디지털산업정보학회 논문지 제12권 제4호-2016년 12월
http://dx.doi.org/10.17662/ksdim.2016.12.4.059

사이버보안 전문인력 획득을 위한 사이버보안 훈련생에 특화된 훈련성과 측정 모델에 관한 연구

김 기 훈* · 엄 정 호**

A Study on the Model of Training Performance Measurement Specialized to Cyber Security Trainee for Cyber Security Professionals Acquisition

Kim Kihoon · Eom Jungho

〈Abstract〉

We proposed a specialized model of performance measurement to measure the training performance of the trainees in cyber practical training. Cyber security professionals are cultivating their expertise, skills, and competencies through cyber practical training in specialized education and training institutions. The our proposed process of trainee evaluation is consisted of an evaluation component discovery, evaluation item selection, evaluation index catalog, ratings and criteria decision, and calculation formula. The trainee evaluation is consisted of a formative evaluation during the training and an overall evaluation after finished training. Formative evaluation includes progress evaluation and participation evaluation, and overall evaluation includes practice evaluation and learning evaluation. The evaluation is weighted according to the importance of evaluation type. Because it is evaluated actual skills and abilities, competencies are assigned a high weight, while knowledge and attitudes are assigned a low weight. If cyber security trainees are evaluated by the proposed evaluation model, cyber security professionals can be cultivated by each skill and knowledge level and can be deployed by importance of security task.

Key Words : Cyber Security, Security Professionals, Training Evaluation, Cyber Actual Training

Ⅰ. 서론

최근 발생하는 사이버공격이나 테러로 인해 사이버보안 전문가 양성에 많은 심혈을 기울이고 있다. 특히, 공공기관의 정보보안 담당자들은 업무역량을 향상시키기 위해서 실전적 훈련 프로그램에 적극적으로 참여하고 있다. 훈련 프로그램을 운영하는 기관들은 훈련자들의 실전적 보안능력을 향상시키기 위해서 보호대상을 국가기반체계로 세분화하고 규모는 점점 대형화하며, 훈련생 참여 정도와 수준에

* 대전대학교 군사학과 교수
** 대전대학교 군사학과 교수(교신저자)

따라 훈련과정과 방법을 전문화하고 있다. 아울러 훈련 프로그램 개발과 검증에 심혈을 기울이고 있으며, 훈련생들에 대한 훈련성과 측정 방법 연구에도 관심을 갖기 시작했다. 훈련체계에 대한 프로그램 개발과 훈련환경 개선에는 투자를 아끼지 않는 반면, 훈련생들의 훈련 성과에 대한 평가에는 수동적으로 단순한 설문형으로 진행되는 경우가 많았다[1]. 일반교육 분야에서는 교육 프로그램, 훈련성과에 대한 정확한 평가를 위해서 많은 전문가들이 활발하게 연구가 진행되고 있는 반면, 사이버훈련 분야에서는 훈련 프로그램의 성숙도와 훈련생의 역량 향상 측정 연구는 미진한 상태이다. 특히, 훈련생들의 훈련과정 목표에 부합되는 훈련성과 도달 수준을 측정할 수 있는 평가 방법론 개발 분야는 이제 연구가 막 시작되는 시점이다.

훈련생들은 사이버보안 역량을 높이기 위해서 본인의 사이버보안 지식 및 기술 수준에 따라 훈련과정의 수준 즉, 기본, 중급, 고급, 전문과정 중에 한 과정을 선택하여 훈련을 받는다. 훈련종료 후에는 훈련과정 목표 수준에 따라 그에 맞는 임무를 수행한다. 그런데, 훈련생이 훈련과정 목표에 맞는 역량을 갖추지 못하고 사이버보안 직무를 수행한다면, 소속 기관에서 사이버공격이 발생할 경우에 신속하게 위협을 차단하고 피해를 줄이지 못할 것이다. 그래서 사이버보안 훈련에 참가하는 훈련생의 참여도, 지식, 숙련도 등을 정확히 측정할 수 있는 사이버보안 훈련에 특화된 훈련생 평가 방법 개발이 필요하다[2-4].

본 논문에서는 사이버보안 훈련생이 훈련 목표에 어느 정도 도달했는지를 측정할 수 있는 훈련 성과 측정 모델을 제시한다. 훈련 과정을 이수한 훈련생의 훈련 성과의 달성 수준을 측정하는 것으로 훈련생의 지식, 기술과 행동요령 등을 종합적이고 객관적으로 검증하는 방법이다. 사이버실전훈련의 이론학습, 실습 방식 등을 기반으로 사이버보안 훈련생에 특화된 평가 항목, 지표, 기준, 평가 산출식 등의 평가 방법을 제안한다.

본 논문은 2장에서 훈련센터의 사이버보안훈련 현황을 분석하고 3장에서 훈련생에 특화된 훈련성과 측정 모델을 제시하였다. 4장에서는 제안한 모델을 훈련과정에 적용하였고 5장에서 결론을 맺는다.

Ⅱ. 사이버보안훈련 현황[5]

공공기관 정보보안 담당자를 대상으로 한 사이버보안훈련 기관 중에 전문성을 갖춘 기관은 00훈련센터이다. 사이버보안 실전훈련으로 사이버 위협 예방훈련과 사이버 위기 대응 훈련으로 구분된다. 사이버 위협 예방 훈련은 선제적 방어를 위해 다양한 실제 사이버 공격 사례를 중심으로 사이버 위협 예방훈련 기본과정과 전문과정을 운영한다. 사이버 위기 대응훈련은 인터넷, 정부, 기반시설, 모바일 영역과 종합훈련 5가지 영역으로 구분하여 진행하며, 각 영역에서 발생하는 사이버 공격에 대한 실제적인 대응훈련을 실시한다. 또한, 과정별로 기본과 전문 과정으로 구분하여 훈련생의 수준별로 훈련이 진행된다. 본 연구에서는 평가 대상을 사이버 위기 대응훈련에 참여한 훈련생으로 제한한다. 사이버 위기 대응훈련은 각 영역별로 발생할 수 있는 공격에 대한 탐지, 분석, 복구 등 대응 훈련이 주를 이룬다. 아울러 이론이나 설명보다는 훈련생이 직접 행동절차를 습득하는 실습 위주의 훈련으로 진행한다. 교수는 기초적인 이론이나 훈련절차, 훈련환경, 공격 및 방어에 사용되는 프로그램이나 장비에 대해 설명하고, 훈련생은 과정 전반에는 대응절차를 습득하는 실습을 하고 중/후반에는 교수가 제시한 시나리오에 따라서 훈련생이 실제적으로 대응 활동을 수행한다.

훈련 과정은 크게 과정 소개, 훈련 설명, 훈련 실습으로 구성되며, 훈련과정 소개는 공격 및 대응 관련 이론, 공격 사례, 공격 및 방어 절차를 설명하고 훈련 설명은 공격 절차, 훈련 절차 및 환경, 공격 및 방어에 사용되는 프로그램이나 장비 사용법을 설명하며, 훈련 실습은 초기에는 대응 절차를 실습한 후 시나리오에 따라서 자의적으로 대응 활동을 수행한다. 다음 표 1은 훈련 과정 단계를 보여준다.

<표 1> 사이버 위기 대응훈련 단계

단계	내 용
과정소개	이론, 사례, 공격/방어 설명
훈련설명	공격절차 소개, 훈련절차/환경 설명 공격 및 방어 도구(장비) 사용법
훈련실습	훈련절차에 따른 실행

훈련생이 직접 침입에 대응하는 훈련 실습에서는 훈련절차에 따라 대응방법과 보안 장비의 사용법을 교수의 설명대로 실습하고 각 실습 단계별로 주어진 미션에 의해서 스스로 대응하고 문제를 해결한다. 훈련 실습 과정에서는 다음 표 2와 같이 6단계로 구성되며, 단계별로 교수와 훈련생의 역할이 구분되고 준비 단계를 제외하곤 각 단계별 미션이 부여된다.

<표 2> 사이버 위기 대응훈련 실습 과정

단계	내 용
준비	교수 : 공격 준비 및 실행 훈련생 : 방어 준비 및 보안장비(프로그램) 확인
탐지	이상징후 탐지(역할별 업무 수행) 침해사고 확인, 상황 통보문 작성
초동조치	1차 침입경로 제거, 정밀분석 자료 수집 대응전략 수립, 침해사고 초동조치 보고서 작성
분석	공격 의심 IP 식별, 로그분석을 통한 공격 확인 공격정보 분석 및 대응전략 수립 침해사고 분석보고서 작성
복구	방어 대책 수립, 보안장비 설정 및 업데이트 피해 시스템 복구, 침해사고 사고조치 보고서 작성
보안강화	보안설정 강화, 보안정책 업데이트 침해사고 조치 보고서 작성

① 준비: 교수는 공격을 준비하고 실행하며, 훈련생은 대응을 위해서 보안 장비를 확인한다.

② 탐지: 훈련생은 비정상적인 이상징후가 포착되면, 시스템을 점검하여 침입여부를 확인하여 대응절차의 수행 여부를 결정한다.

③ 초동조치: 시스템의 침입을 인지한 후, 분석 이전에 시행할 조치를 수행하는 단계로, 침입경로 제거, 정밀분석 자료 수집, 대응전략을 수립한다.

④ 분석: 침입 흔적을 통해 침입 근원지, 피해 시스템, 유출정보 등을 분석하여 복구 및 대응방법을 결정하는 단계로, 침입 유형을 확인하고 침입 정보를 분석하여 대응전략을 수립한다.

⑤ 복구: 분석단계 결과를 참고로 취약점에 대한 보안설정을 수행하고 피해 시스템을 복구하는 단계로 방어대책 수립, 보안장비 설정 및 업데이트, 피해 시스템의 정상 기능을 회복시킨다.

⑥ 보안강화: 보안설정을 강화하는 단계로 보안정책을 업데이트한다.

Ⅲ. 훈련생에 특화된 훈련성과 측정 모델

3.1 훈련성과 측정 모델 설계를 위한 요구사항

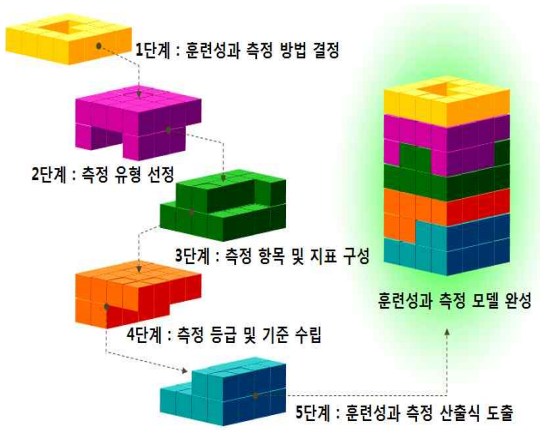
사이버실전훈련에 참가한 훈련생의 훈련성과 측정은 훈련 과정을 통해서 훈련생이 습득한 지식의 향상과 기술의 숙달 정도를 측정하는 것이 목적이다. 훈련생에 특화된 훈련성과 측정 모델은 기존에 연구되고 개발된 훈련 평가 방법과 다르게 훈련생의 문제해결 능력 즉, 사이버공격에 대해 실질적으로 대응할 수 있는 역량을 평가한다. 기존의 훈련 평가는 훈련 과정이나 프로그램의 적절성을 판단하거나 체계적인 훈련체계를 갖추기 위한 훈련 과정의 가치 및 훈련의 효과성 및 유용성을 평가하는 반면에 사

이버실전훈련 훈련생에 특화된 훈련성과 측정 모델은 평가 대상이 훈련생에게만 한정되고 평가 방식도 훈련생의 훈련성과 측정에 집중된다. 아울러 측정 방식에 따른 평가 항목이나 지표도 훈련생의 훈련 참여도, 실습정도 및 지식 습득 수준 등의 요소로 구성된다. 기존의 훈련 평가는 훈련생 평가도 포함되어 있기 때문에 제안한 훈련생 평가 방법에 의한 평가 결과를 훈련 평가에 적용할 수 있다. 즉, 훈련생 평가 수준이 전반적으로 낮거나 표준편차가 심할 경우는 훈련생의 자질, 역량 및 기술 수준, 훈련과정 내용 및 수준, 교수의 역량 등 여러 측면에서 검토할 수 있는 자료로 활용할 수 있다[6-8].

사이버실전훈련의 훈련생에 특화된 훈련성과 측정 목적은 앞서 언급한 바와 같이 훈련생의 훈련성과 수준을 측정[9]하는 것으로 훈련생의 지식(이론) 습득 정도, 기술의 향상 정도 및 보안기술의 적용 능력 등의 문제해결 능력을 중점으로 평가한다. 우선, 훈련 과정이 의도한 훈련 목표를 훈련생이 성취하였는지를 평가한다. 사이버실전훈련은 각 과정별로 훈련 목적과 목표가 있기 때문에 훈련 특성에 부합된 기술이나 지식의 습득 여부를 평가한다. 둘째, 훈련생들이 훈련 프로그램을 진행하면서 훈련생들이 부족한 부분을 확인한다. 모든 훈련생이 훈련 프로그램에 따라 훈련 성과를 달성하면 좋겠지만, 훈련생 개개인이 뛰어난 부분이나 부족한 부분이 있기 때문에 그 부분을 찾아내어 훈련생들의 부족한 부분을 충족시킨다. 셋째, 훈련생들이 교육 과정에서 습득한 지식이나 기술 이외에 다른 창의적인 기술을 통해서 대응할 수 있는 방법을 찾아낼 수 있는 능력을 도출한다. 훈련 과정의 실습과 미션 수행을 통해서 습득한 기술을 기반으로 새로운 대응 기술을 발견할 수 있도록 마련해 준다. 예를 들면, 공격 시나리오를 주고 그에 따른 대응을 수행할 수 있도록 평가하는 실행평가에서는 기존의 방법 이외에 다른 방법을 통해서 대응할 수 있도록 모든 방법을 허용해 준다. 마지막으로 훈련성과 측정 결과를 토대로 교육, 실습이나 평가 등의 명확성과 타당성을 검토한다. 훈련성과 측정 결과가 매우 낮으면 훈련 프로그램의 수준이 너무 높거나 훈련생의 수준이 훈련 입과 요구 수준에 미달한 것으로 판단할 수 있다. 또한, 결과의 표준편차가 클 경우에는 개인별 훈련 역량이 상이한 것으로 훈련생 선발 절차에 오류가 있을 가능성도 있다. 아울러 전체적인 훈련 프로그램 내용이나 훈련 방식, 교수자의 능력 등의 요소에 문제점이 있을 수 있다.

3.2 훈련생에 특화된 훈련성과 측정 모델 설계

모델 설계는 평가개발 절차에 따라 명확한 측정 방법과 절차를 수립한다. 본 연구에서는 평가 목적, 평가 대상 및 범위가 선정되어 있어서 성과 측정 방법과 유형, 측정 항목과 지표, 측정 등급과 기준, 그리고 성과측정 산출식만 도출한다. <그림 1>은 훈련생에 특화된 훈련성과 측정 모델 개발 절차를 보여준다.



<그림 1> 훈련성과 측정 모델 개발 절차

① 훈련성과 측정 방법 결정: 성과 측정 종류에는 훈련 전에 실시하는 진단평가, 훈련 중에 하는 형성평가, 훈련 종료 후에 하는 총괄평가가 있다. 진단평가는 훈련 전에 훈련생의 지식수준, 배경, 관련 분야 교육 이수 정도 등을 평가하여 훈련과정에 입과 할 수 있는 자격을 측정한다. 형성평가는 훈련생의 훈련 참여도를 측정하기 위해서 훈련 과정 중에 교수가 훈련생의 활동을 관찰하여 평가한다. 총괄평가는 훈련 결과를 최종적으로 측정하는 것으로 훈련생들의 지식 향상 정도, 문제해결 방법, 처리절차 준수, 새로운 해결방법 창안 등의 항목에서 평가한다. 본 논문에서는 훈련생의 훈련성과 측정이 목표이기 때문에 진단평가를 제외한 형성평가와 총괄평가만 진행한다.

② 훈련성과 측정 유형 선정: 훈련생의 훈련성과 측정은 훈련생의 역량 즉, 자질, 이론, 기술 분야에서 향상 정도를 측정한다. 본 논문에서는 표 3과 같이 학습(이론)평가, 실습평가와 근태평가를 선정하였다. 평가방법에 따라 형성평가에는 근태평가와 진행평가, 총괄평가에는 학습평가와 실행평가를 포함한다.

<표 3> 훈련성과 측정 유형의 종류

종류	기간	유형	설 명
형성평가	훈련중	실습(진행)평가	실습을 진행하면서 한 단계씩 진행될 때 마다 훈련실습 시나리오나 미션을 부여하여 그 문제를 얼마나 잘 해결하는 지 평가
		근태평가	훈련 기간 중에 훈련생의 전반적인 학습 태도, 참여정도 등 교수가 직접 평가
총괄평가	훈련후	실습(실행)평가	최종적으로 과정이 종료되면 종합적인 특정 상황을 부여하여 그에 따른 관련 지식, 해결방법, 처리절차, 새로운 방법 탐구 등의 측면에서 평가
		학습평가	사이버공격과 대응 방법 측면에서 얼마나 이론적으로 지식 습득 정도 평가

진행평가는 실습 단계가 진행될 때마다 훈련실습 시나리오나 미션을 부여하여 그 문제의 해결 능력을 평가하며, 실행평가는 최종적으로 훈련과정이 종료되면 종합적인 특정 상황을 부여하여 그에 따른 관련지식, 해결방법, 처리절차, 새로운 방법 탐구 등의 측면에서 평가한다. 근태평가는 훈련기간 중에 훈련생의 전반적인 학습태도와 참여정도를 교수가 직접 평가한다. 학습평가는 사이버공격과 대응 방법 측면에서 어느 정도의 지식을 습득하였는지를 평가한다.

③ 성과 측정 항목 및 지표 구성: 학습평가는 훈련 주제와 내용에 맞게 이론적으로 사이버공격과 대응방법에 대해서 어느 정도 지식을 습득하였는지에 대한 평가 항목 및 지표를 도출한다. 즉, 사이버공격의 개념, 절차, 특징, 피해현상 등을 위주로 사이버 공격 대응 방법의 종류, 절차, 보안 시스템(프로그램) 활용법 및 복구 방법 등에서 평가 항목을 도출한다. 근태평가는 훈련생의 훈련시간 준수, 훈련준비도, 실습태도, 훈련참여도 등에서 도출한다.

<표 4> 성과 측정 항목 및 지표

유형	항목	지 표
실습평가 (진행평가)	'준비-탐지-초동조치-분석-복구-보안강화' 단계별 수행 절차	・탐지: 이상징후 탐지시간, 공격정보 수집 여부 등 ・초동조치: 침입경로 제거 수행절차, 수집정보 정확도, 향후 대응방법 수립 여부 등 ・분석: 공격 IP(공격자) 정보 정확도, 공격 유형 분석 정확도 등 ・복구: 보안장비 설정 및 업데이트 수행 여부, 피해 시스템 확인 및 복구 실행 여부 등 * 보안장비(프로그램) 활용 및 보고서 작성 능력은 전 단계 적용 가능
실습평가 (실행평가)	공격 시나리오	탐지여부, 공격에 따른 초동조치의 신속성, 분석의 정확도, 피해 시스템 확인 및 복구 신속성 및 복구 수준, 공격에 따른 보안 강화 수행 방법의 적절성 등
학습평가	사이버공격 사이버방어 (대응)	・사이버공격: 개념, 절차, 특징, 피해현상 및 변형 가능성 등 ・사이버방어: 대응방법의 종류, 절차, 보안 시스템(프로그램) 활용법 및 복구 방법 등
근태평가	훈련 참여도	훈련시간 준수, 훈련준비도, 실습태도, 훈련참여도 등

진행평가는 훈련 진행 중에 훈련 주제에 따라서 평가 항목과 지표를 구성하면 된다. 즉, '준비-탐지-초동조치-분석-복구-보안강화' 단계별 실습이 종료될 때마다 단계별 핵심 실습 내용에 대해서 평가한다. 실행평가는 훈련 종료 후에 전체적인 훈련 내용에 대해서 전체적으로 사이버공격 시나리오를 부여하여 공격 특성에 맞게 사이버공격 대응 절차대로 수행하는지의 여부를 평가하면 된다. 이 때, 실습평가는 훈련내용 이외에 새로운 해결 방안을 제시할 경우에 가산점을 부여할 수 있다.

④ 성과 측정 등급 및 기준 수립: 사이버실전훈련 훈련생은 훈련목표 달성 여부를 측정하는 것이기 때문에 훈련생간 상대평가보다는 절대평가를 선택하는 것이 타당하다. 그리고 성과 측정 방식을 정량적 또는 정성적으로 할 것인지를 결정해야 한다. 본 연구에서는 평가 결과는 백분율로 산출하되, 각 평가 문제별로 매트릭스 스케일링 방식에 따라 정성적인 평가로 진행한다. 즉, 평가 문제에 따라 점수로 채점하는 방식이 아닌 평가 등급에 따라 채점을 한다. 평가의 정확성을 높이고 고성과자와 저성과자의 분류를 명확하기 위해서 성과 측정 등급은 다음 표 5와 같이 5단계의 평가 등급을 적용한다.

<표 5> 성과 측정 등급

구분	S	A	B	C	D
평가등급	현저히 우수(탁월)	대체로 우수(우수)	기대수준 (보통)	기대 이하 (미흡)	현저히 기대 이하 (미달)
평가점수	10	9	8	7	6

5등급 평가체계는 나승일의 '과정이수형 자격의 평가체계 개발 연구'[7], 중소기업진흥공단의 '중소기업지흥공단 신인사제도 구축 연구[10], 그리고 인천항만공사의 '인사제도 개선 및 성과연봉제 설계[11]'에서 제시한 평가체계를 요약하여 적용하였다. 5등급 평가체계는 성과차등에 대한 훈련생들의 수용성을 높일 수 있으며, 평가자의 측정 부담을 해소할 수 있다. 표 6은 등급별 성과 측정 기준으로 보여주며, 성과 측정 기준은 훈련생이 훈련과정에서 기대하는 목표에 맞게 평가유형에 따라 출제한 문제의 해결 능력이 어느 정도 수준에 도달했는지를 측정하는 척도를 의미한다. 앞서 언급한 바와 같이 성과 측정 등급에 따라 평가목표 도달 수준을 5단계로 구분하고, 평가기준은 훈련생의 평가 과정을 통해서 보여주는 이론, 기술, 능력 등을 포함한다.

<표 6> 등급별 성과측정 기준

구분	기 준
S (탁월)	문항의 평가기준 수준을 만족시키거나 초과하여 이론, 기술, 학습 등의 측면에서 완벽하게 수행할 수 있는 탁월한 답안을 보여준 수준
A (우수)	문항의 평가기준에서 기대되는 수준을 원활하게 작성하였을 뿐만 아니라 풀이과정 중에 우수한 문제해결 능력을 나타내고 본인 개인의 역량 향상을 완수하는 수준
B (보통)	문항의 적합한 답안 작성을 위해 착실하게 답안을 작성하고 학습한 내용을 충분히 서술한 수준
C (미흡)	답안 작성을 하였으나, 문제해결에 미흡하고 주어진 문제를 능동적이고 창의적인 자세가 아닌 수동적으로 작성한 수준
D (미달)	문제해결 능력이 부족하고 강의내용을 대부분 이해하지 못한 내용으로 답안을 작성하였으며, 답안 작성이 상당히 부족한 수준

④ 훈련성과 측정 산출식 도출: 최종 산출식은 우선 각 측정 유형별로 평가를 진행하고, 각 유형별 측정 결과에 가중치를 적용한다. 가중치는 기업에서 사용하고 있는 인사고과평가[11], 직무수행능력평가 및 역량평가[12]를 참조로 적용하였다. 대체적으로 기술과 역량을 보여주는 요소에 가중치가 높으며, 지식이나 태도에 대한 평가 요소에는 가중치가 낮았다. 본 연구에서는 '학습평가는 0.2, 진행평가는 0.3, 실행평가는 0.4, 근태평가는 0.1'의 가중치를 적용하

였다. 이후에 합계를 산출하면 최종 평가 점수를 다음과 같이 알 수 있다.

*총 평가 = [(학습평가*0.2)+{실습평가((진행평가*0.3)+(실행평가*0.4))}+(근태평가*0.1)]*

Ⅳ. 특화된 훈련성과 측정 모델의 적용

본 논문에서 제시한 훈련성과 측정 모델을 00훈련센터의 사이버실전훈련의 00영역훈련에 적용해 본다. 00영역훈련에서 전문과정은 파밍공격, 내부침투공격, DDoS 훈련이 주를 이루고 있으며, 훈련대상은 국가·공공기관 전산 및 보안 담당자이다.

학습평가는 다음 표 7과 같이 실습 이전에 훈련개요, 사이버공격 및 대응의 개념, 특징, 절차, 종류, 장비, 피해규모, 복구방법 등의 이론적 강의 내용을 바탕으로 습득한 지식을 평가한다. 학습평가는 훈련생이 문제의 정답을 선택하는 사지선다형보다는 훈련생 스스로 정답을 작성하고 새로운 답안을 찾을 수 있도록 유도하는 평가 방식을 선택한다. 즉, 학습 과정에서 습득한 지식을 기반으로 훈련생 나름의 축적된 지식을 창의적이고 논리적이면서도 설득력 있는 답안을 작성하도록 한다. 그래서 훈련과정별로 난이도와 변별력을 줄 수 있는 평가 문항을 개발하고 평가 방식도 문제에 맞는 정답에 따라 점수화하는 것이 아니라 평가 등급에 의해서 평가하도록 한다.

<표 7> 00영역훈련의 학습평가 적용

구분	평점	기 준
S (탁월)	10	문제 의도를 정확히 알고 있으며, 강의시간에 학습한 내용을 100% 작성하고 보다 더 창의적이고 효과적인 내용 추가
A (우수)	9	문제 의도를 정확히 알고 있으며, 강의시간에 학습한 내용의 대부분 작성
B (보통)	8	문제 의도를 알고 있으며, 단답형 형식이나 개념적인 내용을 답안으로 작성
C (미흡)	7	문제를 어느 정도 이해하고 있으며, 답안은 작성하였으나 의도한 답안을 제대로 작성하지 못함.
D (미달)	6	주어진 문제를 이해하지 못하며, 답안 작성을 하지 못함

위 표를 보면, 강의시간에 학습한 내용을 그대로 적더라도 'S(탁월)' 등급을 부여하지 않는 이유는 훈련생들로 하여금 창의적이고 획기적인 내용이나 방법을 유도하기 위함이다. 아울러 사이버실전훈련에 참가하는 훈련생들의 경우는 이론적 배경과 개념보다는 사이버공격에 대한 대응 실전훈련을 하는 만큼 실질적인 사항에 대한 문항으로 문제를 구성하는 것이 바람직하다. 다음 표 8은 00영역훈련에서 전문과정의 학습평가 문항의 예시를 보여준다.

<표 8> 00영역훈련의 학습평가 적용

평가 항목	평가 문항	평가등급					점수
		S	A	B	C	D	
DDoS 대응 훈련	1. 이상징후 발생 시 공격 근원지 확인을 위한 네트워크 증거 수집 방법을 설명하시오	10	9	8	7	6	
	2. DDoS 공격 차단을 위한 보안장비(프로그램) 2가지 이상 설명하시오.						
	3. GET Flooding 공격 방식을 설명하고 이와 유사한 피해효과를 낼 수 있는 공격 방식 하나를 설명하시오.						
파밍 대응 훈련	4. 웹서버를 통해 악성코드 감염된 사실을 알았을 경우에 가장 먼저 조치해야 할 사항을 적으시오.						
	5. 악성코드 패킷 분석도구와 분석 방법에 대해서 설명하시오(1가지)						
	6. 악성코드에 감염된 웹서버의 파일 복구 및 악성코드 제거 방법을 설명하시오.						

평가 항목	평가 문항	평가등급 S	A	B	C	D	점수
내부 침투 대응 훈련	7. PMS를 통해 악성코드에 감염이 될 경우, 피해예상 현상을 설명하시오.						
	8. 사이버공격으로 인해 MBR이 손상될 경우에 MBR 복구방법을 설명하시오.						
	9. PMS의 기능을 적으시고 PMS 보호 대책을 설명하시오.						
기타	10. 미래에 발생할 공격 방식에 대해서 자유롭게 제시하시오.						
평가 등급	**S : 매우 우수 , A : 우수 , B : 보통, C : 미흡, D : 매우 미흡**	**총계**					

진행평가는 00영역훈련이 주제별로 대응 단계 절차 실습 방식으로 진행되기 때문에 '준비-탐지-초동조치-분석-복구-보안강화' 단계별 실습이 종료될 때마다 단계별 중점 실습 내용을 기반으로 평가한다. 실행평가는 훈련과정이 종료된 후에 전체적으로 실습한 사이버공격 중에 하나를 선택하여 공격 시나리오를 부여하고 그에 따른 대응 활동을 평가한다. 이때, 실습평가는 훈련내용 이외에 새로운 방법으로 대응하였을 경우에 가산점을 부여할 수도 있다.

진행평가는 표 9와 같이 훈련단계별 훈련실습이 종료될 때마다 절차 숙지, 보안장비 활용도, 신속성, 완전성 등의 관점에서 중점 실습 내용을 평가한다. 예를 들어 DDoS 공격 대응훈련일 경우, 각 단계별로 평가표를 작성하여 측정할 수 있다. 본 논문에서는 탐지단계의 평가 문항 적용만 예를 들어 제시한다.

<표 9> 00영역훈련의 진행평가 중 탐지단계 평가 적용

평가 항목	평가 문항	평가등급 S	A	B	C	D	점수
이상 징후 탐지 (30)	1. 운영 보안장비의 활용 수준은?	10	9	8	7	6	
	2. 트래픽 현황을 제대로 모니터 하였는가? (각 보안장비별)						
	3. 운영 보안장비별 이상징후를 정확히 탐지하였는가?						

평가 항목	평가 문항	평가등급 S	A	B	C	D	점수
침해 사고 확인 (60)	4. 실시간으로 공격 정보를 확인 하였는가?						
	5. 다른 보안장비에서 탐지한 이상 징후를 확인하고 비교하였는가?						
	6. 공격명, 공격자 등에 대한 정보를 획득하였는가?						
상황 통보문 작성(10)	7. 사고내용, 특이사항 등 상황통보 문을 제대로 작성 하였는가?						
기타 (가중치)	8. 새로운 방법의 제안, 창의적인 방법을 활용하였는가?						
평가 등급	**S : 매우 우수 , A : 우수 , B : 보통, C : 미흡, D : 매우 미흡**	**총계**					

다음 표 10은 실행평가의 적용을 보여주며, 사이버공격 시나리오가 주어지면 대응 절차나 새로운 대응 방법으로 조치한 사항을 평가한다. 즉, 각 진행평가를 종합적으로 평가한다.

<표 10> 00영역훈련의 실행평가 적용

평가 항목	평가 문항	평가등급 S	A	B	C	D	점수
탐지 (25)	1. 이상징후 식별 여부 및 신속성 수준은?	10	9	8	7	6	
	2. 정확하게 침해 정보를 수집하였는가?						
초동 조치 (25)	3. 침입경로를 신속하게 차단하였는가?						
	4. 정밀 조사를 위한 데이터와 정보를 수집하였는가?						
분석 (20)	5. 로그분석을 통해 공격 유형을 정확히 확인하였는가?						
	6. 공격으로 인한 피해 시스템을 식별하였으며, 규모를 파악하였는가?						
복구 (20)	7. 복구 방법에 따라 복구절차를 수행하였으며, 정상 가동이 되었는가?						
보안 강화 (10)	8. 유형에 따른 보안정책을 업데이트 및 보안장비를 재설정하였는가?						
기타	9. 새롭거나 창의적인 방법으로 문제 해결 방안을 제안하였는가?						
평가 등급	**S : 매우 우수 , A : 우수 , B : 보통, C : 미흡, D : 매우 미흡**	**총계**					

근태평가는 훈련생이 훈련과정에 얼마나 적극적이고 성실하게 참여했는지를 측정하는 평가이다. 본 논문에서는 기업의 인사평가 방법 중에 자질평정척도법[13]을 활용한다. 이 방식은 피평자의 성실성, 적극성 등과 같은 자질을 평정척도로 측정하는 방법으로 직무성과와 관련된 일반적인 인적자질을 평가한다는 점과 평정이 쉽다는 점에서 광범위하게 활용된다. 한국의 기업에서 능력과 태도와 관련한 자질을 평가할 때 가장 많이 사용하고 있는 방법 중에 하나다. 다음 표 11은 훈련생에 대한 평가 항목 적용을 보여준다.

<표 11> 00영역훈련의 근태평가 적용

평가 항목	평가 문항	평가등급					점수
		S	A	B	C	D	
준비도	1. 훈련시간을 준수했는가?	10	9	8	7	6	
	2. 훈련과 관련된 지식을 사전에 인지하고 있는가?						
	3. 전 과정에 결처서 훈련 실습을 위한 준비를 하였는가?						
참여도	4. 훈련시간에 교수의 강의에 집중하였는가? (스마트폰을 사용하거나 다른 웹사이트에 방문한 횟수 등)						
	5. 주제별 훈련 절차대로 훈련생이 제대로 실습하였는가? (다른 보안프로그램 실행, 다른 훈련내용 진행 등)						
	6. 창의적이고 새로운 방법에 대해 진지하게 질문하고 토론하려는 태도가 있었는가?						
학습태도	7. 훈련기관의 생활 및 훈련 수칙과 규정을 제대로 이행하였는가?						
	8. 팀 프로젝트에서 훈련생의 역할을 충실히 수행하였으며, 동료들을 도와주려고 하였는가?						
	9. 훈련시간에 직무와 관련된 업무를 하지 않았는가?						
기타	10. 문제해결에 있어서 창의적이고 도전적으로 노력하였는가?						
평가등급	**S : 매우 우수 , A : 우수 , B : 보통, C : 미흡, D : 매우 미흡**	**총계**					

본 논문에서 제시한 훈련성과 측정 모델은 다음 표 12와 같이 훈련생의 훈련 참여도, 학습 이론, 문제해결 능력 부분에서 평가를 진행하고, 평가 요소는 각 평성과 측정 부분별로 특화된 요소를 도출하였다.

<표 12> 훈련생에 특화된 훈련성과 측정 모델 요소

평가유형		평가도구	수행자	평가요소	척도	배점	가중치
학습평가		시험문제	훈련생	서술형	5단계	100	0.2
실습평가	진행평가	단계별 시나리오	훈련생	수행 절차	5단계	100	0.3
	실행평가	훈련단위별 시나리오	훈련생	대응방법 및 절차	5단계	100	0.4
근태평가		평가표	교수	참여도	5단계	100	0.1

모든 평가의 배점은 각 100점으로 하여 평가 문제별 5단계의 평가척도로 구분하여 평가한다. 평가지표는 실습내용에 따라 무리없이 해결한 것을 기준으로 '탁월, 우수, 보통, 미흡, 미달'로 평가척도를 작성하였다. 또한, 사이버실전훈련의 목적은 훈련생이 사이버공격을 얼마나 신속하게 탐지하고 초동조치를 수행하며, 얼마나 정확하게 분석하고 피해시스템을 정상수준으로 복구할 수 있는 능력의 향상시키는 것이기 때문에 실습평가 부분에 상대적으로 가중치를 높게 부여하였다. 그래서 제안한 훈련성과 측정 모델은 기존의 평가 방식보다 정확하고 명확하며, 객관적인 평가 방식이라 할 수 있지만, 평가자의 평가 방식과 중점에 따라 주관적인 평가 결과가 나올 수 있는 단점도 있다.

Ⅴ. 결론

본 논문에서 제시하는 훈련생에 특화된 훈련성과 측정 모델은 00훈련센터에서 진행하는 사이버실전훈련에 참여하는 훈련생 평가에 기반을 둔다. 그래

서 사이버실전훈련 과정별 특징, 훈련 및 평가 방식에 대해서 관찰하고 분석하여 분석 결과를 기반으로 사이버실전훈련 훈련생에 특화된 훈련성과 측정 모델을 제시하였다.

사이버실전훈련에 참여한 훈련생의 훈련성과 측정 모델은 평가 시스템 설계의 기본원칙의 타당성 측면에서 평가항목의 중복성이 나타날 수 있으며, 신뢰성 측면에서 교수의 전공 및 평가중점에 따라 평가 결과가 다를 수 있는 오류도 있다. 또한, 평가체계 설계 시 주요내용에서 평가항목, 요소, 배점 등은 사이버실전훈련의 훈련생에 특화되게 맞춤형으로 설계할 수 있지만, 이 또한 평가의 객관성을 헤칠 수 있는 위험이 있다. 향후 이러한 문제점을 해결하기 위해서 국내·외 사이버훈련 평가 방법론을 연구하여 보다 객관적이고 설득력 있는 평가 방법론을 개발하고 자동화 평가 도구로 개발이 가능한 지를 검토할 것이다.

참고문헌

[1] 엄정호, “사이버보안 역량 강화를 위한 맞춤형 사이버훈련체계 개선 방안,” 보안공학연구논문지, 제12권, 제6호, 2015, pp. 567-580.

[2] 배재화·엄정호 “사이버훈련 성과 평가 방법에 관한 연구,” 디지털산업정보학회 학술대회논문지, 2016, pp. 27-29.

[3] 엄정호, “효과적인 사이버보안 교육훈련을 위한 교육과정 문제점 및 개선 방안,” 보안공학연구논문지, 제12권, 제4호, 2015, pp. 337-350.

[4] 박동철·권두순·황찬규, “NCS환경에서 ICT분야 교육에 ARCS 동기이론이 상호작용성과 학습몰입을 통해 학업성취도와 학습전이에 미치는 영향,” 디지털산업정보학회 논문지, 제11권, 제3호, 2015, pp. 179-200.

[5] http://www.nisa.or.kr/cstec/kor/html/sub02/sub0203.html, 2016.

[6] 장혜정·나현미·손희전, “중소기업 사업주 위탁훈련의 질 제고를 위한 훈련성과 평가 모델 개발,” 한국직업능력개발원, 연구보고서, 2014.

[7] 나승일, “과정이수형 자격의 평가체계 개발,” 서울대학교, 연구보고서, 2011.

[8] 이종락, “수요자 중심의 정보보호 전문 인력 양성을 위한 교육과정 설계,” 디지털산업정보학회 논문지, 제9권, 제3호, 2013, pp. 99-106.

[9] 길대환, “최신 교육훈련평가 모형을 활용한 교육성과 분석,” (주)케이엠플러스컨설팅, 연구보고서, 2012.

[10] “중소기업진흥공단 신인사제도 구축 연구,” 중소기업진흥공단, 연구보고서, 2010.

[11] “인사제도 개선 및 성과연봉제 설계,” 인천항만공사, 연구보고서, 2011.

[12] 조경호·전종순·최진식·장다정, “행정안전부 성과평가의 공정성 측정기준 개발,” 한국행정학회, 연구보고서, 2011.

[13] http://web.sungshin.ac.kr/~parkcom/class/hrm1101/chap8/images/13.hwp, 인사평가의 방법, 2016.

■ 저자소개 ■

김 기 훈
Kim Kihoon

2012년 3월~ 현재 대전대학교 군사학과 교수
2012년 2월 대한민국 육군 준장 예편
2016년 8월 대전대학교 군사학과(박사)
2003년 2월 대전대학교 사회복지학과(석사)
1980년 2월 육군사관학교 문학사

관심분야 : 군사전략, 무기체계 획득, 사이버전
E-mail : kkh1003@dju.kr

엄 정 호
Eom Jungho

2011년 3월~ 현재 대전대학교
군사학과&국가안전융합학부 조교수
2011년 3월 성균관대학교 정보통신공학부 BK21
연구교수
2010년 8월 대한민국 공군 장교
2008년 2월 성균관대학교 컴퓨터공학과(박사)
2003년 2월 성균관대학교 컴퓨터공학과(석사)
1994년 2월 공군사관학교 항공공학과(학사)

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

논문접수일 : 2016년 11월 28일
수 정 일 : 2016년 12월 07일
게재확정일 : 2016년 12월 09일