KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.7 pp.321~328 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.7.321

Enhancing Education Curriculum of Cyber Security Based on NICE

Wonhyung Park† · Seongjin Ahn††

ABSTRACT

As the cyber threats become more sophisticated and intelligent, the cases of cyber-infringement accidents are rapidly increasing. As a result, awareness of the importance of cyber security professionals has led to many cyber security-related educational programs. These programs provided with education curriculum aimed because cyber security workforce and job-based cyber security education research are not properly done. In this study, we developed a new cyber security education curriculum that defines and reflects cyber security personnel and knowledge system. In this study is not composed solely of the education contents related to the defenses emphasized in the existing education curriculum, but developed education curriculum to train a professional and balanced cyber security manpower by adding education contents in the attack field.

Keywords : NICE, Cybersecurity, Security Education, Security Workforce, Security Knowledge System

NICE 기반 사이버보안 교육커리큘럼 개선 연구

박 원 형† · 안 성 진††

요 약

사이버 위협이 고도화되고 지능화되어짐에 따라 사이버 침해사고로 인한 피해사례가 급격하게 증가하고 있다. 이로 인해 사이버보안 전문인력의 중요성을 인식하여 다수의 사이버 보안관련 교육 프로그램이 운영되고 있지만 사이버보안 인력 현황 및 직무에 기반한 사이버보안 교육연구가 이루어지 않아서 교육 수요자 및 공급자가 목표한 교육과정이 제공되지 않고 있다. 이에 따라 본 연구에서는 사이버보안 인력 및 지식체계를 정의하고 이를 반영한 새로운 사이버보안 교육 커리큘럼을 개발하였다. 본 연구에서 개발한 교육 커리큘럼은 기존 교육 커리큘럼에서 강조하고 있는 방어와 관련된 교육내용만으로 구성하는 것이 아니라, 공격분야의 교육내용을 추가하여 전문적이고 균형적인 사이버보안 인력양성을 위한 교육 커리큘럼을 개발 및 개선하였다.

키워드 : NICE, 사이버보안, 보안교육, 보안인력, 보안 지식체계

1. 서 론

사이버 위협의 고도화, 지능화에 따라 새로운 수법을 통해 사이버 침해사고로 인한 피해사례가 꾸준히 증가하고 있으며, 이에 따른 사이버대응 전문 인력의 수요 또한 급증하고 있다. 이에 따라 사이버 사고 대응 인력의 중요성을 인식하여 다양한 교육프로그램이 운영되고 있지만 아직까지 국내 사이버보안 인력 현황과 관련한 통계조차 제대로 없는 상황이라 직무와 관련된 사이버보안 교육 수요를 파악하고 이에 맞는 교육과정을 기획하는 것이 어렵다. 이와 같은 상황으로 인해 기존에 시행되고 있는 사이버보안 인력 양성 사업의 경우에도 교육 대상 및 제공하는 교육 내용이 차이가 많이 있다. 물론 이러한 차이가 그 자체로 문제라고 할 수는 없지만, 향후 해당 사업을 계속하는 경우 교육 수요자 및 교육 공급자 모두 목표와 방향을 예측하기 어렵다는 문제 이다. 교육 수요자 및 공급자 모두 목표와 방향을 예측할 수 있도록 교육내용을 표준화하는 것이 필요하다[1, 2].

이에 따라 본 논문은 기존의 시행되고 있는 사이버보안 인력양성사업 교육과정 및 국내 교육과정에 대한 분석을 토대로 사이버보안 인력에 대한 커리큘럼을 제시하고자 한다. 최적화된 사이버보안 인력 교육훈련 표준 커리큘럼을 개발하기 위해 국외에서 가장 많이 사용되어지고 신뢰성이 있는 NICE workforce framework을 기준자료로 하여 국내 사이버보안 인력 양성교육 커리큘럼을 분석하고자 한다. 또한 본 연구에서는 기존의 교육 커리큘럼에서 강조하고 있는 방어와 관련된 교육내용만을 구성하는 것이 아니라, 최정예 사이버보안 인력 양성을 위한 교육 및 훈련 프로그램을 개발하기 위해 공격분야의 교육내용을 추가한 개선된 커리큘럼을 개발한다.

† 종신회원 : 극동대학교 산업보안학과 조교수
†† 종신회원 : 성균관대학교 컴퓨터교육학과 교수
Manuscript Received : February 22, 2017
Accepted : May 17, 2017
* Corresponding Author : Seongjin Ahn(sjahn@skku.edu)

2. 사이버보안 인력 및 지식체계

기존 사이버보안 교육 분석 및 최적화 된 표준커리큘럼을 개발하기 위해 우선적으로 사이버보안 인력 및 지식체계를 정의하고자 하였다. 본 연구는 국외에서 가장 많이 활용되어지고 신뢰성이 있는 미국 NICE(National Initiative for Cybersecurity Education)의 Workforce Framework을 기준으로 사이버보안 인력 및 지식체계를 정의하였다[3, 4].

NICE의 Workforce Framework는 사이버보안과 관련된 업무 및 전문기술을 카테고리별로 분류하고 특정 업무마다 개인에게 요구되는 역량을 세밀히 분석한 정보보호 지식체계이다. 이는 사이버 영역 전반을 포괄하는 범위에서 사이버보안 인력양성을 다루기 위한 것으로 각 업무 분류별 세부 직종마다 주요 업무 내용과 필요한 지식 등을 구체적으로 정리하고 기업 및 단체가 현재 필요한 인재를 파악해 추가 인력 확보 및 사이버보안 교육 프로그램 계획 등 폭넓게 활용하기 위해 제작되었다. 이러한 Workforce Framework는 31개 전문 영역을 7개 분야로 분류하여 제시하고 있으며, 자세한 내용은 Table 1과 같다[5, 6].

NICE 사이버보안 교육 분류체계의 구성은 공격과 방어의 관점에서 구성이 되어 있으나, 대부분의 방어관점의 지식체계를 다루고 있다. 따라서 커리큘럼 개발과정에서 방어 분야의 내용만 아니라 공격 분야의 교육내용도 추가하여 진행할 필요가 있다[7-10].

Table 1. Education Classification System in NICE Cyber Security

Sort	Specialty Areas
Securely Provision	Systems Requirements Planning
	System Development
	Software Assurance and Development Security
	System Security Architecture
	Test and Evaluation
	Technology Research and Development
	Information Warranty Compliance
Operate and Maintain	System Administration
	Network Services
	Systems Security Analysis
	Customer Service and Technical Support
	Data Administration
	Knowledge Management
Collection and Operate	Collection activity
	Cyber Mission Planning
	Cyber Mission Operating
Protect and Defend	Vulnerability Assessment and Management
	Incident Response
	Computer Network Defense (CND) Analysis
	Computer Network Defense (CND) Infrastructure Support
Investigate	Investigation
	Digital Forensics
Analyze	Cyber Threat Analysis
	Exploit Analysis
	Target Analysis
	Information Analysis
Oversight and Development	Legal Advice and Advocacy
	Education and Training
	Strategic Planning and Policy Development
	Information Systems Security Operations
	Security Program Management (Chief Information Security Officer

3. 민간 교육기관 사이버보안 교육 커리큘럼 분석

3.1 코어시큐리티

코어시큐리티의 사이버보안 교육은 총 3개의 도메인("악성코드 탐지", "쉘 코드 분석기법", "침해대응을 위한 디지털 포렌식")으로 나누어진다.

"악성코드 탐지" 도메인은 메모리, 파일시스템, 실행파일, 레지스트리 등 윈도우 운영체제의 다양한 아티펙트 조사를 통한 악성코드 탐지 방법을 설명하고 있다. "쉘 코드 분석기법" 도메인은 PDF, Office 파일 등에 포함되어 있는 악성 쉘 코드 추출하고 그 동작원리를 분석하는 방법을 다루고 있다. "침해대응을 위한 디지털 포렌식" 도메인은 손상된 파티션 복원, 삭제된 파일 복원 등 디스크에서 수행할 수 있는 디지털 포렌식 기술을 초중반부에 다루고 있다. 본 교육의 자세한 내용은 다음의 Table 2와 같다.

Table 2. Cybersecurity Education Curriculum in Coresecurity

Subject	Chapter	Contents
Malware detection	Detection technique	o Detecting malware through memory forensics o Detecting Malicious Code Using Meta files o PE file analysis
Digital Forensics for Responding to Infringement	Volume Analysis	o Understanding partitions / extended partitions
	File System Analysis	o File system structure analysis o File recovery technique
	Web browser usage trace analysis	o Usage Trace Analysis using cookies, temporary files, History
	Registry Analysis	o Understanding the registry structure o Registry Key Recovery

3.2 씨드젠

씨드젠의 사이버보안의 교육은 총 5개의 도메인("모의해킹 프로세스", 웹 어플리케이션 해킹", 안드로이드 해킹과 보안", "악성코드 분석 과정", "APT 공격 사례 및 관련 취약점 분석방법")으로 나누어진다. "모의해킹 프로세스" 도메인은 하나의 공격 시나리오를 예로 들어 실습을 진행한 후 보고서 작성을 하면서 마무리 된다. "웹 어플리케이션 해킹" 도메인은 OWASP Top 10 목록과 관련하여 가장 빈번하게 발견되는 취약점 6 개를 예로 들어 공격 실습을 진행하며, 서버 보안 설정을 통해 대응방법을 학습한 후 마무리 된다. "안드로이드 해킹과 보안" 도메인은 안드로이드를 기반으로 하는 악성코드에 대한 동적/정적 분석 방법을 학습한다. 또한 악성코드가 숨겨져 있는 악성 앱을 리패키징하여 배포하는 방법을 다루고 있다. 후반부에는 코드 난독화, 암호화, 권한관리 등의 대응 방안을 다루면서 마무리 되고 있다. "악성코드 분석과정" 도메인은 Windows 운영체제기반 악성코드에 대한 동적분석 및 언패킹을 주된 주제로 하고 있다. "APT 공격사례 및 관련 취약점 분석방법" 도메인은 사용자의 시스템 제어 권한을 획득하는데 많이 사용되는 악성 문서 및 쉘 코드 분석 방법을 주된 주제로 다루고 있다. 본 교육의 자세한 내용은 다음의 Table 3과 같다.

Table 3. Cybersecurity Education Curriculum in Seedgen

Subject	Chapter	Contents
Simulation Hacking Process	Simulation Hacking Methodology and Environment Construction	Theory, Concept, Scenario, Simulation Hacking
	Simulation Hacking Practice #1	o Googleling o shodan Search o nmap Scan o zone transfer o OpenVAS
	Simulation Hacking Practice #2	o Password Brute Forcing o Exploit code production
	Simulation Hacking Theorem	Remote system penetration and reporting
Web application hacking	Web Hacking Overview and Basics	Web Hacking Overview and Theory
	Introduction to Web Vulnerabilities	Understanding OWASP Top10 List
	Web Hacking Attack Practice	Practice based on OWASP Top10 List
	Web hacking Attack Countermeasures	Server security settings

3.3 라온 화이트햇센터

라온 화이트햇센터의 사이버보안 교육은 총 6개의 도메인("악성코드 분석", "침해사고 분석", "시스템 취약점 분석", "네트워크 포렌식", "Metasploit을 이용한 모의침투", "웹 해킹과 보안")으로 나누어진다.

"악성코드 분석" 도메인은 리버스엔지니어링 기술을 초반부에 다루고 있으며 중반부에는 악성코드에 대한 동적분석 기법을, 후반부에는 정밀분석 방법을 다루고 있다. "침해사고 분석" 도메인은 초반부에 타임라인 분석기법, 로그분석기법, 레지스트리 분석기법, 루트킷 탐지 기법을 다루고 있으며, 중반부에는 웹 사이트 해킹을 기반으로 한 침해사고 대응 시나리오를 교육하고 있다. 후반부에는 침해사고 대응 업무수행과 관련된 결과 보고서 작성 방법을 다루고 있다. "시스템 취약점 분석"은 전통적인 익스플로잇 기법을 초반/중반부에서 다루고 있으며, 후반부에서는 쉘 코드 분석 기

Table 4. Cybersecurity Education Curriculum in Raon Whitehatcenter

Subject	Chapter	Contents
Malicious code analysis	Reverse Engineering Definition	Reversing theory
	Utilizing tools for reverse engineering	Introduction to the debugger for malware analysis
	Usage of Reverse Engineering	Crackme practice
	Malicious Code Analysis	Dynamic analysis of malicious code through network monitoring
	Dynamic Analysis & Static Analysis	Code analysis (Precise analysis)
Simulation Penetration using Metasploit	Concept	Metasploit framework
	Info-gathering	Information gathering techniques
	Personal computer	Attack procedure using Windows vulnerability
	Personal computer-cont	Attack procedure using Windows vulnerability
	Social Engineering	Attack procedure using Windows vulnerability
	Linux-server	Attack procedure using Linux server vulnerability
	window-server	Attack procedure using window server vulnerability
	database	Attack procedure using mssql vulnerability
	MSF Extended Usage	Understanding the Metasploit Add-In

법을 다루고 있다. “네트워크 포렌식” 도메인은 초반부에는 네트워크에서 사용되는 기본 프로토콜들의 동작원리와 터널링의 동작원리에 대해서 다루고 있다. 중반부에는 패킷 덤프를 대상으로 한 wireshark/tshark 도구 활용 방법을, 중후반부에는 DDoS, ARP Spoofing, P2P 봇넷과 관련된 네트워크 트래픽 분석 방법을 교육하고 있다. 후반부에는 침입탐지시스템 운영 및 룰 작성방법으로 마무리된다. “Metasploit을 이용한 모의침투” 도메인은 Metasploit Framework 를 이용하여 기존 발표된 시스템 취약점 기반 공격 기법을 시나리오 형태로 구성하고 있다. “웹 해킹과 보안” 도메인은 초반부에 HTTP 프로토콜의 기본 구조를 다루고 있으며 중반부에는 XSS, CSRF, SQL Injection, File Upload와 같은 주요 취약점들을 다루고 있다. 본 교육의 자세한 내용은 Table 4와 같다.

3.4 테크데이타 웹타임 교육센터

테크데이타 웹타임 교육센터의 사이버보안 교육은 총 5개의 도메인(“웹의 이해”, 웹 취약점 이해”, “웹 Exploit 공격과 분석”, “웹 DDoS 이해”, “웹 침해 분석”)으로 나누어진다. “웹의 이해” 도메인은 웹에서 사용되는 HTTP의 헤더구조, 메서드, 클라이언트/서버 측 언어, 쿠키 및 세션과 관련된 내용을 소개한다. “웹 취약점 이해” 도메인은 OWASP Top 10 목록과 관련된 5가지 취약 요소들을 다루고 있다. “웹 Exploit 공격과 분석” 도메인은 OWASP Top 10 목록의 Injection 취약점과 관련된 주제를 주된 내용으로 다루고 있다. 더불어 Metasploit의 SET(Social-Engineer Toolkit)을 이용한 공격 시나리오도 다루고 있다. “웹 DDoS 이해” 도메인은 전통적인 네트워크 기반 DDoS 기법과 응용계층 기반 DoS&DDoS 공격 기법을 소개하고 있다. “웹 침해 분석” 도메인은 웹 기반 보안위협에 대응하기 위한 시큐어 코딩 및 보안설정을 교육하며, 보안 사고가 발생한 후 수행해야 할 로그 분석 기법을 다루면서 마무리 되고 있다. 본 교육의 자세한 내용은 Table 5와 같다.

Table 5. Cybersecurity Education Curriculum in Techdata Webtime

Subject	Chapter	Contents
Web information protection specialist	Understanding Web	Understanding http protocols, methods, web languages, cookies / sessions
	Understanding Web Vulnerabilities	o Web Vulnerabilities o Googleling o SQL Injection o XSS o CSRF o Clickjacking
	Web Exploit Attack and Analysis	o Web2.0이해 o DOM Injection o XML Injection o JSON Injection o Attacks using vulnerability tools
	Understanding Web DDoS	Understanding and responding to DDoS attacks
	Web Infringement Analysis	o Secure Coding o Secure Testing o Log analysis o Server security settings

3.5 한국첨단기술진흥원 컨소시엄

한국첨단기술진흥원 컨소시엄의 교육은 총 2개의 도메인으로 나누어진다.

첫 번째 도메인인 “대한민국 정보보호 실무 개론”은 교육과정 소개를 시작으로 3.20 대란에 대한 내용을 개론 수준으로 다루고 있다. 두 번째 도메인인 “최정예 사이버보안 인력 양성 교육”에 핵심 교육과목 내용들의 대부분이 포함되어 있다. 두 번째 도메인은 크게 12개의 하위분류로 나누어진다. 본 교육의 자세한 내용은 Table 6과 같다.

Table 6. Cybersecurity Education Curriculum in K-EMDEC Consortium

Subject	Chapter	Contents
Cyber Security Workforce Training	Simulation Hacking Principles and Techniques	o Understanding APT o Malicious code production using VB script
	Understanding Shell Codes	o Reversing Basics o Shell Code Analysis
	Making Malware	o Understanding malicious code types and behavior o Malware creation
	Malware Analysis	o API analysis mainly used by malicious code
	Making Shellcode	o Understanding Shell Codes o Shellcode creation
	Heap spray Attack	Understanding and creating Heap Sprays
	Bypass Anti-Virus	o PE structure theory o Section encoding techniques
	SEH Overwrite	o Understanding BOF and SEH Overwriting Techniques o Security Cookie
	Firewall	Applying firewall rules and iptables rules
	ARP Spoofing	o Understanding ARP protocol structure
	XSS & CSRF	Understanding Attack Techniques
	SQL Injection	Understanding Attack Techniques

3.6 한국정보보호교육센터

한국정보보호교육센터의 교육은 총 5개의 도메인("정보보호 기본실무", "네트워크 공격과 방어 실전", "웹 공격과 방어 실전", "시스템 보안", "침해대응 및 디지털 포렌식")으로 나누어진다. "정보보호 기본실무" 도메인은 정보보안 기술과 관련된 동향 및 개론 수준의 내용을 담고 있다.

"네트워크 공격과 방어 실전" 도메인은 정보수집 기술인 Footprinting, Scanning을 시작으로 SSH MITM, DNS Spoofing, SSL MITM 등의 네트워크 기반 공격 기법을 담고 있다. 후반부에는 DDoS 관련 공격 기법 및 대응 방법에 대해서 다루고 있다. "웹 공격과 방어 실전" 도메인은 HTTP 프로토콜의 기본 구조 및 동작원리를 설명하는 것을 시작으로 웹 기반 정보수집기법, OWASP Top10 소개, 웹 기반 도구 활용 방법 등을 중반부에 다루고 있다. 후반부에는 XSS, CSRF, 파일 업로드/다운로드와 같은 웹 어플리케이션의 대표적인 공격 기법들을 다루고 있다. "시스템 보안" 도메인은 초반부에 윈도우 및 리눅스 운영체제의 리소스 및 디렉터리 구조 등을 간단하게 소개하고 중반부에는 정보수집 및 패스워드 크래킹 등의 내용을 다루고 있다. 후반부에는 Metasploit Framework를 이용한 악성 PDF 파일 제작방법 및 공격 시나리오에 대해서 다루고 있다. "침해대응 및 디지털 포렌식" 도메인은 초반부에 침해사고 대응 절차와 디지털 포렌식 관련 개요를 다룬다. 디지털 포렌식 부분의 경우 파일시스템, 윈도우 아티펙트 분석 기법에 초점을 두며, 침해사고 부분의 경우 리눅스 및 윈도우 시스템에서 침해사고가 발생했을 때 조사해야 할 내용들을 담고 있다. 후반부에는 포렌식을 방해하기 위한 안티 포렌식 기술들을 소개하고 있다. 본 교육의 자세한 내용은 Table 7과 같다.

Table 7. Korea Information Security Education Center Cyber Security Education Curriculum

Subject	Chapter	Contents
Basic practice of Information Security	Recent Trends in Security Technology	Introduction
	Introduction to information protection	Introduction
Network Attack and Defense Practice	Information gathering	Understanding footprinting, scanning techniques and using tools
	MITM	o Sniffing plain text data o SSH MITM o DNS Spoofing o SSL MITM
	Types of DDoS attacks and malicious code treatment	Understanding and responding to DDoS attack types
Web Attack and Defense Practice	Web service security	Understanding the http protocol, methods
	Web hacking procedure	o Information gathering techniques o Understanding OWASP top10 list attack techniques o Installing the Public Inspection Tool
	Web hacking practice	o File upload / download vulnerability o XSS o CSRF

4. 기존 교육과정과 비교분석

본 연구는 개발한 표준 커리큘럼과 기존의 운영되고 있는 사이버보안 교육과정간의 차이점 및 연관성을 분석하기 위해서 비교분석을 했다.

코어시큐리티의 교육 과정은 "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 중 "방어" 카테고리의 3개 과목, "기타" 카테고리의 1개 과목과 연관성을 가진다. "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 4개가 연관성을 가지므로 17%의 매핑률을 보이고 있었다. 주로 침해사고 상황이 발생 했을 때 수행하는 악성코드 탐지 및 분석 파트에 콘텐츠의 비중이 높은 편이다. 과목의 밸런스 측면에서 보면 "공격" 카테고리의 비중이 작고 "방어" 카테고리에 편중된 편이였다. 또한 악성코드 탐지 및 분석, 쉘 코드 분석 분야에 대해서는 다양한 접근 방법을 소개하고 있다.

씨드젠의 교육 과정은 "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 중 "공격" 카테고리의 5개 과목, "방어" 카테고리의 5개 과목, "기타" 카테고리의 1개 과목과 연관성을 가진다. "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 11개가 연관성을 가지므로 47%의 매핑률을 보이고 있다. 대체적으로 공격과 방어 양쪽 카테고리에 속하는 과목들이 균등하게 구성되어 있으나 로그분석, 보안 솔루션, 패킷분석 등과 같이 "방어" 카테고리에 속하는 콘텐츠의 비중이 적은 편이다.

라온 화이트햇센터의 교육 과정은 "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 중 "기초" 카테고리의 1개 과목, "공격" 카테고리의 2개 과목, "방어" 카테고리의 8개 과목과 연관성을 가진다. "사이버보안 인력 교육훈련 표준 커리큘럼"에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 11개가 연관성을 가지므로 47%의 매핑률을 보이고 있다. "방어" 카테고리와 연관된 콘텐츠의 비중이 높은 편이며, "공격" 카테고리의 경우 네트워크 보안 및 모바일 보안 관련 콘텐츠의 비중이 낮은 편이다. "공격"과 "방

어” 카테고리에서만 비교분석 했을 때 전반적으로 콘텐츠의 밸런스가 균등한 편이다.

테크데이타 웹타임 교육센터의 교육 과정은 “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 중 “공격” 카테고리의 2개 과목, “방어” 카테고리의 3개 과목과 연관성을 가진다. “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 5개가 연관성을 가지므로 21%의 매핑률을 보이고 있다. 콘텐츠의 구성이 “웹 기반 취약점 분석 및 공격” 과목에 상당히 편중되어 있으며 “공격” 및 “방어” 카테고리에서 필수적으로 요구되는 APT, 모바일 보안, 악성코드 분석, 패킷분석 등의 콘텐츠를 다루지 않고 있다.

한국첨단기술진흥원 컨소시엄의 교육 과정은 “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 중 “공격” 카테고리의 4개 과목, “방어” 카테고리의 3개 과목, “기타” 카테고리의 1개 과목과 연관성을 가진다. “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 8개가 연관성을 가지므로 34%의 매핑률을 보이고 있다. 상대적으로 “공격” 카테고리 보다 “방어” 카테고리의 비중이 적은 편이지만 두 카테고리간의 밸런스는 균등한 편이다. 디지털 포렌식과 관련된 콘텐츠는 다루고 있지 않다.

한국정보보호교육센터의 교육 과정은 “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 중 “기초” 카테고리의 1개 과목, “공격” 카테고리의 4개 과목, “방어” 카테고리의 4개 과목, “기타” 카테고리의 3개 과목과 연관성을 가진다. “사이버보안 인력 교육훈련 표준 커리큘럼”에서 다루는 과목 개수를 기준으로 보았을 때 총 23개 중 12개가 연관성을 가지므로 52%의 매핑률을 보이고 있다. 교육 과목들이 “기초”, “공격”, “방어”, “기타” 카테고리에 걸쳐서 균등하게 분포되어 있는 편이다. 악성코드와 관련된 콘텐츠는 거의 다루고 있지 않다.

5. 개선된 사이버보안 교육과정 개발

본 연구는 우선적으로 사이버보안 교육 표준커리큘럼의 분류체계를 사이버보안 인력 및 지식체계를 토대로 분류하였다. 지식체계는 선행연구 분석을 토대로 기초, 공격, 방어, 기타 4개 대분류를 기준으로 하였다. 공격 분야는 적용 기술 분류에 따라 웹, 네트워크, 시스템, 모바일 등 4개 중분류에 따라 각각 세분화하였다. 방어는 일반적인 침해사고 대응 절차인 예방, 사전조치, 대응에 운영을 포함하여 4개 중분류를 적용하였다. 공격, 방어의 선수지식으로서 기초 분류를 제시하였으며, 공격, 방어 모두에 적용되는 요소들은 공통 분야로 별도 분류하였다. 다음의 Table 8은 지식체계 구성도에 대한 자세한 내용이다.

Table 8. Cyber Security Knowledge System Diagram

Category	Division	Section
Basic	-	Operating System Basics
		Designing and building network infrastructure
Attack	Web security	Web-based vulnerability analysis and attack
	Network Security	Wired network-based vulnerability analysis and attack
		Wireless network-based vulnerability analysis and attack
	System Security	Software vulnerability analysis and attack
		Embedded Vulnerability Analysis and Attack
	Mobile Security	Mobile-based vulnerability analysis and attack
Defence	Operation	security solution Operation
	prevention	Secure Coding
	Proactive Action	Vulnerability testing and analysis
	Response	Network traffic and packet analysis
		Shell code analysis
		Log analysis
		Malware detection and analysis

다음으로 사이버보안 인력 및 지식체계 정의를 토대로 각각의 과목의 세부 내용을 개발하였다. 각 과목은 개요 및 해당 교육을 통해 학습해야 할 내용, 그리고 각 챕터별 교육 지침을 포함하고자 한다. 지식체계에서 다루지는 않은 과목 가운데, 공격/방어 각각 시나리오 기반 실전 훈련, 보고서 작성과목을 추가하였다. 기타 과목 중에 최신기술 동향 분석 과목도 추가하였다. 자세한 표준 교육커리큘럼은 다음의 Table 9와 같다.

6. 결 론

사이버 위협의 고도화, 지능화에 따라 새로운 수법을 통해 사이버 침해사고로 인한 피해사례가 꾸준히 증가하고 있으며, 이에 따른 사이버대응 전문 인력의 수요 또한 급증하고 있다. 하지만, 사이버보안 교육프로그램 관련하여 정확한 업무 구분이나 직무에 대해서 제대로 파악이 되지 않고 있고 그로 인해 직무에 맞는 교육과정을 기획 및 제공하는 것이 쉽지 않은 상황이다. 정보보호 교육 서비스를 제공하는 다양한 기관, 단체들이 제각각 나름의 커리큘럼을 제시하고 교육을 진행해왔지만, 각각의 교육과정을 비교 검토할 기준조차 부재한 상황에서 교육과정에 대한 평가나 성과 예측은

Table 9. Standard Education Curriculum in Cyber Security

Category	Division	Section
Basic	Operating systems and systems	Operating system basics
	Network Infrastructure	Designing and building network infrastructure
Attack	Web Security	Web-based vulnerability analysis and attack
	Network Security	Wired network-based vulnerability analysis and attack
		Wireless network-based vulnerability analysis and attack
	System Security	Software vulnerability analysis and attack
		Embedded Vulnerability Analysis and Attack
	Mobile Security	Mobile-based vulnerability analysis and attack
	ETC	Scenario-based combat training
		Reports creating
Defence	Operation	security solution Operation
	Prevention	Secure Coding
	Proactive Action	Vulnerability testing and analysis
	Response	Network traffic and packet analysis
		Shell code analysis
		Log analysis
		Malware detection and analysis
	ETC	Scenario-Based Practice Defense Training
		Reports creating

교육 담당자 혹은 몇몇 전문가들의 주관적 평가에 의존할 수밖에 없다. 이에 따라 본 논문에서는 NICE의 workforce framework을 기준으로 사이버보안 인력이 갖추어야 할 지식체계를 정의하였다. 다음으로 이러한 지식체계를 반영하여 기존의 진행되어지고 있는 교육의 문제점을 해결할 수 있는 개선된 교육커리큘럼을 제시하였다. 기존의 정보보호 교육 서비스를 제공하는 다양한 기관, 단체들이 제각각 나름의 커리큘럼을 제시하고 교육을 진행해왔지만, 각각의 교육과정을 비교 검토할 기준조차 부재한 상황에서 교육과정에 대한 평가나 성과 예측은 교육 담당자 혹은 몇몇 전문가들의 주관적 평가에 의존할 수밖에 없었다. 본 연구는 많은 산업 분야에서 지식체계(BOK - Body of Knowledge) 형태로 해당 산업 분야가 요구하는 지식 요소들을 제시하고 이를 인력 채용, 선발 및 교육 훈련의 기초로 활용한다는 측면에서 사이버보안 분야 산업의 증진에 다양하게 활용 될 수 있을 것으로 기대한다.

References

[1] D. S. Lee, “A Study on Impact on Affect Students by Problem Solving Centric Lecture,” *Korean College Composition and Communication*, Vol.9, pp.229-247, 2014.

[2] S. W. Seo, W. J. Oh, and H. G. Kim, “Research on cyber Warfare Manpower Training Strategy for Securing Defense Information System Using AHP Analysis,” *Journal of Security Engineering*, Vol.12, No.2, pp.109-120, 2015.

[3] H. W. Lim, “Security Education and Research in Accordance with the Paradigm Shift in the Industry Security,” *Journal of Security Engineering*, Vol. 12, No. 6, pp.597-608, 2015

[4] H. M. Na, “Comparative Analysis on the Curriculums of Information Systems Security,” *Journal of The Korean Assocaition of Information Ecucation*, Vol.9, No.4, pp.661-671, 2005.

[5] J. Y. Park, “An Analysis on Training Curriculum for Educating Information Security Experts,” *Korea Journal of Business Administration,* Vol. 31, No.1, pp.149-165, 2012.

[6] C. Paulsen and E. McDuffie, “NICE: Creating a Cybersecurity Workforce and Aware Public,” *IEEE Security & Privacy*, Vol. 10, No.3, pp.76-79, 2012.

[7] D. Manson and R. Pike “The Case for depth in cyber security education,” *ACM Inroads*, Vol.5, No.1, pp.47-52, 2014.

[8] C. Paulsen and E. Mcduffie, “NICE: Creating a Cybersecurity Workforce and Aware Public,” *IEEE Security & Privacy*, Vol.10, No.3, pp.76-70, 2012.

[9] S. L. Pfleeger and D. D. Caputo, “Leveraging behavioral science to mitigate cyber security risk,” *Computers & Security*, Vol.31, No.4, pp.597-611, 2012.

[10] Y. Yasinsac, R. F. Erbacher, and D. G. Marks, “Computer forensics education,” *IEEE Security & Privacy*, Vol.99, No.4, pp.15-23, 2003.

박 원 형

e-mail : whpark@kdu.ac.kr

2003년 서울과학기술대학교 산업정보시스템공학과(공학사)

2005년 서울과학기술대학교 정보산업공학과(공학석사)

2009년 경기대학교 정보보호학과(박사)

2016년 성균관대학교 컴퓨터교육학과(박사수료)

2012년~현 재 극동대학교 산업보안학과 조교수/학과장

관심분야 : 산업보안, 침해사고대응, 인공지능, 빅데이터

안 성 진

e-mail : sjahn@skku.edu
1988년 성균관대학교 정보공학과(학사)
1990년 성균관대학교 정보공학과(석사)
1998년 성균관대학교 정보공학과(박사)
현 재 성균관대학교 컴퓨터교육학과 교수
관심분야 : 정보보호교육, 네트워크