

사이버보안 인력의 효율적 관리를 위한 자격등급 모델 설계*

엄 정 호*, 김 홍 준*, 최 윤 성**

요 약

대규모 사이버공격이나 테러가 발생하여 국가가 막대한 피해를 보거나 안보에 치명적인 위협이 되었을 때에서야 비로소 사이버보안 인력 양성에 대한 사회적 관심은 높아진다. 또한, 정부에서는 사이버보안 인력 양성과 확보 정책을 제시하곤 한다. 하지만, 양성된 사이버보안 인력이 관련 기관이나 기업에 취업한 이후에 이들을 체계적으로 관리할 수 있는 시스템은 아직 미약하다. 소프트웨어 인력은 표준화된 자격등급 모델이 있어서 각 등급별로 적합한 직무를 설정하여 관리하고 있다. 사이버보안 인력도 경력, 학력, 교육훈련 실적 등을 고려한 특화된 자격등급 모델이 필요하다. 자격등급을 부여함으로써 각 등급별로 수행할 수 있는 직무를 설정하고 부서의 직책과 직위도 등급을 고려하여 부여해야 한다. 따라서 본 논문에서는 사이버보안 인력의 효율적으로 관리하기 위한 자격등급 모델을 제안한다.

An Qualification Level Model for Efficient Management of Cyber Security Workforce

Jung-Ho Eom*, Hong-Jun Kim**, Youn-Sung Choi***

ABSTRACT

When a large-scale cyber attack or terrorism occurs and the country suffers enormous damage or poses a fatal threat to security, social interest in nurturing cybersecurity workforce increases. In addition, the government often suggests policies and guideline to train cybersecurity workforce. However, the system that can systematically manage trained cyber workforce after they are employed in related organizations or companies is still weak. Software workforce has a standardized qualification level model, so appropriate jobs are set and managed for each level. Cyber workforce also need a specialized qualification level model that takes into account their career, academic background, and education&training performance. By assigning a qualification level, the duties that can be performed for each level should be set, and the position and duty of the department should also be assigned in consideration of the level. Therefore, in this paper, we propose a qualification level model for cyber security workforce.

Key words : Cyber Security, Qualification Level, Cyber Security Workforce, Cyber Index, Cyber Security Level

접수일(2022년 2월 07일), 수정일(2022년 3월 23일), 게재
확정일(2022년 3월 30일)

★ 이 논문은 2020년 대한민국 교육부와 한국연구재단의 인
문사회분야 중견연구자지원사업의 지원을 받아 수행된
연구임(NRF-2020S1A5A2A01044520).

* 대전대학교 군사학과&안보융합학과 부교수(주저자)

** 대전대학교 컴퓨터공학과 부교수(공동저자)

*** 인제대학교 AI-융합대학 조교수(교신저자)

1. 서 론

사이버보안 인력 양성을 위해서 전문대학 이상의 고등 교육기관뿐만 아니라 민간 교육기관에서도 교육이 이루어지고 있다. 또한, 정부 지원을 받는 사이버보안 인력 양성 프로그램을 포함하여 지역 협력연구센터 등을 통해서도 고급 인력을 양성하고 있다[1-3]. 하지만 양성된 사이버보안 인력이 연구기관이나 기업에 취업한 이후에 체계적으로 관리할 수 있는 제도나 프로그램이 부족한 실정이다. 범용 소프트웨어 분야에서는 ITSQF(IT Sectoral Qualifications Framework)[4]처럼 인력의 지식, 기술, 능력 등을 평가하여 등급을 결정하는 다양한 자격등급 모델이 있다[1]. 사이버보안 분야에도 양성된 인력을 대상으로 경력, 학력, 교육훈련 등의 요소를 고려하여 자격등급 제도를 수립할 필요가 있다. 그래서 보안분야의 직책/직위, 그리고 직무를 부여할 때 사이버보안 인력의 등급을 고려사항으로 활용할 수 있다.

본 논문에서는 양성된 사이버보안 인력의 체계적인 관리를 위해서 ITSQF와 국가직무능력표준(NCS: National Competency Standards)을 기반으로 자격등급 모델을 설계하고자 한다. 제안하는 자격등급 모델의 구성 요소는 ITSQF의 평가 요소를 근간으로 하고 자격등급 수준은 ITSQF와 NCS 등급을 균형있게 반영한다. 2장에서는 소프트웨어 인력 수준 모델을 설명하고 3장에서 사이버보안 인력의 자격등급 모델을 제안한다. 4장에서는 예시를 들어 자격등급 모델을 평가하고 5장에서 결론을 맺는다.

2. 소프트웨어 인력의 역량 등급체계

소프트웨어 분야에서는 소프트웨어 인력에 대한 다양한 자격등급제도가 있다. IT 산업 현장에서 직무를 수행하는 데 필요한 능력을 국가가 표준화한 NCS, IT 산업 분야의 역량 인정 체계인 ITSQF, 소프트웨어산업 진흥법에 명시된 소프트웨어 기술자의 기술등급 및 인정 범위가 대표적이다. 소프트웨어 인력의 역량과 자격등급 제도를 살펴봄으로써 사이버보안 인력의 자격등급 모델에 포함될 수 있는 요소와 평가 기준을 도출하고자 한다.

2.1 NCS 수준 체계[5,6]

국가직무능력표준은 산업 현장에서 직무를 수행하는 데 필요한 능력(지식, 기술, 태도)을 국가가 표준화한 것이다. 또한, 산업 현장, 교육 훈련, 자격을 연계하고 평생학습능력 성취 단계를 제시하며, 자격의 수준 체계를 구성하는데 활용된다. 국가직무능력표준 개발시 8단계의 수준체계에 따라 능력 단위 및 능력 단위 요소별 수준을 평정하여 제시하고 있다. NCS 체계는 8단계로 구성되어 있으며, 각 수준별 정의를 명시하고 있다. 수준별로 구분하기 위해서 지식 및 기술 수준, 역량 수준, 경력 요소로 평가하고 있다. 세부 수준 체계는 참고문헌 [5,6]에서 확인할 수 있다.

2.2 ITSQF[4,7]

ITSQF는 IT 산업분야의 역량 인정 체계로 역량에 관련된 학력, 자격, 현장경력 및 교육훈련, 대회수상 경력 등을 종합적으로 반영하여 소프트웨어 기술자의 역량 수준을 평가한다. ITSQF의 역량 인정 요소는 학력, 자격, 교육훈련, 현장 경력으로 구분한다. ITSQF의 역량 요소의 인정은 IT 유관학과 졸업과 IT 유관 업무를 수행한 현장경험일 경우에 인정되며, 자격, 교육훈련 등 모든 역량 인정 요소는 SW 분야와 관련성이 있어야 하며, 공식적이고 객관적으로 증명이 되어야 한다. 역량 인정 요소의 정의는 다음과 같다.

학력은 IT 유관학과를 졸업해야 하며 학사는 J5, 석사는 I6, 박사는 A8의 수준부터 인정한다. 해당 학위의 관련 직종에서만 그 수준을 인정하며, IT 분야의 학위가 아니거나 특정 직종과 무관한 경우 해당 학력을 인정하지 않는다.

자격은 국가자격증인 IT 관련 산업기사, 기사, 기술사의 경우 각각 J3, J5, A8 수준으로 인정해주고 있으며, IT 기술자들이 취득하는 여러 자격증은 객관적으로 파악하기 위해 IT 관련 전문가 집단의 심사를 거쳐 해당 자격의 수준을 인정하는 자격인정제도를 도입하고 있다. 자격의 수준을 인정하는 판단은 해당 자격시험의 세부항목이 연관된 직무능력 요구치를 충족할 수 있는가를 측정하여 이루어진다.

교육 훈련은 IT 기술자들이 졸업 이후 학습하는 교육 훈련을 인정하되, 특정 수준에서 상위수준으로 이

동하는데 필요한 필수 교육 단위를 이수해야 하고 상 위수준으로 올라가기 위해서는 50시간의 교육과정을 반드시 이수하여야 한다.

현장 경력은 유관 직무를 수행한 현장 경력이 객관적으로 이루어질 경우에 해당 직종의 역량을 인정하고 직종 간의 인정 비율을 통해 표준 경력 연차를 산출한다. IT 유관회사에서 경력을 쌓더라도 해당 직종의 직무와는 직접적인 연관성이 없는 직무를 수행하는 경우를 고려하여 산정한다. 직종 간의 경력인정 비율은 상위 수준으로 올라갈수록 인정 비율이 조금씩 낮아지도록 설계되었다.

ITSQF는 SW 기술자의 역량을 1~9단계로 구분하고 각 단계별 요구 능력을 정의하고 있다. 기존 NC S 기반의 SW 기술자의 역량을 9개 수준으로 재분류하고, 각각의 등급에 필요한 경력, 학력, 자격요건을 매핑한다.

2.3 소프트웨어 기술자의 기술등급[8]

소프트웨어산업 진흥법 시행령에 명시되었던 기술 등급은 최근 개정령에는 삭제되었으나, 아직까지 SW 기술자 등급 체계를 개발하고자 할 때는 참고하고 있다. 소프트웨어 기술(기능) 분야의 업무를 수행하는 소프트웨어 관련 해당 분야에서 계획·설계·개발·시험·운영·유지보수·감리 등의 업무를 수행한 자를 말한다. SW 기술자 등급체계는 각 기술자격자와 학력/경력자별로 수준에 따라 등급을 결정하며, 기술사를 제외한 7등급으로 구분된다.

기술자격자는 국가기술자격법의 기술자격종목 중 정보처리 분야 기술자격을 취득한 자 또는 자격기본법등 관계 법령에 따라 인증된 공인민간자격 중 지식경제부장관이 고시하는 자격을 취득한 자를 말한다. 경력인정 방법 및 절차 등은 지식경제부장관이 정하며, 지식경제부장관은 공인민간자격을 단계별 등급으로 분류(초급·중급 등)하여 고시한다.

학력·경력자는 해당 전공학과의 범위, 교육기관, 경력인정 방법 및 절차 등에 따라 구분한다. 첫째, 초·중등교육법 또는 고등교육법에 따른 해당 학교에서 소정의 과정을 이수하고 졸업한 자, 둘째, 그 밖의 관계 법령에 따라 국내 또는 외국에서 가목과 동등 또는 그 이상의 학력이 있다고 인정되는 자, 셋째, 지식경제

부장관이 정하는 교육기관에서 소정의 소프트웨어 기술(기능) 관련 교육과정을 이수한 자, 마지막으로 그 밖에 소프트웨어기술(기능)을 가진 자로서 소프트웨어사업자 신고업체 및 소프트웨어 기술(기능)분야에서 일정기간 근무한 자로 구분한다. 소프트웨어 기술자의 기술 등급의 세부 내용은 참고문헌 [8]에서 확인할 수 있다.

3. 사이버보안 인력의 자격등급 모델 설계

3.1 자격등급 모델의 필요성

자격은 직무를 수행함에 있어서 요구되는 능력과 자질을 의미한다. 소프트웨어 분야에서 역량 등급, 기술등급 등의 자격등급제도를 운영하는 것은 소프트웨어 개발, 운영, 시험 및 평가, 관리 및 감독 등의 각 직무를 수행하는데 필요한 능력과 자질을 요구하고 있기 때문이다. 예를 들어, 현장 경험이나 교육훈련 기간이 많지 않은 소프트웨어 인력이 소프트웨어 프로젝트 매니저 직무를 수행하기에는 사실상 힘들다. 사이버보안 분야도 마찬가지이다. 정보보안 시스템이나 프로그램 설계, 개발, 운용, 시험 및 평가, 보안 프로젝트 매니저 등의 직무를 수행하기 위해서는 요구되는 능력과 자질을 갖추어야 한다. 행정규칙 ‘보안관제 전문기업 지정 등에 관한 공고(2016.11.16.)[9]에는 보안관제 인력에 대한 자격 기준을 명시하고 있다. 보안관제 인력의 자격 기준은 4단계로 구분하였으며, 관련 자격 및 학력, 관련 자격 및 비관련 학력으로 구분하여 학력, 자격증, 경력 요소로 평가하고 있다. 하지만 자격 기준의 내용을 보면 보안관제에 특화되었다기보다는 일반적인 정보보안 관련 자격 기준에 가깝다.

사이버보안 인력의 자격등급도 소프트웨어 인력의 자격등급과 마찬가지로 직무 수행에 요구되는 능력과 자질을 자격등급으로 명시함으로써 해당 직무에 필요한 자격등급을 갖춘 인력에 의해 수행할 수 있게 한다. 아울러 모든 직책과 직위가 요구하는 역량을 자격등급으로 명시함으로써 인력이 원하는 직책과 직위로 이동하기 위해서 해당 자격등급을 취득하기 위해서 개인적인 역량 향상에 매진할 수 있도록 해준다. 기업이나 연구소 등에서 유사한 사이버보안 직무를 수행할 때 필요한 역량을 표준화시킬 수 있다. 마지막으로

사이버보안 인력의 체계적인 인사관리나 성과관리에 기반자료로 활용할 수 있다.

3.2 자격등급 모델의 설계 요구사항

사이버보안 인력의 자격등급 모델의 신뢰성과 객관성을 보장하기 위해서는 다음과 같은 요구사항을 충족해야 한다.

첫째, 자격등급 모델의 등급 구분이다. 연구를 진행하면서 관련 연구문헌을 찾아본 결과 대부분 IT 관련 자격등급을 5등급으로 분류하였다. 광미선의 박사학위 논문인 '소프트웨어 개발자의 전문성 발달 수준과 교육훈련, 자격 및 직무경력의 관계(2016)[10]'에서의 개발자 전문성 발달 수준, Dreyfus의 학술논문인 'A FIVE-STAGE MODEL OF THE MENTAL ACTIVITIES INVOLVED IN DIRECTED SKILL ACQUISITION(1980)[11]'에서 전문성 발달 단계, 그리고 '소프트웨어 인력의 노임단가 등급[12]'에서 자격등급을 <표 1>과 같이 5등급으로 분류하고 있다.

<표 1> 자격등급의 역량 등급

개발자 전문성 발달 수준	전문성 발달 단계	SW 인력의 노임단가 등급
초급 개발자	Novice	초급 기술자
중급 개발자	Competence	중급 기술자
고급 개발자	Proficiency	고급 기술자
특급 개발자	Expertise	특급 기술자
개발 전문가	Mastery	기술사

둘째, 자격등급 모델의 구성요소 선정이다. ITSQF의 역량 인정 체계와 NCS 수준체계, 강성미의 학술논문 '국내 건설사업관리 기술인력 역량평가 개선 모델(2020)[13]'에서 평가 요소로 학력, 경력, 자격, 교육 훈련 등을 사용하였으며, 보안관계 인력의 자격 기준에도 학력, 경력, 자격은 포함하고 있다. 본 논문에서도 구성요소로 학력, 경력, 자격, 교육훈련으로 선정하였다.

셋째, 각 구성요소별 평가점수의 배분이다. 공군의

'공군 소프트웨어 인력관리 표준방안 연구[14]'에서 전문가의 설문조사를 통한 공군 SW 인력 자격등급제도의 평가요소별 가중치 선정 결과와 국내 건설사업관리 기술인력 역량평가 개선 모델에서의 평가요소별 가중치를 참조하였다. 평가요소별 점수는 100점 만점 기준으로 경력 35점, 교육훈련 25점, 자격 20점, 학력 20점으로 결정한다.

넷째, 모델의 구성요소 내에서 세부 평가요소의 질적인 측면 평가 방법이다. 본 논문에서는 정량적인 평가 이외에 정성적인 평가가 필요한 부분은 보정계수를 활용한다. 보정계수는 학력, 자격, 교육훈련, 경력 요소에 모두 적용되며, 보정계수의 범위는 다음 단계의 점수 이상으로 올라가거나 아래 단계의 점수 이하로 내려가지 않도록 한다.

다섯째, 정규 교육기관이 아닌 사이버보안 전문 교육기관에서 받은 교육의 평가 방법이다. 사이버보안 인력을 양성하기 위해서 정부 주도로 짧게는 3~6개월, 길게는 12개월 진행되는 교육과정이 있다[1]. 이러한 교육은 대부분 정규교육을 받은 인력들이 보안기술을 보다 더 심층있게 배우기 위해서 입학하기 때문에 학력에 포함시킬 수 없다. 또한, 자격등급을 유지하기 위한 단기 교육이 아니기 때문에 교육훈련에 포함시킬 수 없다. 그래서 본 논문에서는 장기 집중형 교육과정은 경력에 포함시켜 6개월 미만은 1년, 6개월 이상은 2년 경력으로 산정한다.

여섯째, 해킹 방어 대회나 특허 등록 등이 실적에 대한 평가 방법이다. 여러 참고문헌을 살펴본 결과 실적은 대부분 가산점으로 적용하고 있어서 본 논문에서도 가산점으로 평가한다.

마지막으로 보정계수 결정, 전문 교육기관 교육, 실적 등에 대한 평가를 보다 객관적으로 평가하기 위해서 자격등급평가위원회를 설치하여 위원회의 의견을 수렴하도록 한다.

3.3 사이버보안 인력 자격등급 모델 설계

자격등급 모델은 <표 1>의 자격등급의 역량 등급에서 대부분 5등급으로 구분한 바, 본 논문에서도 동일한 5등급으로 구분하되, 단계는 4급, 3급, 2급, 1급, 특급으로 구분한다. 구성요소는 요구사항에서 제시한

경력, 자격, 학력, 경력으로 하며, 이 외에 반영될 요소는 가산점을 부여한다. 구성요소별 가중치는 공군 소프트웨어 인력의 자격제도에서 제시한 경력(35), 교육훈련(25), 자격(20), 학력(20)을 준용하기로 한다. 이는 소프트웨어 인력이나 사이버보안인력이 수행하는 직무가 소프트웨어 개발 계획, 설계, 프로그램, 시험 및 평가, 운용, 관리 및 감독 등 큰 차이가 없기 때문이다.

3.3.1 자격등급 모델의 구성요소

경력(은 사이버보안 관련 직무를 수행한 경험으로 입사 초기에는 근무 연수에 따라 기술 수준의 차이가 나기 때문에 점수차이를 크게 하고 근무 연수가 많을수록 경력에서 점수차이를 적게 한다. 이를 위해서 로그값을 이용하며, 이러한 방식을 사용한 건설기술인 역량지수의 경력 산정 공식[13]을 참고한다. 건설기술인의 경력 산정 방식은 경력 초기에는 연차별로 차이를 두다가 일정 경력기간에 도달할 때는 연간 점수 차이가 나지 않는다. 4급 기술자와 3급 기술자의 직무 경험은 자격에 영향을 미칠 수 있으나, 일정 경력기간이 지나면 직무 경험이 역량에 크게 영향을 미치지 않는다는 것을 의미한다. 본 연구에서는 최대 근무 연차를 20년으로 정했지만, 적용하는 기관에 사정에 따라 정할 수 있다. 경력에서 고려할 사항은 사이버보안 직능에서 첨단 보안기술 개발과 행정업무를 구분하고자 한다. 다른 연구에서도 주 직능 업무와 행정업무는 구분하고 있다. 본 연구에서는 차세대/스마트/지능형 보안기술 개발 TF 직무에는 1.1, 행정 직무는 0.9의 보정계수()를 적용한다.

$$\text{경력 점수} = \frac{\log_{=1}^n (\gamma_n)}{\log 0} \times 35$$

여기서, n은 근무 연수, γ 는 보정계수이다. 교육훈련은 취업 이후의 수료한 교육훈련을 인정하되, 연간 최소 교육훈련 이수 시간을 정한다. 국가정보원은 매년 정부기관과 공공기관 등을 대상으로 정보보안관리실태평가[15]를 실시하는데, 평가 항목 중에 정보보안 교육 항목에서 1인당 연간 최소 교육시간을 40시간 이상으로 정하고 있다.

1년간 교육훈련 시간이 40시간을 초과하더라도 최대치를 연간 40시간으로 정한다. 이는 사이버보안 인력의 지속으로 역량을 유지하기 위해서 매년 교육훈련을 받도록 유도하고자 함이다. 교육훈련 요소의 평가 방식은 <표 2>와 같다.

<표 2> 교육훈련 점수

점수	기준(%)	평가 방식
25	100	$n \sum_{h=1}^n (h_n \times \gamma) / (n \times 40)$ <p>n : 근무 연차 h : 교육훈련 시간 Y: 보정계수 * 교육훈련 시간은 연차별로 계산</p>
24	95~99	
23	90~94	
22	85~89	
21	80~84	
20	75~79	
19	70~74	
18	65~69	
17	60~64	
16	55~59	
15	50~54	
:	:	

교육훈련에서 보정계수는 사이버보안 SW 개발 관련 교육과 일반 교육, 그리고 교육과정의 이론과 실습 구성 비율을 고려하여 설정한다. 우선 사이버보안 SW 개발 교육은 SW 설계, 분석, 코딩, 실험 등 실습 중심의 교육과 사이버공방훈련 참여는 중요도가 높기 때문에 보정계수를 1.1로 정하고 일반 사이버보안 교육훈련 중에서 이론 비중이 70% 이상이면 보정계수를 0.9로 정한다. 교육내용의 이론과 실습 비율 결정은 자격등급평가위원회에서 결정할 수 있다.

자격은 SW 인력의 자격등급 모델에서 적용하고 있는 SW 관련 국가기술 자격증의 등급에 따라 기능사, 산업기사, 기사, 기술사로 구분하며, <표 3>과 같이 배정한다. 현재 사이버보안과 직접적으로 관련된 국가기술 자격증은 정보보안기사와 정보보안산업기사가 있다. 기술사 중에서는 정보관리기술사의 출제기준에 정보보안이 포함되어 있다. 그리고 정보처리 기능

사·산업기사·기사에서 보안 관련 사항이 출제되므로 관련 있는 자격증이라 할 수 있다.

<표 3> 자격증 점수

자격증	점수
기술사	20
기사	16
산업기사	13
기능사	10

국내 민간단체에서 발급한 자격증과 국제공인 자격증은 자격등급평가위원회에서 유사 국가기술자격증에 해당하는 점수를 부여한다. 1인이 다수의 자격증을 보유한 경우에는 보정계수를 활용하여 점수를 부여한다. 다만, 사이버보안 계열 자격증이 다수일 경우에는 최상위 자격증 점수만 부여한다. 계열이 서로 상이한 자격증이 다수일 경우에는 최상위 자격증 기준으로 보정계수 1.05를 적용하고, 자격증 등급이 동일하고 계열이 서로 다를 경우에는 자격증 해당 등급 기준으로 보정계수 1.1을 적용한다.

학력은 대부분의 자격등급 모델의 학력 기준을 고졸, 전문학사, 학사로 구분하고 있기 때문에 본 연구에서도 고졸, 그리고 정보통신 계열 전문학사, 학사로 구분하여 <표 4>와 같이 점수를 부여한다.

<표 4> 학력 점수

학위	점수
학사	20
전문학사	16
고등학교	11

사이버보안 인력의 자격등급 모델이지만, 전국 대학(전문대학 포함)에 설치된 정보보안 관련 학과가 많지 않기 때문에 전문학사와 학사는 정보통신 계열 학위를 대상으로 한다. 다만, 정보보안 관련 특목고나 학과를 졸업할 경우에는 보정계수를 활용하여 가산치를 부여한다. 석사와 박사 학위, 그리고 정보보안 계열 전공은 보정계수를 활용하여 <표 5>와 같이 가중치를

부여한다. 석사와 박사 학위는 정보보안 계열과 정보통신계열을 구분하여 보정계수를 적용하며, 전문학사 및 학사 학위에서도 정보보안 전공은 보정계수를 활용하여 가중치를 부여한다. 고등학교는 정보통신계열 특목고를 졸업할 경우에 보정계수를 활용하여 가산 점수를 부여한다.

<표 5> 학력 보정계수

학위	보정계수
정보보안 계열 박사	학사×1.2
정보보안 계열 석사	학사×1.15
정보보안 계열 학사	학사×1.1
정보보안 계열 전문학사	전문학사×1.1
정보통신 계열 특목고	고졸×1.3
정보통신 이외 전공	해당 학위×0.9

가산점은 보안관련 대회 입상과 특허 등록 실적을 고려하여 배점하되, 3점 이내로 한다. 예를 들어 국의 대회 입상은 3점, 전국대회 입상은 2점, 지방대회 입상은 1점, 국제 특허 등록은 2점, 국내 특허 등록은 1점으로 할 수 있다. 다른 자격등급 모델에서도 가산점을 부여하는 경우에는 3점 이내로 하고 있으며, 제한한 자격등급 모델의 요소별 등급간 점수 차이도 1~3점이기 때문에 가산점으로 인해서 자격등급이 바뀌지 않게 하려 함이다. 또한, 동일한 성과에 대해서는 가산점을 한 번만 적용하고 최대 3점을 초과하지 않도록 한다. 이 외의 가산점을 부여할 수 있는 개인성파나 가산점의 유효기간은 자격등급평가위원회에서 결정할 수 있다.

3.3.2 자격등급 모델의 평가 및 등급

평가는 100점 만점 기준으로 경력은 35점, 교육훈련은 25점, 자격은 20점, 학력은 20점으로 정한다. 구성요소별 점수는 각 25점 기준으로 각 구성요소별 중요도와 가중치를 공군 소프트웨어 인력관리 표준방안 연구에서 전문가 설문조사 결과를 반영하여 결정하였다. 또한, 해킹대회 수상이나 특허 등록 등에 대한 실적은 자격등급평가위원회에서 가산점(a)으로 적용 여부와 점수를 결정한다.

자격등급 점수(100점) = [경력(35점) + 교육훈련(25점) + 자격(20점) + 학력(20점)] + α

<표 6> 자격등급 모델의 구성요소별 평가

요소		배 점			
경력 (35)	기준	$\log_{=1}^n (\gamma_n) \times 35$			
	점수	* n: 근무 연차, γ: 보정계수			
교육 훈련 (25)	기준	$\sum_{n=1}^n (h_n \times \gamma) / (n \times 40)$			
	점수	* n: 근무 연차, h: 교육훈련 시간, γ: 보정계수 * 교육훈련 시간은 연차별로 계산			
자격 (20)	기준	기술사	기사	산업기사	기능사
	점수	20	16	13	10
학력 (20)	기준	학사	전문학사	고등학교	
	점수	20	16	11	
가산 점(a)	기준	사이버보안 대회 입상 및 특허 등록			
	점수	3	2	1	

사이버보안 인력의 자격등급은 앞서 설명한 바와 같이 5등급으로 구분하며, ITSQF와 NCS 수준과도 유사하게 단계별로 등급을 설정하였다. 등급별 점수 구간은 경력, 자격, 학력을 기준으로 자격등급 분포도가 항아리 모형 비율[6]이 될 수 있도록 설정하였다.

<표 7> 자격등급 모델의 등급

등급	점수	비 고
특급	95점 이상	ITSQF 수준 9 NCS 수준 L8 상위
1급	90점 ~94점	ITSQF 수준 7~8 NCS 수준 L8
2급	85점 ~89점	ITSQF 수준 5~6 NCS 수준 L6~7
3급	76점 ~84점	ITSQF 수준 2~4 NCS 수준 L3~5
4급	65점 ~75점	ITSQF 수준 1 NCS 수준 L1~2

4. 자격등급 모델의 적용

예를 들어 <표 8>과 같은 사이버보안 인력이 있다고 가정하고 제안한 사이버보안 인력의 자격등급 모델을 적용하여 자격등급을 산출하면 <표 9>와 같은 결과를 갖는다.

<표 8> 사이버보안 인력 이력 예시

구분	A 개발자	B 개발자
근무 기간	3년 (임사후 지능형 보안 기술 개발 TF 근무)	8년 (3년차에 인사팀 근무)
교육 훈련	1차년도:30시간 (사이버보안훈련) 2차년도:60시간 (알고리즘 개발 교육) 3차년도:20시간	1차년도:30시간 2~7차년도:매 년 40시간 초과 8차년도:40시간 (보안관리자 과정으로 이론 중심 교육)
자격증	정보보안기사 CISSP 자격	정보보안기사
학위	컴퓨터공학과 대졸	대학원 (정보보안학과)
기타	코드게이트 준우승	알고리즘 국내 특허 등록

A 개발자는 경력 점수는 근무기간이 3년이고 기술 개발 TF에서 근무하였기 때문에 보정계수 1.1을 곱해서 산정한다. 보정계수를 적용하지 않으면 12.8점이나 보정계수를 적용하여 13.9점으로 산정된다. 교육훈련 점수는 1차년도와 2차년도에는 실습 교육과 훈련 참여로 인해서 보정계수 1.1을 적용한다. 1차년도는 보정계수를 적용하여 33시간, 2차년도는 최대 40시간을 이미 초과하였기 때문에 40시간으로 하며, 3차년도에는 20시간으로 하면, 교육훈련 시간은 총 93시간으로 3년 120시간 기준으로 약 78% 달성하였으며, 점수는 20점이 된다. 자격 점수는 기사 16점, CISSP 자격증은 국제공인 자격증으로 자격등급평가위원회를 통해서 보정계수 1.1를 적용토록 하면 17.6점을 부여되어 이 중에 가장 높은 점수로 하여 17.6점이 된다. 학력은 학사학위 소지자이기에 20점을 부여한다. 기타 사항으로 국제해킹대회인 코드게이트에서 준우승한 기록이 있어서 가산점 3점을 부여한다. A 개발자는 경력 13.9점, 교육훈련 20점, 자격 17.6점, 학력 20점, 가

산점 3점으로 총 74.5점으로 4급에 해당된다.

B 개발자는 경력 점수는 8년 근무 중에 행정(인사팀) 직무를 1년 수행하여 1년은 보정계수 0.9를 적용하여 총 7.9년이 되고 계산하면 24점이 된다. 교육훈련 점수는 8년차에 이룬 중심 교육으로 보정계수 0.9를 적용하면 36시간이 된다. 8년동안 교육훈련 시간은 306시간으로 8년 320시간 기준 95% 달성하여 24점이 부여된다. 자격 점수는 기사 자격증 보유자로 16점이 부여된다. 학력 점수는 사이버보안 계열 석사 학위자로 보정계수 1.15를 적용하면 23점이 된다. 가산점은 국내 특허 등록이 있어서 1점이 부여된다. B 개발자는 경력 24점, 교육훈련 24점, 학력 23점, 자격 16점, 가산점 1점으로 총 88점으로 2급에 해당된다.

<표 9> 사이버보안 인력 등급 평가 결과

구분	A 개발자	B 개발자
경력	13.9점	24점
교육훈련	20점	24점
자격	17.6점	16점
학력	20점	23점
가산점	3점	1점
총점수	74.5점	88점
등급	4급	2급

ITSQF의 SW 기술자 역량 인정 체계로 B 개발자의 역량을 평가했을 경우에 경력 8년, 기사자격증, 교육훈련시간 초과 등을 고려했을 때, I6 수준 이상으로 5단계 이상으로 판단된다. <표 7>의 자격등급의 모델 등급을 살펴보면, 사이버보안 인력의 자격등급이 2급일 경우에 ITSQF의 SW 기술자의 5~6단계에 해당됨으로 제안한 자격등급 모델이 유효성을 갖는 것으로 판단된다. 각 개발자들에게 소프트웨어 개발 주기 기준으로 직무를 부여한다면, A 개발자는 구현 단계에서 코딩을 수행할 수 있는 수준이며, B 개발자는 계획 및 분석, 구현 단계에서 직무를 수행할 수 있는 수준이다.

5. 결 론

정보보안 연구, 개발, 산업체에서는 해마다 사이버보안 인력이 부족하고 이직률이 높다는 의견들이 많다. 그렇기 때문에 대학이나 민간 사이버보안 인력 양성기관에서는 사이버보안 인력 양성에 집중하고 있다. 하지만 사이버보안 인력 양성만큼이나 중요한 것은 사이버보안 인력이 전문성을 확보하고 역량을 증진시킬 수 있는 효율적인 관리이다. 사이버보안 인력을 관리하기 위해서는 개개인마다 역량을 확인하고 역량에 맞게 직무를 부여하며 성과를 창출할 수 있도록 해야 한다. 사이버보안 인력의 역량 관리는 IT 분야에서 실시하는 자격등급 모델을 활용해도 된다.

본 연구에서는 ITSQF와 NCS 수준 모델을 기반으로 사이버보안 인력의 자격등급 모델을 설계하였다. 자격등급 모델은 5등급으로 구분하였으며, ITSQF와 NCS 수준을 고려하여 등급별 점수를 결정하였다. 자격등급 모델은 경력, 교육훈련, 학력, 자격으로 구성되며, 각 구성요소의 중요도에 따라서 평가 점수를 다르게 하였다. 또한, 구성요소별 평가 내용에 따라 가중치를 적용하기 위해서 보정계수를 활용하였으며, 자격등급평가위원회를 두어 보정계수의 활용 여부를 결정하도록 하였다. 설계한 자격등급 모델은 전체적인 프레임워크와 평가 방식을 제안하였기 때문에 조직에서 활용할 경우에는 각 조직에 사이버보안 직무 특성과 환경을 고려하여 구성요소를 유연하게 조절하면 된다.

참고문헌

- [1] “2020 국가정보보호백서”, 국가정보원, 2020.
- [2] 김인중, 이수진, “국방 디지털 전환에 따른 사이버역량 강화 방안 연구”, 융합보안논문지, 제21권 4호, pp.3-13, 2021.
- [3] 박혜민, 이재균, 이창무, “대학생 보안의식 함양을 위한 보안교육 프로그램 제안에 관한 연구”, 융합보안논문지, 제21권 5호, pp.107-119, 2022
- [4] 안성원, 유호석, “ITSQF기반 SW 기술자 경력관리 체계 개선 방향”, 소프트웨어정책연구소 이슈 리포트, 제2017-008호, 2018.

- [5] <https://www.ncs.go.kr/th01/TH-102-001-03.scdo>, “NCS 구성”, (검색일: 2021.10.04).
- [6] “2021년 NCS 국가직무능력 표준 교육 및 홍보자료”, 한국산업인력공단 국가직무능력표준원, 2021.
- [7] “IT 분야 역량체계(ITSQF) 직무기술서”, 한국소프트웨어산업협회, 2018
- [8] <https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=136038#0000> (검색일: 2021.10.05).
- [9] <https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000077371#AJAX> (검색일: 2022.3.05).
- [10] 광미선, “소프트웨어 개발자의 전문성 발달 수준과 교육훈련, 자격 및 직무경력의 관계”, 서울대학교 대학원 박사학위논문, 2016.
- [11] Stuart E. Dreyfus and Hubert L. Dreyfus, “A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition”, Research Report, 1980.
- [12] <https://it.smplatform.go.kr>, “공급기업 투입인력 등급기준 및 등급별 직접인건비 단가”, (검색일: 2022.01.21.).
- [13] 강성미 외 5명, “국내 건설사업관리 기술인력 역량평가 개선 모델”, 한국건설관리학회 논문집, 제21권 제2호, pp.47-58, 2020.
- [14] “공군 소프트웨어 인력관리 표준방안 연구”, 공군본부, 2021.
- [15] “정보보안관리실태평가집”, 국가사이버안전센터, 2021.

[저 자 소 개]



엄 정 호 (Jung-Ho Eom)
 1994년 2월 공군사관학교 항공공학과 학사
 2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
 2008년 2월 성균관대학교 컴퓨터공학과 박사
 1994년 3월~2010년 8월 : 대한민국 공군 장교
 2010년 9월~2021년 2월 : 성균관대학교 정보통신공학부 연구교수
 2011년 3월~현재 대전대학교 군사학과&안보융합학과 부교수
 email : eomhun@gmail.com



김 홍 준 (Hong-Jun Kim)
 2004년 2월: 한국과학기술원 전자전산학과 학사
 2007년 2월: 한국과학기술원 전자전산학과 석사
 2014년 2월: 한국과학기술원 전기및전자공학과 박사
 2014년 2월~2015년 4월: 삼성전자 책임연구원
 2015년 5월~현재: 대전대학교 컴퓨터공학과 부교수
 email : hjkim99@dju.kr



최 윤 성 (Youn-Sung Choi)
 2006년 2월 : 성균관대 정보통신공학부 학사
 2007년 8월 : 성균관대학교 전자전기 컴퓨터공학부 석사
 2013년 2월 : 경북대학교 법학전문대학원 형법전공 박사수료
 2015년 8월 : 성균관대학교 전자전기 컴퓨터공학부 박사
 2010년 6월~2013년 5월 : 육군3사관학교 정보공학과 조교수
 2016년 3월~2020년 2월 : 호원대학교 사이버보안학과 조교수
 2021년 3월~현재 : 인제대학교 AI융합대학 (산업보안전공) 조교수
 email : cys2020@inje.ac.kr