

## 사이버보안 교육훈련 전문 인력의 역량에 관한 연구

엄정호\*

### *A Study on the Capability of Cyber Security Education and Training Professional Personnel*

Eom Jungho

#### 〈Abstract〉

This research proposed the necessary capability of cyber security professional personnel for cyber security education and training. Cyber security professional personnel were required specialized capability because the curriculum of cyber security education and training is structured around practice and training. Based on the knowledge, skills, and attitudes of professors, we derive candidate capabilities and index through the results of precedent research. As a result, we derived capability such the candidate capability group as teaching qualification, expert knowledge, practical ability, lecture ability, and research ability, and detailed capability index was derived accordingly. Finally, based on the questionnaire results of the professors related to the information security, it was determined that the capability required for the cyber security education and training professional personnel were expert knowledge, practical ability, and lecture ability. Among the capabilities, executive ability means that they have to fulfil abundant executive experience due to the high proportion of practical training due to the characteristics of cyber security education and training.

Key Words : Cyber Security, Education&Training, Security Professional, Capabilities, Capability Index

### I. 서론

국가·공공기관의 정보보안을 담당하는 인력들은 보안 역량을 향상시키기 위해서 전문적인 사이버보안 교육기관에서 주기적으로 교육훈련을 받는다. 이들은 현업에서 정보보안 직무를 수행하고 있기 때문에 이론보다는 실무에 직접 적용할 수 있는 실습과 훈련 위주의 교육훈련을 원한다. 그래서 사이버보안 교육훈련을 담당하는 교육기관의 교육훈련 과정은

대부분이 실습과 훈련 실행으로 구성된다. 대표적인 사이버보안 교육기관인 사이버안전훈련센터의 교육 훈련 과정 대부분이 실습과 훈련으로 구성되어 있다 [1]. 한국인터넷진흥원의 최정예 사이버 정보보안 인력양성 과정도 1차 과정에서 훈련생의 실습 위주로 진행되고 2차 과정에서는 주요 사이버공격 사례를 기반으로 공격과 방어로 구분하여 훈련을 진행한다[2].

사이버보안 교육훈련을 담당하는 교수(강사)들도 이론보다는 전문 지식과 실무 역량을 갖춘 전문가로 구성된다[3]. 하지만, 이러한 교육훈련 인력들에 대해

\* 대전대학교 군사학과&안전융합학부 부교수

서 정확하게 요구되는 역량을 정의한 연구는 드물다. 교수 역량에 대한 다양한 연구논문을 분석해 보면, 교수의 역량은 교육을 효과적으로 진행하기 위한 지식, 기술, 태도 등으로 이루어진 집합체로 정의하고 있다[4]. 이러한 연구들은 대부분 대학교수들의 역량에 치중되어 있어서 사이버보안 교육훈련 전문 인력에게 요구되는 역량과는 구분이 된다. 예를 들면, 대학교수는 교육대상자가 학생이기 때문에 이론교육을 위한 지식도 중요하다. 하지만, 사이버보안 교육훈련 전문 인력들은 교육대상자가 대부분의 현업에서 정보보안 직무를 수행하는 인력이기 때문에 실제로 발생한 사이버공격을 대응해야 하기 때문에 전문 지식과 실무 역량이 필요하다. 본 논문에서는 사이버보안 교육훈련 전문 인력에게 요구되는 역량을 선행연구와 설문조사 결과를 토대로 도출하였다.

본 논문은 2장에서 사이버보안 교육훈련 현황을 살펴보고, 3장에서는 역량과 지표 개발 절차에 따라 사이버보안 교육훈련 전문인력의 역량과 지표를 도출한다. 마지막으로 4장에서 결론을 맺는다.

## II. 사이버보안 교육훈련 현황 분석

### 2.1 사이버보안 교육훈련 현황

대표적인 사이버보안 교육훈련은 사이버안전훈련센터의 사이버위기 대응훈련과 한국인터넷진흥원의 최정에 사이버 정보보안 인력양성 과정이다. 사이버위기 대응훈련 과정[5]은 과정소개, 훈련 설명, 훈련 실습으로 구성되며, 훈련 첫날에 과정소개와 훈련 설명이 진행되고 나머지 훈련기간 동안 실습과 훈련이 진행된다. 다음 표 1은 훈련 과정 단계를 보여준다.

훈련과정은 이론보다는 공격과 방어의 행동절차를 습득할 수 있도록 실습과 훈련으로 진행한다. 교수는 훈련과 관련된 기초적인 설명만 하며, 교육생은 과정

<표 1> 사이버 위기 대응훈련 단계

단계	내용
과정소개	이론, 사례, 공격/방어 설명
훈련설명	훈련절차/환경 설명, 공격절차 소개, 공격 및 방어 도구(장비) 사용법 설명
훈련실습	훈련절차에 따른 실험 * 준비-탐지-초동조치-분석-복구-보안강화

초기에 대응절차를 실습하고 중/후반에는 훈련 시나리오에 따라서 실제적으로 대응을 훈련한다.

최정에 사이버 정보보안 인력 양성 과정[6]은 1, 2차로 구분하여, 1차는 외부 교육운영기관(학원)에서 이론과 실기 교육과정을 진행하고 2차는 한국인터넷진흥원(KISA) 사이버 훈련장에서 진행된다. 1차 과정에서는 교육생의 공격 분석 능력 향상을 위해서 네트워크 패킷 분석, 악성코드 분석 등을 실습하고 2차 과정에서는 실제 발생했던 주요 사이버 공격 사례를 기반으로 훈련 시나리오를 제작하여 공격과 방어로 훈련을 진행한다. 또한 시뮬레이션 훈련과 침투팀과 방어팀으로 구성된 모의훈련이 교육생 중심의 팀 프로젝트 방식에 의해 진행된다.

### 2.2 사이버보안 교육훈련의 특징

사이버안전훈련센터와 한국인터넷진흥원의 사이버보안 교육훈련 과정을 분석하면 다음과 같은 특징을 알 수 있다.

첫째, 교육생은 보안 초보자가 아닌 소속기관(업)에서 정보보안을 담당하는 인력 또는 컴퓨터나 정보보안 관련 전공자나 취업 희망자 등으로 정보보안의 기초적인 지식을 갖고 있다. 보안 전공자나 취업 희망자 또는 보안 실무나 관리자를 대상으로 하기 때문에 교육훈련 과정이 이론과 지식을 학습하기 보다는 실무에 적용할 수 있는 기술 중심으로 이루어진다.

둘째, 이론 교육보다는 실습과 훈련 중심으로 이루어

어진다. 현업 정보보안 실무자가 교육훈련 대상일 경우에는 교육과정이 실무에 적용할 수 있거나 알고 있는 지식을 활용하여 실제 사이버공격이 발생할 경우에 어떻게 방어하는지에 대한 훈련과정으로 편성된다. 즉, 교육과정의 교육 목표가 이론 지식을 학습하는 것이 아니라 실무능력 배양에 중점을 두고 있기 때문에 실습과 훈련 위주로 교육훈련이 진행된다.

셋째, 실습 과정은 보안 기법을 실습하는 단계와 훈련 시나리오에 의해서 교육생이 주도적으로 보안 기법을 적용하는 단계로 구성된다. 우선, 교수가 기본적인 보안 기술을 설명하고, 학생이 실습을 진행한다. 그리고 보안 기술 실습이 끝나면 학생 스스로가 훈련 시나리오에 따라 보안 기술을 공격 절차대로 대응할 수 있도록 적용하는 훈련으로 진행된다.

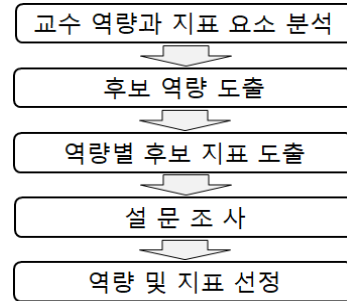
마지막으로, 교수자는 보안 실무의 경험이 있거나 담당과목의 전문가로 구성된다. 사이버안전훈련센터의 경우는 센터 소속의 교수나 연구소의 연구원으로 교육이 진행된다. KISA 아카데미 경우에는 해당 교과목의 전문 지식과 실무 경험이 있는 외부 전문가를 활용하기도 한다. 실습과 훈련을 진행하기 위해서는 이론을 교육하는 교육 전문가보다는 실무 능력을 겸비하거나 연구경험이 풍부한 전문가가 적합하다.

### III. 사이버보안 교육훈련 전문인력의 역량과 지표

#### 3.1 역량과 지표 개발 모델

사이버보안 교육훈련 전문인력의 역량과 지표를 도출하기 위해서 군 교육담당자의 교수역량 모델[7]을 기반으로 아래 그림과 같이 역량과 지표 개발을 진행하였다.

교수 역량 모델[8,9], 최근 공학 교수, 소프트웨어 교육자, 직업훈련 및 능력개발훈련 교수들에게 요구



<그림 1> 역량과 지표 개발 모델

되는 역량 연구 자료[4,10,11], 그리고 NICE Cybersecurity Workforce Framework (NCWF)[12]를 분석하여 교수의 역량과 지표를 분석하였다.

후보 역량과 지표 도출은 기존 연구문헌에서 가장 많이 제시한 역량과 정보보안 실무자의 역량을 포함하여 후보 역량을 도출한다. 그리고 역량별로 보안 기술의 실행능력을 갖출 수 있는 지표를 추출하였다.

설문조사는 대학의 컴퓨터공학과를 비롯한 정보보안학, 사이버안보학 등에서 재직하고 있는 교수를 대상으로 하였다. 역량은 대부분의 선행연구에서 역량을 3가지로 분류하여 본 연구에서도 동일하게 결정하였으며, 역량별 지표는 4가지로 결정하였다.

최종 사이버보안 교육훈련 전문인력의 역량과 역량 지표는 설문조사 결과를 기반으로 3개의 역량과 4개의 역량별 지표를 선정하였다.

#### 3.2 후보 역량 및 지표 도출

사이버보안 교육훈련 전문인력에 요구되는 후보 역량은 기존의 연구[8-10]와 NICE Cybersecurity Workforce Framework (NCWF)에서 제안한 사이버 전문 인력의 요구사항인 지식(Knowledge), 기술(Skills), 능력(Abilities) 중에서 능력을 포함하여 아래 표와 같이 도출하였다.

<표 2> 사이버보안 교육훈련 전문 인력의 후보 역량

후보역량	내용
교수 자질	교수자로서의 역할을 수행할 수 있는 소명의식, 인격, 교육관 등을 지니고 그에 맞는 자격을 갖출 수 있는 역량
전문 지식	사이버보안과 관련된 전문적인 학업을 이수하고 담당 훈련에 필요한 최신 지식, 훈련방식, 장비 등에 관한 지식 역량
실무 능력	교육생의 수준을 고려하여 담당 교육과 관련된 사이버보안 업무 또는 연구 경험이 풍부하고 교육생을 리드할 수 있는 실무 능력
강의 능력	교육생들에게 지식을 전달하고 능력을 향상시키며, 훈련 안내자 역할을 수행할 수 있는 능력으로 의사소통, 집중 유도, 문제 해결 등의 능력
연구 능력	사이버보안 및 담당 교육 내용과 관련된 새로운 지식과 기술을 습득하고 훈련 방식이나 내용에 관한 새로운 방법을 찾아낼 수 있는 능력

후보 역량별 지표도 기존의 연구[8-10] 결과, 국가 직무능력표준(NCS)[13], 전문가의 자문을 통해서 도출하였다. 역량별 5~9개의 후보 지표를 도출하였으며, 각각의 후보 지표는 역량을 충족시킬 수 있는 자질, 자격, 지식, 능력, 경험, 잠재력 등을 고려하였다.

교수자질은 교수자로서의 기본적인 인성과 강의능력, 훈련을 진행할 수 있는 실무 지식과 연구 능력 중심으로 선별하였다. 우선, 훈련교수가 교육자로서의 인격과 올바른 교육관을 갖고 교직원리를 준수하는 인성, 지식 전달과 학습 지도(안내)를 할 수 있는 정량적 자격으로 지표를 도출하였다. 최근에는 교수의 비리와 부정부패 사건이 도마에 오르면서 교수 선발 이전에 인성검사를 수행하는 대학도 늘어나고 있어 교수 인격의 중요성을 강조하고 있는 추세이다.

전문지식은 일반적인 정보보안관련 지식이 아닌 실제로 실습과 훈련을 진행하는 학생들을 지도할 수 있는 능력을 기준으로 선별하였다. 전문지식은 다음 표처럼 사이버보안 훈련과 관련된 보안 이론 지식, 훈련 내용과 직접적으로 연관된 사이버 공격 및 보안 기술 지식과 동향, 훈련에 사용되는 장비와 소프트웨어 활용 능력 등에서 도출하였다. 특히, 훈련 내용이

<표 3> 교수자질 역량의 후보 지표군

후보지표	내용
인성	교수자의 인격으로 자신의 감정과 생각을 올바른 방향으로 제어할 줄 알고 교육생/동료 교수와의 원만한 관계를 유지하며, 조직(센터) 내에서 융합할 줄 아는 성향
윤리 의식	확고한 가치관과 건전한 교육관, 확고한 도덕적 기준을 갖고 교육생들에게 솔선수범하고 교육생의 인격과 개성을 존중하며, 훈련교수간의 존경과 신뢰, 이해와 협조할 수 있는 교육 윤리
준법 정신	소속 연구소와 교육훈련 기관의 내규와 교육 규칙, 질서를 준수하고 교육생들에게 훈련 및 생활 규칙을 안내할 수 있는 태도
관심도	담당 과목에 대한 소명의식을 갖고 훈련 준비와 진행을 정열적이고 성실하게 임하는 자세
학위	담당 과목과 관련된 학위(학사/석사/박사) 취득 수준
전공	담당 과목과 관련된 전공분야로 정보보안, 컴퓨터공학, 정보통신 공학 등의 학문 분야
강의 경력	이전에 고등교육기관이나 정부/공공기관의 교육원(부서)에서 사이버보안과 관련된 강의 경험
자격증	정보보안과 컴퓨터 등과 관련된 국가공인기관이 주관하는 자격증 취득 현황
직위 (직책)	소속 연구소에서의 직위(연구원/선임/책임)와 직책(실장/부장/본부장 등)의 수행 경험

<표 4> 전문지식 역량의 후보 지표군

후보지표	내용
보안 이론	정보보안의 개념과 사이버방어 예방, 탐지, 분석, 피해평가, 복구, 역추적 등의 이론적 보안 지식
훈련 시나리오 실행 지식	공격 시나리오에 따른 탐지, 초동조치, 분석, 복구, 보완 등의 훈련 절차 진행에 관한 지식
사이버공격 지식	훈련 시나리오의 사이버 공격 특성, 침투 방식/경로, 피해 등에 관한 지식
신형 공격/보안기술 지식	공격의 진화와 변종, 새로운 공격 및 그에 따른 보안 기술에 관한 지식
최신 공격/보안기술 동향	담당 과목과 관련된 공격/보안 기술의 발전 추세와 보안 정책에 관한 지식
장비/소프트웨어 지식	사이버보안 훈련에 사용되는 장비/소프트웨어 제원, 성능, 사용방법 등에 관한 지식

주로 사이버 공격에 대한 대응훈련이기 때문에 사이버 공격에 대한 지식과 분석 능력도 포함시켰다.

실무능력은 교수자가 실제로 사이버공격과 방어와

관련된 업무를 수행하였거나 보안 소프트웨어 개발과 활용 경험이 있는 지표 위주로 선별하였다. 아래 표의 내용처럼 사이버보안 교육훈련이 이론 교육보다는 교육생이 주도적으로 공격에 대한 대응절차를 적용하는 실무 중심의 실습 교육이기 때문에 실제로 관련 실무나 연구를 수행한 경험이 필요하다.

<표 5> 실무능력 역량의 후보 지표군

후보지표	내용
보안실무 능력	정부/공공기관 또는 기업에서 보안 실무를 수행한 경력이나 연구소 내에서 관제, 분석, 평가 등의 보안 실무와 유사한 경험
보안관리 능력	기업 및 연구소에서 보안업무와 관련된 프로그램, 시스템, 장비 등을 관리하였거나 보안관련 부서, 인력 등을 관리한 경험
보안 S/W 개발/활용 능력	정보보안 관련 소프트웨어를 개발하였거나 실무 또는 연구 부서에서 사용한 경험
보안기술 연구 경력	사이버보안 기술 등의 보안 프로그램이나 장비, 방법 등에 관한 연구 경험
보안 정책/예산 수립 경험	기관이나 기업에서 보안 정책, 가이드라인 수립 및 예산 등의 업무를 수행한 경험

강의능력은 이론 강의가 아닌 훈련을 진행하면서 교육생들과의 문제해결을 위한 의사소통 능력과 장비 활용 능력 위주로 선별하였다. 아래 표와 같이 훈련 내용과 관련된 지식을 전달하고 교육생이 문제를 해결할 수 있는 능력을 극대화할 수 있는 안내자의 역할을 수행할 수 있는 능력이다. 훈련 안내자로서의 역할은 교육생과의 의사소통과 훈련과정에서의 문제 발생 시에 해결할 수 있는 능력 등도 포함한다.

연구능력은 아래 표처럼 훈련의 질과 성과를 향상시키기 위한 학습과정 설계, 훈련 방식 개발, 훈련 장비(소프트웨어) 개선 등의 지표를 포함한다. 또한, 훈련교수간 또는 다른 분야와 융합연구를 통해서 기술과 지식이 축적되고 고도화된 훈련과정을 개선하고 훈련 프로그램 개발할 수 있는 능력을 지녀야 한다.

<표 6> 강의능력 역량의 후보 지표군

후보지표	내용
교육훈련 설명 능력	담당 과목에 대해 완벽하게 이해하고 교육생들에게 훈련 방식, 훈련 절차, 훈련 장비 등에 대해서 전달할 수 있는 능력
의사소통 능력	교육생들에게 일방적으로 교과서적인 지식 전달을 하고 정해진 훈련 방식만 고집하는 것이 아니라 교육생 스스로가 훈련 방식을 설계하고 진행할 수 있도록 조력자, 튜터와 같이 지속적으로 의견을 상호 전달하고 문제 발생이나 새로운 방식을 찾아낼 때 서로 고민하고 토론할 수 있는 능력
실습 진행 파악 능력	실습 진행 과정, 즉 교육생들이 훈련 시나리오에 의해서 실습할 때 교육생 개개인의 훈련 진도를 파악하고 교육생들에게 나타난 문제와 훈련 방해 요소를 파악할 수 있는 능력
실습 집중 유도 능력	교육생들에게 지적 호기심을 갖게 하고 문제 해결의 욕구가 생기게 하며 새로운 방법을 모색할 수 있는 창의적인 사고의 기회를 줄 수 있는 능력
문제해결 능력	교육생이 실습을 진행할 때 방해 요소가 발생하면 해결할 수 있는 실마리를 제공하고 훈련 진도를 내지 못할 때 해결 방안을 제시하며, 새로운 방식을 발견할 때 인정하고 체계화할 수 있는 능력
교육훈련 장비 활용 능력	훈련장에 설치된 시스템과 사용하는 프로그램 등을 실무자처럼 자유롭게 사용할 수 있으며, 고장이나 이상이 발생할 때 일차적 조치를 취할 수 있는 능력

<표 7> 연구능력 역량의 후보 지표군

후보지표	내용
논문 게재 및 발표	사이버보안, 훈련 방식, 훈련 프로그램, 훈련 소프트웨어 등과 관련된 연구 결과를 논문으로 게재하거나 학술대회에 발표한 실적
저서 발간	보안 정책, 보안 가이드, 사이버 공격/보안 기술 정보보안 이론 등의 저서 출간 또는 해외 유명 서적의 번역서 발간 실적
특허 개발	사이버보안, 훈련 프로그램과 소프트웨어 등과 관련된 특허 출원 및 등록 실적
교재 발간	담당 과목을 운영하기 위한 주교재, 참고서, 가이드라인 등의 훈련 교재 발간 실적
교수법 개발/제안	교육 진행시에 훈련 방식, 훈련 도구, 훈련 시나리오에서 발생했던 문제점에 대해서 개선점을 제안하고 새로운 방법을 개발한 실적
교육훈련 S/W 개발	사이버보안 또는 훈련 프로그램에 사용하고 있는 프로그램의 기능을 개선하거나 새로운 소프트웨어를 개발한 실적

### 3.3 설문 조사

설문조사에 참여한 교수는 총 33명이고 설문지는 구글 설문지를 활용하였으며, 후보 역량 중에서 3개, 역량별 후보 지표 중에서 4개를 선택하게 하였다.

아래 표와 같이 설문조사 결과 역량은 전문지식, 실무능력, 강의능력이 선택되었다. 교수자질이나 연구능력은 상대적으로 선택 비중이 적었다. 교수 자질은 단기간 사이버보안 교육훈련을 하는 전문인력에게는 3가지 역량에 비해 중요도를 낮게 평가되었으며, 연구능력은 대학 교수의 역량으로서는 중요한 요소이지만, 교육훈련 전문인력에게는 실무능력을 더 중요시하기 때문에 우선순위가 낮았다.

설문조사 결과를 분석하면, 전문지식 역량은 교육훈련 전문인력이 사이버보안 교육훈련을 담당하는 만큼 사이버보안과 관련된 지식과 담당과목의 사이버보안과 공격 지식을 보유해야 한다는 것이 설문 참여자들의 공통적인 의견이다. 이는 선행연구의 교수역량이나 직업훈련 교수(교수)의 역량을 살펴보다도 관련 전공의 지식이 포함되어 있어서 공통성을 갖는다. 실무능력은 교육생들이 기관(기업)의 정보보안 실무자이거나 취업 준비자이기 때문에 교육훈련 전문인력도 담당 교과목에 대한 실무 지식과 능력을 갖춰야 한다는 의견이다. 즉, 사이버보안 교육훈련은 기초적인 이론 교육과 보안 지식이나 기술의 동향을 학습하기 보다는 실무능력 향상을 목표로 진행되기 때문에 훈련 진행 중에 문제가 발생할 경우에 교수의 실무 지도가 필요하다. 예를 들면, 교육생이 새로운 탐지 및 분석 방법을 제안할 경우에 그것을 확인하고 검증할 수 있는 능력이 갖춰야 한다. 강의능력은 교육훈련 전문인력이 지속적으로 강의를 진행한 교수자가 아니며, 전문적으로 교수법을 익힌 교수가 아니기 때문에 최소한의 강의 진행 능력만 갖춰면 된다고 보았다. 교육훈련 전문인력은 단기간에 교육생들에게 실무 지식과 실행 능력을 향상시키는 것이 목적이기

<표 8> 설문조사 결과

후보역량	후보 지표	인원(%)
교수자질 (14/42.4%)	윤리의식	24(72.7)
	인성	21(63.6)
	관심도	21(63.6)
	전공	20(60.6)
	강의경력	18(54.5)
	준법정신	13(39.4)
	학위	6(18.2)
	자격증	2(6.1%)
전문지식 (32/97%)	직위(직책)	0(0)
	보안 이론	29(87.9)
	신형 공격/보안 기술 지식	22(66.7)
	최신 공격/보안 기술 동향	22(66.7)
	훈련 사이버 공격 지식	19(57.6)
	장비/소프트웨어 지식	18(54.5)
실무능력 (25/75.8%)	훈련 시나리오 실행 지식	17(51.5)
	보안 실무 경력	31(93.9)
	보안 S/W 개발 및 활용 경력	29(87.9)
	보안기술 연구 경력	29(87.9)
	보안관리 경력	24(72.7)
	보안 정책/예산 수립 경험	9(27.3)
강의능력 (23/69.7%)	기타 보안 실무 경험	5(15.2)
	교육훈련 설명 능력	28(84.8)
	의사소통 능력	28(84.8)
	문제 해결 능력	19(57.6)
	교육훈련 장비 활용 능력	19(57.6)
	실습 진행 파악 능력	17(51.5)
연구능력 (4/12.1%)	실습 집중 유도 능력	17(51.5)
	논문 게재 및 발표	30(90.9)
	교재 개발	27(81.8)
	교수법 개발/제안	26(78.8)
	저서 발간	18(54.5)
	교육훈련 S/W 개발	14(42.4)
특허 개발	10(30.3)	

때문에 실습 및 훈련 진행의 조력자의 역할에 중점을 두어야 한다는 것이 일반적인 의견이다.

### 3.4 사이버보안 교육훈련 전문인력의 역량과 지표 선정

설문조사 결과에서 선택된 역량별 지표 분석은 다음과 같다. 우선, 전문지식에서는 보안이론, 신형 공격/보안 기술 지식, 최신 공격/보안기술 동향, 훈련 사이버공격 지식이 선택되었다. 보안 이론 지표는 사이버보안 교육훈련을 담당하는 전문인력은 기본적으로 보안 이론에 대해서 해박한 지식을 갖추어야 된다는 의견이다. 또한, 사이버보안 교육훈련은 과거나 현재 사용되었던 사이버 공격과 보안 기술을 기반으로 교육훈련이 진행될지라도 새로운 공격 방식이나 변형, 변종된 공격 방식을 예측하고, 그에 대비한 보안을 위해서 최신 사이버 공격/보안 기술의 동향과 새로운 공격 및 보안 기술에 대한 지식을 보유한다는 의견을 모았다. 훈련 시나리오 실행 지식은 교육훈련 진행 중에 교육생들이 공격에 대한 질문을 할 때 답변하고 의문을 제기할 때 해결할 수 있는 능력 측면에서 선택된 것으로 분석된다.

둘째, 실무 능력은 보안 실무자가 정보통신시스템을 대상으로 관제, 위협 탐지 및 분석, 복구 등의 실무 경험을 중요시 하였으며, 소프트웨어 개발이나 보안 기술에 관한 연구 경력도 중요한 요소로 간주하였다. 반면에 보안정책이나 예산 분야와 인적/물적/관리적 보안 측면에서는 실무 능력이 아닌 관리 능력으로 판단하였다.

마지막으로, 강의능력 역량 지표는 일반 교육자의 교육이나 강의 역량이 아닌 사이버보안 교육훈련 특성을 충분히 고려한 것으로 판단된다. 최근에 대학이나 교육기관에서는 학생 중심의 주도적이고 창의적인 학습법을 선호하고 있다. 교수자는 주로 학생들이 학습을 진행하기 전에 학습 내용에서 설명하고 학습도중에 문제가 발생할 경우에 문제를 해결할 수 있는 방법을 알려주며, 결과 도출 시에 결과를 평가해 주는 학습 안내자나 조력자의 역할을 한다. 사이버보안

교육훈련도 대부분이 교육 시간이 학생들이 훈련 시나리오에 의해서 공격에 대한 방어를 실습하는 방식으로 탐지, 조치, 분석, 복구 등의 절차를 스스로 실습하고 있기 때문에 교수자는 주도자가 아닌 조력자의 역할을 수행해야 한다. 그래서 설문자들은 사이버보안 교육훈련 전문인력의 훈련 이해 및 설명 능력, 문제 발생 시, 교육생들과의 의사소통과 문제 해결 능력, 훈련 장비와 소프트웨어의 능숙한 활용 능력을 우선시 하였다. 교수자로서의 훈련 진행과 교육생 집중 유도 능력은 다른 역량 지표에 비해서 상대적으로 다소 중요하지 않다고 판단하였다.

다음 표는 연구결과로 선택된 사이버보안 교육훈련 전문인력에게 요구되는 필수 역량과 지표를 보여준다.

<표 9> 사이버보안 교육훈련 전문인력의 필수 역량 및 지표

후보역량	내용
전문 지식	보안 이론
	신형 공격/보안 기술 지식
	최신 공격/보안 기술 동향
	훈련 사이버 공격 지식
실무 능력	보안 실무 경력
	보안 S/W 개발 및 활용 경력
	보안기술 연구 경력
	보안 관리 경력
강의 능력	교육훈련 설명(이해) 능력
	의사소통 능력
	문제 해결 능력
	교육훈련 장비(S/W) 활용 능력

## V. 결론

교육생 중심으로 진행되는 사이버보안 교육훈련은 이론보다는 실습과 훈련 과정으로 구성되어 있다. 이러한 교육훈련을 담당하는 전문인력은 일반 대학에서 정보보안을 강의하는 교수나 일반 정보보안 교육

기관에서 초빙되는 전문가보다는 보다 더 전문지식과 실무능력을 갖춰야 한다. 아울러 훈련과 실습을 원활하게 진행시킬 수 있는 강의능력도 보유해야 한다. 본 연구에서는 기존의 교수 역량 연구 결과와 미국의 정보보안 전문교육의 필수 요소와 국가직무능력표준을 기반으로 사이버보안 교육훈련 전문인력의 필수 역량과 지표를 도출하였다. 도출한 역량과 지표는 대학에서 정보보안과 관련된 강의를 진행하는 교수들의 설문조사를 통해서 3개의 역량과 역량별 4개의 지표를 선정하고 검증하였다.

사이버보안 교육훈련을 담당하는 전문인력의 경우는 실습과 훈련과 관련된 사이버공격과 보안 전문 지식, 실습과 훈련 과정 중에서 문제가 발생할 경우에 신속하게 해결할 수 있는 실무능력, 그리고 교육생과 상호 소통할 수 있고 이해시킬 수 있는 강의능력을 필수 역량으로 선정되었다.

본 연구결과는 사이버보안 교육훈련을 실습과 훈련 중심으로 진행하는 교육기관에서 교육훈련 전문인력을 초빙할 경우에 선발 기준 자료로 활용할 수 있다.

## 참고문헌

- [1] 엄정호, 이우일, 박광기, “국방 사이버전사 역량 강화를 위한 특화된 사이버훈련체계 구축 방안,” 보안공학연구논문지, 제13권, 제2호, 2016, pp.99-112.
- [2] 엄정호, “효과적인 사이버보안 교육훈련을 위한 교육과정 문제점 및 개선 방안,” 보안공학연구논문지, 제12권, 제2호, 2015, pp.337-350.
- [3] 양진석, 정태명, 엄정호, “효과적인 사내 정보보호 직무교육을 위한 사내강사 운영관리 방안,” 디지털산업정보학회 논문지, 제14권, 제4호, 2018, pp.109-116.
- [4] 이현영, 김영수, 허희옥, “공과대학 교수역량 (Teaching Competency) 진단도구 개발 연구,” 교육공학연구, 제28권, 제3호, 2012, pp.439-469.
- [5] 김기훈, 엄정호, “사이버보안 전문인력 획득을 위한 사이버보안 훈련생에 특화된 훈련성과 측정 모델에 관한 연구,” 디지털산업정보학회 논문지, 제12권, 제4호, 2016, pp.59-69.
- [6] 이종찬 외 5명, “정부 주도 사이버 보안 인력 양성 과정 개선 방안,” 보안공학연구논문지, 제13권, 제2호, 2016, pp.113-130.
- [7] 백근예, “군 교육담당자의 교수역량 모델 개발-육군 병과학교를 중심으로,” 고려대학교 석사학위논문, 2009, pp.37-41.
- [8] 안상란, 임규연, “사이버대학 교수자의 교수역량 진단을 통한 교육요구도 탐색,” 교육방법연구, 제27권, 제3호, 2015, pp.375-400.
- [9] 노혜란, 최미나, “인적자원 개발을 위한 교수 역량 모델 개발,” 직업능력개발연구, 제7권, 제2호, 2004, pp.1-28.
- [10] 노정진, “직업교육훈련 교원의 교수역량 모델 개발-한국폴리텍대학을 중심으로,” HRD연구논문지, 제20권, 제1호, 2018, pp.131-165.
- [11] 이은상, “기술 교사의 공학 교수역량 모델 개발,” 충남대학교 박사학위논문, 2015, pp.21-51.
- [12] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” NIST Special Publication 800-181, 2017, pp.5-6.
- [13] <https://www.ncs.go.kr/education/index.do>



■ 저자소개 ■



엄 정 호  
Eom Jungho

2011년 3월~ 현재 대전대학교  
군사학과&안전융합학부 부교수  
2011년 3월 성균관대학교 정보통신공학부  
BK21 연구교수  
2008년 2월 성균관대학교 컴퓨터공학과(박사)  
2003년 2월 성균관대학교 컴퓨터공학과(석사)  
1994년 2월 공군사관학교 항공공학과(학사)

관심분야 : 네트워크/시스템 보안, 사이버전,  
사이버안보, 내부자보안  
E-mail : eomhun@gmail.com

논문접수일 : 2019년 02월 15일
수정일 : 2019년 02월 27일
게재확정일 : 2019년 02월 28일