Journal of The Institute of Electronics and Information Engineers Vol.54, NO.1, January 2017 https://doi.org/10.5573/ieie.2017.54.1.046
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2017-54-1-7

정보보안 전문인력 양성을 위한 교육과정 개발

(A Development of Curriculum for Information Security Professional Manpower Training)

이 문 구*

(Moongoo Lee©)

요 약

정보보안 분야에 대한 사회적 이슈가 고취되고, 인력수요전망이 매우 높아지고 있다. 이에 본 연구는 컴퓨터 및 네트워크 시스템 등 정보보안 분야에서 관련 직무에 종사하고 있는 실무자들로부터 정보보안에 필요한 지식을 설문조사하였다. 설문자료와 NICE에서 제시한 정보보호 직무체계 그리고 NCS 그리고 KISA에서 분류한 IT기술과 보안영역분류체계와의 연관성을 분석하였다. 분석한 자료를 기반으로 정보보안 분야에서 직무를 수행할 수 있는 전문 인력 양성을 위한 교육과정을 제안한다. 제안하는 교육과정은 2년제, 3년제 그리고 4년제 학제에 각각 적용할 수 있도록 하였다. 제안하는 교육과정은 정보보안 직무체계에서 종사하기를 원하는 많은 인력들이 주어진 학년기간 동안에 반드시 익혀야 될 과정들을 제안하였다. 제안한 각 교육단계는 관련분야와 밀접한 연계성을 갖고 반드시 필요한 교육이 실천될 수 있도록 각 교과목에 세부 지침을 명시하였다. 제안한 교육과정은 반드시 필요하고 기본이 되는 이론교육은 물론 이론과 함께 실시되어야 하는 실무교육을 함께 병행하도록 하여 자칫 이론중심의 교육이거나 단순한 명령어만을 익히는 실습에서 벗어나서 실무와 연계될 수 있는 다양한 시나리오기반의 해킹과 보안 방어 대응책에 대한 교육이 함께 이루어지도록 설계하였다. 이는 스펙이 아닌 직무능력을 갖추어 관련 자격증을 취득하는데 도움이 될 수 있을 뿐만 아니라 차세대 융합형 정보보안 전문인력 양성에 도움이 될 수 있기를 기대한다.

Abstract

Social attention to information security field is inspired, and manpower demand forecast of this area is getting high. This study surveyed information security knowledge of practitioners who work in a field of information security such as computer and network system. We analyzed a connection between survey data, information protection job system that was suggested by NICE, IT skills that NCS and KISA classified and security field classification system. Base on data that analyzed, this study suggests a curriculum that trains professional manpower who perform duties in the field of information security. Suggested curriculum can be applied to 2 year college, 3 year college and 4 year college. Suggested curriculum provides courses that students who want to work in a field of information security must learn during the college. Suggested courses are closely connected to a related field and detailed guideline is indicated to each course to educate. Suggested curriculum is required, and it combines a theoretical education that become basis and a practical education so that it is not weighted to learn theory and is not only focusing on learning simple commands. This curriculum is established to educate students countermeasures of hacking and security defend that based on scenario that connected to executive ability. This curriculum helps to achieve certificates related to a field more than paper qualification. Also, we expect this curriculum helps to train convergent information security manpower for next generation.

Keywords : Information Security 정보보호, Skills and Competency Framework 직무 능력 체계, Curriculum 교육과정, Computer Emergency Response Team컴퓨터 침해 사고 대응반

Ⅰ. 서 론

기존의 정보통신기술뿐만 아니라 클라우드 컴퓨팅, 스마트플랫폼, 빅 데이터 등 새로운 정보통신기술의 발전과 활용은 우리의 삶을 풍요롭게 하는 기반이 되고 있는

* 정회원(평생회원), 김포대학교IT학부 사이버보안과
(Div.of IT, Dept. of Cyber Security, Kimpo University)
© Corresponding Author(E-mail : yeon0330@kimpo.ac.kr)
Received ; October 30, 2016 Revised ; November 16, 2016
Accepted ; December 22, 2016

정보화의 순기능이라고 할 수 있다. 정보통신에 대한 의존도가 상당히 높은 우리나라는 대부분의 가구에서 인터넷 접속이 가능하며, 인터넷 이용률과 인터넷 이용자 수 등이 세계 최고 수준이다. 전자상거래를 비롯하여 각종 경제활동에서 정보통신의 활용이 절대적이며, 사회에 필수적인 기반시설의 제어에도 정보통신이 폭넓게 활용되고 있다[1]. 반면에 정보통신의 급속한 발전으로 정보에 대한 높은 의존도는 정보에 대한 침해사고 발생 시 우리의 삶에 직접적인 위해를 가하게 되며, 이는 개인과 기업에 한정되는 위해가 아니라 국가를 대상으로 하는 공격 형태로 확장되는 정보화의 역기능으로 인한 피해도 더욱 지능화 되고 첨단화되고 있다. 특히 유, 무선 통신기술의 발전과 정보시스템에 대한 의존도가 높은 현실은 보안문제에 대한 방어 시스템의 구축과 취약점 분석에 대한 대응책 등과 이를 해결하기 위한 문제가 중요한 과제로 떠오르게 된다. 그러므로 이러한 정보보안 분야에 대한 사회적 이슈는 곧 우수한 정보보호를 위한 인력을 양성하고 적재적소에 채용하여 활용하는 것은 정보보호 발전의 중요한 요소가 될 것이다.

이에 본 연구는 정보보안 분야에서 개인의 역량(Competency)에 맞는 직무체계 (Skills Framework) 자료와 실무자들로부터 정보보안에 필요한 지식을 설문조사를 기반으로 전문 인력 양성을 위한 교육과정을 제안한다. 제안하는 교육과정은 정보보안 직무에서 종사하기를 원하는 많은 인력들이 주어진 기간 동안에 반드시 익혀야 될 과정들과 관련분야와 밀접한 연계성을 갖고 반드시 필요한 교육이 실천될 수 있도록 세부지침을 각 교육단계에 명시하였으며, 반드시 익혀야 될 이론교육은 물론 실무교육을 함께 병행하도록 설계하였다.

Ⅱ. 관련 연구

1. 정보 보호 직무체계

직무체계(Skills Framework)란 산업현장의 직무에 근거하여 직무분류 및 직무수준을 설정하고 직무 수준별 수행기준을 제시하는 것으로써, 현장 수요에 기초한 교육훈련과정의 개발, 자격 및 인력수급 체계 등을 위한 인프라 정비의 핵심 요소이다[2]. 본 연구에서는 정보보호진흥원(KISA)의 정보보안 직무체계와 국가직무능력표준(NCS) 그리고 미국 사이버보안교육(NICE)에서 제시간 직무체계자료를 참조하여 산업체에서 필요로 하는 직무에 따른 역량을 조사하였다.

가. KISA 정보보안 분류체계

정보보호 직무체계 개발 및 인력수급 실태 조사로 는에서는 2008년 한국인터넷진흥원(KISA)의 위탁을 받아 한국침해사고대응팀협의회(CONCERT)에서 제시한 자료는 [표 1]과 같이 정보보호 직무를 분류하고 있다[3].

표 1. KISA 정보보안 분류체계
Table1. Information Security Classification Framework based on KISA.

직무군	세부 직무
전략 및 계획	위험분석
	정보보호 정책 및 계획 수립
	개인정보보호 관리
마케팅 및 영업	마케팅 메니지먼트
	기술 영업
연구개발 및 구현	연구개발
	구현
교육 및 훈련	일반인 및 사용자 교육
	전문가 교육
관리 및 운영	프로젝트 관리
	정보인프라 보안관리
	물리적 보안
사고 대응	모니터링 및 대응
	디지털 포렌식
	업무지속성 관리
평가 및 인증	평가인증 및 품질보증
	정보시스템 보안 감사

나. NCS 정보보안 분류체계

NCS(National Competency Standard : 국가 직무능력표준) 정보보안 분류체계[4]는 [표 2]와 같이 대분류, 정보기술 중분류, 소분류, 세분류로 분류되어 있다.

표 2. 2016 NCS 정보보안 분류체계
Table2. Information Security Classification Framework based on 2016 NCS.

분 류 체 계			
대분류	중분류	소분류	세분류
20. 정보통신	01. 정보기술	정보기술 전략·계획	정보기술전략
			정보기술컨설팅
			정보기술기획
			SW제품기획
			빅데이터 분석
			IoT응용서비스기획
		정보기술 개발	SW아키텍처
			응용SW엔지니어링
			임베디드SW엔지니어링
			DB엔지니어링
			NW엔지니어링
			보안엔지니어링
			UI/UX엔지니어링
			시스템SW엔지니어링
		정보기술 운영	IT시스템관리
			IT기술교육
			IT기술지원

		정보기술 관리	IT프로젝트관리
			IT품질보증
			IT테스트
			IT감리
		정보기술 영업	IT기술영업
			IT마케팅
		정보보호	정보보호관리·운영
			보안사고분석·진단
			정보침해사고대응

다. NICE 정보보안 직무체계

NICE에 제시된 정보보안 직무체계에 따르면 7개 직무와 각 직무별로 세부 직무로 분류하여 비교적 실무의 직무와 연계하는데 많은 연관성이 있었다[2, 5].

표 3. NICE 정보보안 직무체계
Table3. A Suggested on NICE Information Security Competency Framework.

Categories (직무군)	Speciality areas (세부직무)
Security Provision (정보보호 제품 및 시스템개발)	Information Assurance Compliance (정보시스템 인증)
	Software Assurance and Security Engineering (소프트웨어 개발 및 정보보호 공학기술)
Securely Provision (정보보호 제품 및 시스템 개발)	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 (네트워크 보안)	Computer Network Defense Analysis (네트워크 위협분석)
	Computer Network Defense Infrastructure Support (기반시설 네크워크 방어)
	Incident Response (사고대응)
	Vulnerability Assessment and Management (취약점 분석 및 관리)
Oversight and Development (정보보호 총괄 및 개발 지원)	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 및 유지보수)	Customer Service and Technical Support (고객 관리 및 지원)
	Data Administration (데이터 관리)
	Knowledge Management (지식 경영)
	Network Services(네크워크 서비스)
	System Administration (시스템 관리)
	Systems Security Analysis (시스템 보안 관리)
Investigate (사이버 범죄)	Digital Forensics (디지털 포렌식)
	Investigation (사이버 수사)
Collect and Operate (정보 수집 및 운영)	Collection Operations (데이터 수집 관리)
	Cyber Operations (사이버 범죄 및 테러 관련 증거 수집)
	Cyber Operations Planning (사이버 운영 계획)

Ⅲ. 정보보안 교육과정

1. 정보보안 직무와 역량

연구는 정보보안 분야의 직무에 종사하는 산업체에서 요구하는 직무와 역량에 따른 지식을 [표 4]에 정리하였다. 산업체에서 정보보안 전문 인력에 대하여 필요로 하는 인력에 대한 역량은 원만한 대인관계능력과 기본적인 문서작성능력을 가장 기본으로 갖추고 있어야 한다고 요구하였다. 그리고 모든 보안 시스템은 정보통신을 기반으로 하므로 TCP/IP 기반의 네트워크와 통신보안 기술을 기본으로 갖추고 있어야 한다는 답변이 가장 많았으며, 주목할 점은 서버 보안 시스템 구축 능력과 보안 취약점 분석 능력 등의 순으로 나타났다. 특이 사항은 계속 발전하는 정보통신 기술에 발맞추어 새로운 환경 즉 빅데이터 기술, 클라우드 서버, HTML5기반의 웹 환경과 IPv6주소체계, 종합보안관리시스템(ESM), 보안장비(VPN), DDoS보안장비 등에 대한 실습이 이루어졌는지 혹은 관련 분야의 지식에 대한 요구가 있었다.

표 4. 산업체에서 요구하는 정보보안 직무 역량
Table4. Information Security Skills and Competency Needed in the Industry.

정보보안 직무와 역량
개인정보보호와 프라이버시 및 윤리이해
보안장비 및 관제센터 운영능력
통신프로토콜과 통신보안기술에 대한 이해
PC 보안 기술에 대한 능력
웹 환경(웹언어, 웹3.0, IPv6 등)에서의 보안 분석 및 이해
보안 취약점 분석 능력
서버 보안 시스템 구축 능력
시스템 구조 분석 능력
데이터베이스 백업, 정합, 무결성에 대한 이해
위험관리(위험분석 및 평가) 능력
원만한 대인관계능력
문서작성(워드프로세서 프리젠테이션 기법 등) 능력
정보보호 관련 법률 및 규정에 대한 이해

디지털 포렌식의 이해와 기술
정보보호시스템 평가 및 인증에 대한 이해
암호알고리즘과 수리능력
다양한 플랫폼에 대한 이해
운영체제와 시스템 구조에 대한 지식
영어 및 외국어능력

2. 정보보안 직무와 역량 분석

설문자료는 미국사이버보안교육(NICE)에서 제시한 정보보호 직무체계, NCS에서 분류한 IT기술과 보안영역분류체계 그리고 KISA 의 직무 분류체계와 관련분야 참고문헌 등을 기반으로 연관되는 공통항목을 기반으로 작성하여 배포 하였다[6].

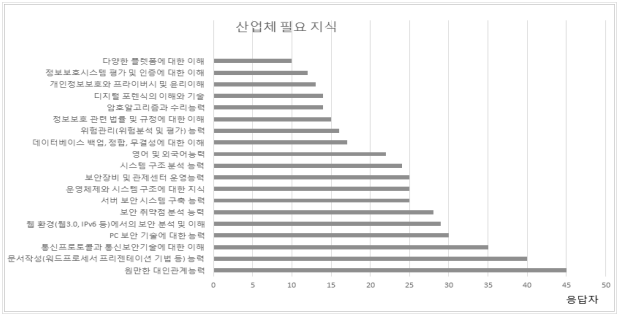

그림 1. 산업체 필요지식
Fig. 1. Knowledge of Needed in the Industry.

정보보안 직무에 종사하는 산업체 담당자들로부터 받은 자료를 기반으로 항목별로 그래프[그림 1]로 정리하였으며, 본 설문자료는 수도권에 소재하는 30여개 관련 업체의 직무에 종사하는 50명을 대상으로 조사한 자료를 기반으로 정리하여 오차범위 ±5%p이며 95%의 신뢰도를 가진다. [표 5]는 산업체에서 요구하는 정보보안 직무 역량을 순위별로 정리하였다.

표 5. 산업체에서 요구하는 정보보안 직무 역량
Table5. Information Security Skills and Competency Needed in the Industry.

순위	산업체 필요 지식
1	원만한 대인관계능력
2	문서작성(워드프로세서 프리젠테이션 기법 등) 능력
3	통신프로토콜과 통신보안기술에 대한 이해
4	PC 보안 기술에 대한 능력
5	웹 환경(웹3.0, IPv6 등)에서의 보안 분석 및 이해
6	보안 취약점 분석 능력
7	서버 보안 시스템 구축 능력
8	운영체제와 시스템 구조에 대한 지식
9	보안장비 및 관제센터 운영능력
10	시스템 구조 분석 능력
11	영어 및 외국어능력
12	데이터베이스 백업, 정합, 무결성에 대한 이해
13	위험관리(위험분석 및 평가) 능력
14	정보보호 관련 법률 및 규정에 대한 이해
15	암호알고리즘과 수리능력
16	디지털 포렌식의 이해와 기술
17	개인정보보호와 프라이버시 및 윤리이해
18	정보보호시스템 평가 및 인증에 대한 이해

3. 정보보안 직업군과 직무 중요도

정보보안 직무[7]와 역량에 따른 직업군과 관련지식의 수요 전망을 조사하여 정성적 평가결과를 [표 6]에 제시하였다. 직업군의 선정은 한국표준직업분류(KSCO) 기준자료를 기반으로 설정하였으며, 설문조사 결과를 보면 악성프로그램치료사(맬웨어치료사, 악성코드전문가)와 컴퓨터바이러스치료사 (컴퓨터바이러스기술자)에 대한 수요전망이 가장 높았고, 웹 프로그램 개발자와 네트워크 설계자에 대한 중요도가 가장 낮았다. 정보보안 직무와 역량에 따른 관련지식을 갖춘 인력의 직업군과 직무의 중요도, 직업전망, 취업성과, 전공 비전 교육효과성 등의 항목을 조사하여 교육과정 개발을 위한 직업군으로 선정하였으며, [표 7]은 관련 직업군을 기반으로 인력양성 유형에 대한 상세 내용을 NCS를 기반으로 정리하였다.

표 6. 정보보안 직업군과 직무 중요도
Table6. Information Security Job Cluster and Competency Importance.

선정 기준 / 직업(군)	직무 중요도	직업 전망	취업 성과	전공 비전	교육 효과성	계	선정
보안프로그램개발자	5	5	4	5	5	24	선정
국가사이버안전요원	5	4	5	5	5	24	선정
악성코드 분석 및 치료사 (맬웨어치료사,악성코드 전문가)	5	5	5	5	5	25	선정
정보보호 프로그래머 (백신프로그램 개발자)	5	4	4	4	5	22	선정
컴퓨터바이러스치료사 (컴퓨터바이러스기술자)	5	5	5	5	5	25	선정
전산보안관제원 (보안관제요원, 전산보안관제요원)	5	5	5	4	5	24	선정
침해대응전문가(cert) (컨트롤시스템엔지니어: Control System Engineer)	5	4	5	5	5	24	선정
사이버수사요원 (디지털포렌식수사관)	5	4	5	5	5	24	선정
웹 프로그램 개발자	4	3	3	4	5	19	미선정
네트워크 설계자	4	3	3	4	5	19	미선정

표 7. 정보보안 인력양성 유형과 주요 직무내용
Table7. A type of Information Security manpower training and Major Competency Contents.

인력양성 유형	주요 직무내용
보안프로그램개발자	- 다양한 해킹방법을 인터넷을 이용하여 조사·연구한다. 보안을 점검할 수 있는 도구로서 시스템의 보안 상태를 점검하기 위한 시험도구(test tool)를 개발한다. - 해킹(hacking)방법을 가상으로 시뮬레이션하여 특정 인터넷 사이트의 보안 상태를 직접 침투함으로써 보안 상태를 점검하고 운영체계(O/S) 버전의 업그레이드 등 필요한 해결책을 제시한다.
국가사이버안전요원	- 국가기관, 산업체, 연구소 등 주요 전산망의 안전성 여부를 확인하여 사이버공격 징후를 탐지한다. 위험요소가 포착될 경우 각 기관에 알려 사이버테러를 예방할 수 있도록 조치한다. - 사이버 공격에 대한 진원지 및 의도를 파악하고, 재발방지를 위한 보안기술을 지원한다. - 보안취약점을 발굴하고 해킹 취약성을 진단하여 보안책을 지원한다. 사이버테러 발생 시 현장 또는 원격으로 사고원인을 분석하고 복구한다. - 사이버 보안교육, 모의훈련 등을 실시한다. - 사이버위협 정보분석, 보안기술 연구, 국내외 사이버위협 동향, 보안취약성 분석 등의 업무를 수행한다. 사이버테러 발생 시 유관기관과 합동으로 복구작업을 한다.
악성코드 분석 및 치료사 (맬웨어치료사,악성코드전문가)	- 정상적인 컴퓨터 사용을 방해하는 악성프로그램(멀 웨어)을 분석한다. - 컴퓨터에 설치되는 프로그램들을 연구하여 사용자가 의도하지 않은 프로그램 자동 설치, 사용자 정보 전송, 컴퓨터 리소스 사용, 무분별한 광고 노출, 지속적인 결제 요청, 해킹 위험 등이 있는지 판단한다. - 악성프로그램이라는 판단이 들면 해당 프로그램을 삭제 및 치료하는 방법과 해당 프로그램이 다시 설치되지 않도록 예방하는 방법을 연구한다. - 악성프로그램을 치료하는 프로그램에 치료 및 예방법을 적용한다. - 바이러스 치료용 프로그램과 같은 프로그램에 기능이 탑재되기도 한다.
정보보호 프로그래머 (백신프로그램 개발자)	- 정보보호 산업의 동향을 파악한다. 고객이 요구하는 수준의 정보보호 제품을 기획한다. 정보보호 제품을 설계한다. 암호화 알고리즘을 개발한다. - 인증서를 이용한 제품을 개발한다. 인증서를 발행하는 프로그램을 개발한다. 정보보호 기술 및 규격에 관한 표준화 작업에 참여한다. - 외부 네트워크로부터의 불법적인 침입을 탐지하기 위한 시스템과 침입을 방지하기 위한 방화벽을 개발한다. - 컴퓨터 바이러스 백신 프로그램을 개발·보급한다.
컴퓨터바이러스치료사 (컴퓨터바이러스기술자)	- 디버그(debug) 같은 바이러스 분석 툴(tool)을 이용하여 메모리 감염 방법, 다른 파일 감염 방법 등 컴퓨터 바이러스가 가지고 있는 특징을 분석한다. 감염 증상 외에 파괴 증상이 있는지 또는 특정한 날에만 활동을 하는지 등도 분석한다. 분석이 끝나면 컴퓨터 바이러스의 치료 데이터를 만든다. - 메모리를 치료하는 방법, 파일을 치료하는 방법, 부트(boot) 바이러스인 경우 원래 부트가 있는 위치 등 컴퓨터 바이러스를 치료하기 위한 모든 정보를 찾는다. - 기존 백신 프로그램에 컴퓨터 바이러스를 치료하기 위한 데이터를 추가한다. - 컴퓨터 바이러스에 관해 사용자들을 대상으로 상담하고 컴퓨터 바이러스를 치료할 수 있는 방법을 설명하거나 해결 방법을 제시한다.
전산보안관제원 (보안관제요원, 전산보안관제요원)	- 보안관제센터(IT자원 및 보안시스템에 대한 운영 및 관리를 전문적으로 수행하는 센터) 및 보안관제서비스센터(MSS, Managed Security Service, 고객이 보유한 정보자산을 보호해주는 보안관리대행서비스)에서 실시간으로 관제화면을 통해 침해위협을 탐지한다. - IDS(Intrusion Detection System, 정보시스템의 보안을 위협하는 침입행위가 발생할 경우 이를 탐지하고 대응하는 시스템), IPS(Intrusion Prevention Systems, 침입차단 시스템) Anti-DDos(Anti-Distributed Denial of Service, DDoS(분산서비스 거부 공격) 방어 시스템), 웹 방화벽(Web Application Firewall, 웹 애플리케이션 서비스 보호 방화벽) 등 보안관제 프로그램을 사용하여 관제한다. - 보안위협이 발생한 경우 대응팀과 협조하여 네트워크와 시스템의 침입을 차단하는 등 발생된 보안위협에 대응한다. 고객 기업에 파견된 경우, 파견된 기업(클라이언트)의 보안솔루션을 관리한다. - 원격으로 관제하는 경우, 원격으로 네트워크 보안장비에 대한 관제업무를 수행하기도 한다.
침해대응전문가(cert) (컨트롤시스템엔지니어: Control System Engineer)	- 고객사의 서버 현황을 실시간으로 모니터한다. 인가되지 않은 서버에 대한 접근을 차단한다. - 시스템 불통으로 인한 고객의 전화에 응대한다. 전 근무자로부터 상황에 대하여 인수인계 받는다. 서버상의 오류 발생 시 수정(디버깅)한다.
사이버수사요원 (디지털포렌식수사관)	사이버수사 요원은 데이터복구, 모바일데이터 분석, 영상/음성 처리등의 디지털증거의 분석 능력으로, 사이버테러대응센터(CTRC, Cyber Terror Response Center)에서 업무를 수행한다.

표 8. 정보보안 전문인력 양성을 위한 교육과정
Table8. Curriculum for Information Security Professional Manpower Training.

과정 / 학년	학기	정보보안 일반과정	보안프로그램 개발과정	시스템 보안과정	네트워크 보안과정	창의적 융합 보안과정	산학 연계 실무과정	
1학년	1	정보보호 개론 (암호학, 위험분석 등)	알고리즘과 자료구조	운영체제와 보안	정보통신과 네트워크	데이터베이스 개론과 보안	문서작성 실무 (HWP, Excel, PPT)	
	2	웹기초 (웹기반언어 이해, 웹기반 인코딩)	프로그래밍언어 (C++)	서버구축 (LINUX 실무)	네트워크 프로토콜	디지털 포렌식 개요	보안특강	
2학년	1	웹응용 (아파치 서버+Asp,Jsp,Php+ Mysql)	프로그래밍언어실무 (C++)	서버 관리 (- 파일 시스템 아키텍처 분석 (FAT, NTFS, EXT - 메모리 분석 - Exploit의 이해, Shellcode 분석)	LAN구축과 NOS실무	디지털 포렌식 실무	보안특강 실무	(2년제) 현장실습
	2	웹 모의해킹과 취약점분석 (시나리오기반의 웹 모의해킹)	악성코드 분석과 제작 (악성코드제작기법)	시스템 해킹과 대응	네트워크보안 공격 및 대응 (각종 스푸핑 공격 및 대응 (ARP, DNS, DHCP, DoS & DDoS)	PC 보안	(2년제 졸업작품) 보안 프로젝트	
3학년	1	애플리케이션 보안 실무 (웹 어플리케이션 보안대책 수립)	백신프로그램제작 (파이선 이해와 설치)	통합보안관제	모바일 보안실무	캡스톤 디자인설계	(3년제) 현장실습	
	2	재난복구 대응	백신 암,복호화 도구개발 (백신 엔진 모듈의 암호화, 복호화, 파이썬 실행 파일로 py2exe, pyinstaller 이용 방법)	클라우드보안	빅데이터보안	캡스톤 디자인구현 (3년제) 졸업작품		
4학년 (전공심화)	1	암호학 이해	백신엔진 커널제(백신 엔진 모듈 우선순위, 백신 엔진 커널 모듈의 개발, 네이티브 라이브러리 개발)	침해대응 실무	IT 거버넌스의 이해	사이버범죄와 보안	정보보호 관리 및 법률	
	2	암호화 응용기술	악성코드 엔진개발 (PE 엔진, OLE 엔진 -스크립트 엔진)	정보보호 표준	정보보안 특론	프로젝트 관리		

[표 8]은 정보보호 전문인력 양성을 위한 교육과정개발을 위하여 각 학제(2년제, 3년제, 4년제)에 맞도록 교육과정을 개발하였다. 교육과정은 과목별로 필요한 세부교육내용을 함께 제안하였으며, 이론과 실무교육이 1: 2의 비율로 진행되도록 교과목을 배정 하였다.

Ⅳ. 결 론

본 연구는 정보보안 전문인력 양성을 위하여, 산업계 NICS의 직무체계, KISA 직무체계, NCS직무체계를 기반으로 설문조사를 수도권 30여개 업체 관련업무 종사자 50명을 대상으로 설문조사를 실시하여 산업체에서 요구하는 정보보안 직무 역량의 순위를 조사하였으며, 정보보안 직무와 관련한 직업군과 교육에 중요도에 대한 정성적 평가 자료로 정보보안 인력양성 유형을 선정하고 그에 대한 주요 직무내용을 정리하였다. 정보보안 인력 양성의 유형에 맞는 교육을 실천하기 위한 교육과정을 2년제, 3년제 그리고 4년제 학제의 교육과정을 개발하였으며 실무교육이 단순한 명령어만을 익히는 실습에서 벗어나서 현장에서 원하는 실무와 연계될 수 있는 다양한 시나리오기반의 모의 해킹, 악성코드, 등을 기반으로 보안 방어 대응책에 대한 교육이 함께 이루어지도록 한다. 이는 차후 정보보안 전문 인력을 양성하는데 도움이 되기를 기대한다.

REFERENCES

[1] “International Information Security White Paper”, 2015. KISA, NIS, Ministry of Science, ICT and Future Planning
[2] Hyo-Jung Jun, Tae-Sung Kim, Jinho Yoo, Sang-Ho Gee, “Development of Skills Framework for Information Security Workforce”, Journal of the Korea Institute of Information Security and Cryptology 19(3), 2009.6, 143-152 (10 pages)
[3] Wongyu Lim, Seongjin Ahn, “A Study on Improvements of the Information Security Department via the Curriculum Analysis”, The Korea Association of Computer Education. Vol. 16, no. 6, pp. 71-80, Nov. 2014.
[4] http://www.ncs.go.kr/ncssearch
[5] NIST. National Initiative for Cyber-security Education, 2011.
[6] Dong-woo Kim, Seung-woan Chai, Jae-cheol Ryou, “A Study on Domestic Information Security Education System”, Journal of the Korea Institute of Information Security and Cryptology 23(3), 2013.6, 545-559,(15 pages)
[7] Onechul Na, Hyojik Lee, Soyung Sung, Hangbae Chang, “Security Knowledge Classification Framework for Future Intelligent Environment”, The Jounal of Society for e-Business Studies 20(3), 2015.08, 47-58 (12 pages)

저 자 소 개

이 문 구(정회원)
1984년 숭실대학교 전자계산학(학사)
1993년 이화여자대학교 대학원 전산교육학(석사)
2000년 숭실대학교 대학원 컴퓨터(공학 박사)

2000년 3월~2016년 현재 김포대학교 스마트 IT학부 사이버보안과 정교수
<주관심분야: 정보보안, 인터넷 보안, 시스템 보안, 네트워크보안, 전자상거래 보안>