해사고의 종류, 침해사고대응 절차 등을 위한 모델로 설계하였다. 제안된 교육과정 모델은 사물인터넷 환경에서의 보안 인식을 향상시키고, 사물인터넷 분야에서의 침해사고대응 전문가를 양성하는 데 기여가 예상된다. 제안된 교육과정 모델은 사물인터넷 환경의 보안을 강화하고, 사물인터넷에서의 침해사고대응을 통한 안전성이 기대된다.

주제어 : 사물인터넷, 침해사고대응, 정보보호, 교육과정, 보안 위협

Abstract The IoT environment is very vulnerable to security threats, and if an intrusion occurs, it can cause great damage. In order to strengthen the security of the IoT environment, a curriculum that considers the characteristics of the IoT environment is needed. In this paper, we propose a curriculum model for cyber incident response in the Internet of Things environment. The proposed curriculum model was designed as a model for security threats in the IoT environment, types of intrusion incidents, and incident response procedures. The proposed curriculum model is expected to contribute to improving security awareness in the IoT environment and fostering cyber incident response experts in the IoT field. The proposed curriculum model strengthens the security of the IoT environment and is expected to be safe through security incident response in the IoT.

Key Words : IoT, Infringement incident response, Information Security, Curriculum, Security threat

1. 서론

사물인터넷(IoT)은 사물과 사물 간의 통신을 통해 정보를 교환하고 제어하는 기술이다. IoT는 다양한 산업 분야에서 활용되고 있으며, 그 규모는 빠르게 증가하고 있다. IoT의 증가는 새로운 보안 위협을 야기하고 있으며, IoT 장비는 보안이 고려되지 않은 상태로 설계되는 경우가 많다. IoT 장비 간의 통신은 복잡하고 역동적으로 구성이 되어 있어서, 전통적인 정보보안 환경보다 침해사고에 더 취약한 단점을 가지고 있다. IoT 환경에서

*이 논문은 2023학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2023년 3월 30일 수정일 2023년 5월 21일 심사완료일 2023년 5월 24일

의 침해사고 대응은 매우 중요한 부분이다. 침해사고가 발생하면 IoT 환경에 큰 피해를 주기 때문이다. 침해사고로 인해 IoT 장비가 제어를 잃거나 IoT 장비에 저장된 개인 정보가 유출될 수 있다. IoT 환경에서의 침해사고 대응을 위해서는 IoT 환경의 특성을 고려한 교육과정이 필요하고, 이러한 교육 과정은 IoT 환경의 보안 위협, 침해 사고의 종류, 침해사고대응 절차 등을 교육해야 한다. 또한, 교육과정은 IoT 환경의 보안 인식을 높이고, IoT 보안 전문가를 양성하는 데 중점을 두어야 한다. 본 연구에서는 IoT 환경에서의 침해사고대응 교육과정 모델을 제안하고자 한다. 제안된 교육과정 모델은 IoT 환경의 특성을 고려하여 설계되었으며, IoT 환경의 보안 위협, 침해사고의 종류, 침해사고대응 절차 등을 교육과정으로 포함한다. 제안된 교육과정 모델은 IoT 환경의 보안을 강화하고, IoT 침해 사고를 예방하는 데 도움이 될 것으로 예상한다[1-3].

본 연구에서는 침해사고대응 관련 연구를 통하여 기존에 제안하고 있는 사물인터넷 환경에서의 침해사고대응 관련 교육과정에 대한 내용을 살펴보고, 제안한 교육 내용에서 좀 더 기업체의 맞춤형 교육과정에 대한 모델을 제안하고자 한다. FGI를 통한 침해사고대응분야의 선두기업 2개사의 주요 요구사항을 접목한 교육과정 모델을 설계하고자 한다. 본 교육과정 모델을 위하여 기존에 진행했던 블록체인 기반의 인재양성 사업의 교육과정 개발과 적용 경험을 바탕으로 침해사고대응 운영의 모델을 제안하고자 한다.

2. 관련 연구

2.1 사물인터넷

사물인터넷은 사물과 사물 간의 통신을 통해 데이터를 수집, 처리, 분석하는 기술을 의미한다. IoT는 다양한 분야에서 활용되고 있으며, 그 범위는 점점 확대되고 있다. IoT 환경은 기존의 정보보안 환경과는 매우 다르고, IoT 환경은 사물, 사물 간의 통신이 매우 복잡하고 역동적이며, 사물은 보안을 고려하여 설계되지 않고 있다. 이러한 특성으로 인해 IoT 환경은 전통적인 정보보안 환경보다 침해사고에 더 취약한 상황이다. IoT 환경에서의 침해사고대응은 매우 중요한 부분이다. 침해사고가 발생하면 IoT 환경에 큰 피해를 줄 수 있다. 침해사고로 인해 IoT 장비가 제어를 잃거나 IoT 장비에 저장된 개인 정보가 유출될 수 있다. IoT 환경의 보안 위협은 다음과 같다.

- 물리적 공격: IoT 장비에 대한 물리적 공격은 IoT 장비를 파괴하거나 데이터를 훔치는 데 사용될 수 있다.
- 네트워크 공격: IoT 장비에 대한 네트워크 공격은 IoT 통신에 대한 장애를 발생시킬 수 있으며, 사물인터넷에서의 서비스 장애를 발생하여 사회적인 문제를 일으킬 수 있다.
- 소프트웨어 공격: IoT 장비에 대한 소프트웨어 공격은 서비스 운용에 다양한 취약점을 내포하고 있으며, 서비스의 장애 유발과 소스코드의 취약점으로 인한 공격시나리오가 가능할 수 있다.
- 인적 실수: IoT 장비에 대한 인적 실수는 IoT 장비를 운영하는데 취약점을 유발하고, 관리의 부재를 통한 관리체계를 취약하게 만들 수 있다.

IoT 환경에서의 침해사고대응 절차는 다음과 같다. 침해사고를 탐지, 침해사고의 원인을 조사, 침해사고의 영향을 평가, 침해사고 복구, 침해사고를 예방하기 위한 조치를 취한다. IoT 환경에서의 침해사고를 예방하기 위해서는 IoT 장비를 안전하게 설정하고, IoT 장비를 최신 상태로 유지하며, IoT 장비에 대한 보안 패치를 설치하고, IoT 장비에 대한 보안 인식을 높이기 위한 교육 등의 다양한 관리체계에 대한 조치를 취해야 한다[4-6].

2.2 국내외 침해사고 현황 및 문제점

2022년 사이버안보 위협 주요 특징 및 내년 전망에 따르면 2022년 침해사고는 국가 배후 해킹조직의 증가, 국내 외교·안보 현안 및 첨단기술 절취를 대상으로 하고 있으며, 내년에는 사회 혼란 목적의 해킹, 공공·기업 대상 랜섬웨어, 공급망 해킹, 첨단기술·안보현안 절취 목적의 공격이 우려되고 있다. 해외 주요국가(미국, 일본, EU 등) 기업 및 조직이 디지털화되며 사이버보안에 대한 수요가 급격하게 증가하고 있으며, 침해사고 대응 산업을 미래 경쟁력의 핵심으로 판단하여 디지털 환경에서 정보보안 산업의 글로벌 경쟁력과 신성장동력 확보에 주력하고 있다. 연도별 사이버 침해사고 건수는 2019년 418건, 2020년 603건, 2021년 640건, 2022 11월기준 1045건으로 연도별 침해사고 건수는 매년 증가하고 있는 추세이다. 국내 사이버 침해사고의 경적적 피해액은 대기업 20억9,000만원, 중견기업 17억4,000만원, 중소기업 4억4,000만원, 비영리재단 2,000만원 등으로 기업 규모가 클수록 침해사고의 경제적 피해액이 증가하고 있다. 세계적으로 사이버 침해사고 건수가 급격하게 증가하고 있으나 기업 인력 수요를 충족하지 못하고 있으며,

민간 사이버 침해대응을 전담하는 KISA 사이버침해사고대응본부의 사고대응 인력은 2019년 120명에서 2021년 121명으로 인력 충원이 부족한 실정이다. 침해사고는 국가 기반시설, 제조업 기업 등의 공격으로 국가 기밀유출, 기업정보 유출, 개인정보 유출과 같은 사고로 인해 향후 국가 경쟁력에 심각한 장애를 초래할 것으로 전망하고 있다[7-8].

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[9-15].

3. 침해사고대응 교육과정 모델 설계

3.1 Focus Group Interview

Focus Group Interview 을 통한 침해사고대응 분야의 선두기업인 2개 사의 침해사고대응 인력양성 수요를 확인하여 인재양성의 목적의식이 뚜렷한 A사, B사를 참여기업으로 선정하여 수요 내용을 확인하였다. 결과 내용으로는 침해사고대응 분야 전문융합 산업 현장에서 필요로 하는 문제 규명, 산업 현장 문제 해결에 필요한 지식/직무 도출, 지식/직무에 대한 우선순위 설정, 산업체 선호 훈련생 역량, 산학 프로젝트 주제 도출, 참여기업의 훈련 참여계획의 내용을 확인하였다. 참여기업의 의견은 다음과 같다.

교육과정은 사물인터넷 환경의 특성을 고려하여 설계되어야 하고, 사물인터넷 환경은 기존의 IT 환경과는 다른 특성을 가지고 있어, 연결된 장치의 수가 많고, 장치의 성능이 낮으며, 보안 기능이 취약한 특성을 고려하여 교육과정은 사물인터넷 환경에서 발생할 수 있는 보안사고의 유형과 대응 방법을 포함해야 한다. 교육과정은 실습 위주로 진행되어야 하고, 실습 위주로 진행되는 교육과정은 학생들이 사물인터넷 보안 기술을 실무적으로 적용하는 방법을 배울 수 있다. 교육과정은 최신 보안 기술 동향을 반영해야 하고, 보안 기술은 빠르게 변화하고 있어서 학생들이 최신 보안 기술을 배울 수 있도록 구성해야 한다.

세부적인 산업체 요구사항은 네트워크기반 사고대응 모델링, 침해사고 및 악성코드 분석, 실무융합, 현장적응 능력이 필요하다는 의견이었다. 2개사에서 제안한 프로젝트 주제와 멘토들을 통해 실제 참여기업이 요구하는 실무 역량을 배양하고, 교수자-학습자-기업간의 밀착형 멘토링 진행시 경제성, 기술 성숙도 등의 여러 측면에서 현업의 실제 프로젝트 수준의 진행이 필요하고, 지속적인 침해사고대응 분야에 대한 최신 트렌드 정보 습득을 통한 디지털 리터리시 확보가 필요하다는 의견이 도출되었다.

〈Table 1〉 Job analysis based on industry demand

Industry Requirements	Competence by job
Network-based incident response modeling	Understanding computer networks
	TCP/IP, P2P network programming
	Understanding Cryptography-Based Technologies and Application
	Understanding types of network-based security incidents
	Network-based incident analysis
	Network-Based Cyber Threat Modeling
	Infringement case-based risk analysis
Incident and malicious code analysis	Incident Response Job Overview
	Understanding cyber attack tactics and techniques
	Intrusion incident types and response techniques through log analysis
	Understanding Malicious Code Types and Countermeasures
Practical convergence	CERT Practical Convergence Project 1
	CERT Practical Convergence Project 2
	CERT Practical Convergence Project 3
	Capstone design in connection with industry mentors

3.2 침해사고 직무별 세부 역량

[표1]에서 2개 참여기업에서는 직무역량을 크게는 네트워크 기반 사고대응 모델링, 침해사고 및 악성코드 분석, 실무융합으로 나뉘어 진다.

네트워크 기반 사고대응 모델링은 컴퓨터 네트워크 이해, TCP/IP, P2P 네트워크 프로그래밍, 암호 기반 기술 및 응용 기술 이해, 네트워크 기반 보안사고 유형 이해, 네트워크 기반 침해사고 분석, 네트워크 기반 사이버 위협 모델링, 침해사고 사례기반 위험 분석으로 나누어진다. 침해사고 및 악성코드 분석은 침해사고 대응 직무 개요, 사이버공격 전술과 기법 이해, 로그분석을 통한 침해사고 유형 및 대응기법, 악성코드 유형 및 대응기법 이해로 구분되어 진다.

실무융합에서는 CERT 실무융합 프로젝트를 학년별로 수행하도록 구성하였다.

3.3 침해사고대응 교육과정 모델

[표2]처럼 참여기업의 요구사항을 반영한 교육과정에서 교과목은 침해사고 대응개론, 사이버 보안 환경의 이해, 융합프로젝트, 사이버 공격 전술과 기법, 네트워크 포렌식, 침해사고 로그분석, 침해사고 위협 모델링, 악성코드 분석, 사례기반 사고분석 교과목으로 구성하였다. 침해사고 대응개론에서는 침해사고 대응업무를 위한 기본지식 습득, 호스트 기반 침해사고 대응을 위한 데이터 수집 절차와 방법 이해 등을 학습하도록 구성한다. 사이버 보안환경의 이해에서는 네트워크 레이어 관점의 인터넷 연결구조 이해, 사이버 공격자와 방어자의 상호작용에 따른 변화 이해를 학습한다.

〈Table 2〉 Infringement response training course model customized for industry

Subject	Lecture content
Intrusion Response Introduction	▸Acquisition of basic knowledge for intrusion response work ▸Understanding data collection procedures and methods for host-based incident response ▸Understanding the threats that analysts need to diagnose in the event of a breach
Understanding the Cybersecurity Environment	▸Understanding the history, components and routing structure of the Internet ▸Understanding the Internet connection structure from the network layer perspective ▸Understanding the changes according to the interaction between cyber attackers and defenders
Convergence Project 1	▸Intensive security incident response project through industry expert mentoring ▸Development of an accident response convergence project by collaborating with mentors on a team basis ▸Project results presentation and expert feedback
Cyber attack tactics and techniques	▸Understanding the cyber attack process based on attacker behavior patterns ▸Understanding attack methods and techniques used by attackers ▸Understanding the operating principles of the attack tools used by attackers in each attack method and technology
Network forensics	▸Introduction to Network Forensics ▸Establishment of environment for network forensics ▸Application of unit accident-based network forensic analysis technology
Convergence Project 2	▸Intensive security incident response project through industry expert mentoring ▸Development of an accident response convergence project by collaborating with mentors on a team basis ▸Project results presentation and expert feedback
Incident log analysis	▸Understanding the types of logs generated by infrastructure where intrusions usually occur ▸Understanding typical attack techniques by infrastructure ▸Acquisition of data analysis techniques for intrusion analysis and response ▸Acquisition of infringement accident analysis know-how through intrusion accident case analysis based on actual cases
Incident Threat Modeling	▸Introduction to Cyber Threat Modeling ▸Basic of big data analysis based on open source ▸Understanding denial-of-service attacks from the defender's point of view
Convergence Project 3	▸Intensive security incident response project through industry expert mentoring ▸Development of an accident response convergence project by collaborating with mentors on a team basis ▸Project results presentation and expert feedback
Malware Analysis	▸Understanding the type of malware that attackers mainly use in intrusion incidents ▸Learn techniques for profiling suspicious malware ▸Learn analysis techniques to identify the cause of malware infection in Windows systems ▸Learn analysis techniques to determine the impact of malware infection on Windows systems
Case-based accident analysis	▸Understanding and analysis of 7.7 DDoS attack based on Silog ▸Understanding and analysis of DrDoS based on Silog ▸Understanding and Analysis of Shilog-based BGP Hijacking ▸Understanding and analysis of APT attacks based on Silog

융합프로젝트에서는 산업체 전문가 멘토링을 통한 침해사고 대응 심화 프로젝트로 팀 단위로 멘토와 협업하여 사고대응 융합프로젝트 개발을 진행한다.

사이버 공격 전술과 기법에서는 공격자 행위 패턴을 기반으로 한 사이버 공격 프로세스 이해, 공격자가 공격 주로 활용하는 공격방법과 기술 이해, 각 공격방법과 기술에서 공격자가 주로 활용하는 공격 도구 동작원리를 이해하는 내용을 학습한다.

네트워크 포렌식에서는 네트워크 포렌식 개론, 네트워크 포렌식을 위한 환경구축, 단위사고 기반의 네트워크 포렌식 분석기술 적용을 학습한다.

침해사고 로그분석에서는 침해사고가 주로 발생하는 인프라에서 생성하는 로그 유형 이해, 인프라 별 대표적인 공격 기법 이해, 침해사고 분석 및 대응을 위한 데이터 분석 기법 습득, 실사례를 기반으로 한 침해사고 케이스 분석으로 침해사고 분석 노하우 습득하는 과정을 학습한다.

침해사고 위협 모델링은 사이버침해사고 위협 모델링 소개, 오픈소스 기반의 빅데이터 분석 기초, 방어자 관점의 서비스거부공격의 이해를 학습한다.

악성코드 분석에서는 침해사고에서 공격자가 주로 사용하는 악성코드 유형 이해, 의심스러운 악성코드를 프로파일링하기 위한 기법 습득, Windows 시스템에서 악성코드 감염 원인을 파악하기 위한 분석 기법 습득, Windows 시스템에서 악성코드 감염에 따른 영향을 파악하기 위한 분석 기법 습득을 학습한다.

사례기반 사고분석에서는 실로그 기반의 7.7 DDoS 공격의 이해 및 분석, 실로그 기반의 DrDoS의 이해 및 분석, 실로그 기반의 BGP하이재킹의 이해 및 분석, 실로그 기반의 APT 공격의 이해 및 분석을 학습한다.

4. 결론

사물인터넷 기술은 빠르게 발전하고 있으며, IoT 환경에서 발생하는 보안 사고의 위험도 증가하고 있다. 이러한 보안 사고를 예방하고 대응하기 위해서는 IoT 보안 전문가의 양성이 필요하다. 본 연구에서는 IoT 환경에서 침해사고 대응을 위한 교육과정 모델을 제안하였다. 제안된 교육과정 모델은 IoT 환경의 특성을 고려하여 설계되었으며, IoT 보안 전문가가 되기 위해 필요한 지식과 기술을 제공하도록 하였다. 또한, 침해사고대응 관련 교육과정은 실습 위주로 진행되어 학생들이 IoT 보안 기술을 실무적으로 적용하는 방법을 배울 수 있다. 제안된 교육과정 모델은 IoT 보안 전문가의 양성을 통해 IoT 환경의 보안을 강화하는 데 도움이 될 것이다.

본 연구에서는 IoT 환경에서 침해사고 대응을 위한 교육과정 모델을 제안하였으나, 몇 가지 한계가 있다. 첫째, 제안된 교육과정 모델은 사물인터넷 환경의 특성을 고려하여 설계되었지만, 실제 교육을 통해 교육 효과를 검증하지 못했다. 둘째, 제안된 교육과정 모델은 IoT 보안 전문가가 되기위해 필요한 지식과 기술을 제공하지만, IoT 보안 기술은 빠르게 변화하고 있기 때문에 교육과정 모델을 지속적으로 업데이트해야 한다. 셋째, 제안된 교육과정 모델은 실습 위주로 진행되어 학생들이 IoT 보안 기술을 실무적으로 적용하는 방법을 배울 수 있지만, 실습 환경을 구축하는 데 비용이 많이 소요될 수 있다.

향후 연구에서는 제안된 교육과정 모델의 교육 효과를 검증하고, 교육과정 모델을 지속적으로 업데이트해야 하고, 실습 환경을 구축하는 데 드는 비용을 줄일 수 있는 방안을 연구하고자 한다.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] "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.

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

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

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

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

[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] 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.

[11] 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.

[12] 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.

[13] 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.

[14] S.B.Kang, S.J.Lee and J.I.Lim, “A Study on the Effective Countermeasures for Preventing Computer Security Incidents”, Journal of The Korea Institute of Information Security and Cryptology, Vol.22, No.1, pp.107-115, 2012.

[15] M.G.Lee, “A Development of Curriculum for Information Security Professional Manpower Training”, Journal of the Institute of Electronics and Information Engineers, Vol.54, No.1, pp.46-52, 2017.

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