Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1167

사이버보안 기술적 대응 직무 역량 프레임워크 제안 및 적용 모델 구현 사례

홍 순 좌,[1†] 박 한 진,[2‡] 최 영 한,[3] 강 정 민[4]
[1,3,4]사이버안전훈련센터 (책임연구원, 실장, 센터장), [2]ETRI부설연구소 (선임연구원)

A Proposal of Cybersecurity Technical Response Job Competency Framework and its Applicable Model Implementation

Soonjwa Hong,[1†] Hanjin Park,[2‡] Younghan Choi,[3] Jungmin Kang[4]
[1,3,4]Cyber Security Training and Exercise Center (Principal Researcher, Manager, Director),
[2]The Affiliated Institute of ETRI (Senior Researcher)

요 약

해킹, 말웨어, 자료 유출 및 도난 등의 사이버 위협은 생활 및 경제, 국가 안보의 중요한 문제가 될 정도로 일상과 밀접한 상황에 직면하고 있다. 국가·산업 차원의 안보 및 경제적 관점에서 사이버 위협 대응은 필수적인 방어책으로 인식하고 있으나, 사이버보안 분야에서의 산·학 기술격차 및 전문인력 부족 문제는 매우 심각한 상황이다. 본 논문에서는 이를 극복하는 방법으로 사이버보안 인력의 직무 역량 개념을 도입하여 사이버보안 기술적 대응 직무 역량(CtrJC) 프레임워크를 제안하고, 국가 및 조직 차원에서 시급히 요구되는 실시간 사이버 위협 대응 기술적 직무 역량(CtrJC-R) 모델을 구현하여 그 타당성을 확인한다.

ABSTRACT

We are facing the situation where cyber threats such as hacking, malware, data leakage, and theft, become an important issue in the perspective of personal daily life, business, and national security. Although various efforts are being made to response to the cyber threats in the national and industrial sectors, the problems such as the industry-academia skill-gap, shortage of cybersecurity professionals are still serious. Thus, in order to overcome the skill-gap and shortage problems, we propose a Cybersecurity technical response Job Competency(CtrJC) framework by adopting the concept of cybersecurity personnel's job competency. As a sample use-case study, we implement the CtrJC against to personals who are charged in realtime cybersecurity response, which is an important job at the national and organization level, and verify the our framework's effects. We implement a sample model, which is a CtrJC against to realtime cyber threats (We call it as CtrJC-R), and study the verification and validation of the implemented model.

Keywords: Cybersecurity Competency, AMCJT, CtrJC, CtrJC-R

I. 서 론

초고속 인터넷 및 무선 통신과 IT 기술의 급속한 발전은 사람들을 사이버공간에 더욱 의존하도록 만들었다. 이와 같은 환경에서 해커들의 사이버 공격은 개인 및 조직에 큰 피해를 야기하고 있으며, 심지어 국가 안보에도 많은 영향을 주므로 국가 차원의 사이버 위협 대응이 국가 생존의 중요한 분야로 자리 잡고 있다. 또한 자율주행차, 무인비행체, 로봇, 인공지능, 빅데이터 등의 4차 산업 시대에 요구되는 IT

Received(09. 07. 2020), Accepted(10. 21. 2020)
† 주저자, hongsj@nsr.re.kr
‡ 교신저자, hjpark@nsr.re.kr(Corresponding author)

인력의 부족도 문제에 직면하고 있으나, 사이버보안 인력의 부족은 더욱 심각한 상황에 직면하였다.

1.1 연구배경

Enterprise Strategy Group에서 발표한 조사에 따르면, 응답한 IT 전문인력의 절반 이상(53%)이 느끼는 가장 중요한 문제점으로 "사이버보안 기술력 부족"을 거론하고 있다[1]. (ISC)²의 연례 보고서에 따르면 65% 조직에서 사이버보안 기술력 부족을 인정하고 있으며, 세계적으로 사이버보안 인력 407만 명이 부족한 상황이라고 밝히고 있다[2].

미국 연방정부는 국가차원의 사이버보안 인력을 육성하고 확보하기 위한 정책의 일환으로 NICE(National Initiative for Cybersecurity Education) 프로그램을 2010년부터 시행하고 있다. 2017년 10월 발표한 "NICE Cybersecurity Workforce Framework"(이하 NICE 프레임워크)는 전문인력 업무 역할(work role)을 52개로 규정하여 사이버보안 연방 인력의 인사코드로 부여하였다[3]. NICE 프로그램의 일환인 CyberSeek에서는 미국 국가 차원의 사이버보안 인력 현황을 쉽게 파악하기 위해 관련 통계자료를 수집·게시하고 있다(2020년 11월 3일 기준, 사이버보안 재직 인력은 922,720명, 부족 인력은 507,924명)[4].

2019년 ENISA는 노동 시장에서 요구되는 사이버보안 전문인력 부족을 지칭하는 사이버보안 기술 부족 현상은 세계 경제의 급속한 디지털화로 인해 경제와 국가 안보 측면의 문제에 영향을 줄 정도로 심각한 상황을 초래함을 경고하고 있다[5]. 또한 노동 시장의 요구조건을 충족하는 전문가 공급 부족의 양적 문제와 시장의 요구에 부응하기 위한 기술력 부족의 질적인 문제를 지적하고 있다[5].

우리나라의 경우 2019 정보보호 실태조사에 따르면 정보보호 관련 책임자가 임명된 국내 사업체의 비율(복수 응답, 2018년 12월 기준)은 '정보관리책임자(CIO)' 10.9%, '정보보호최고책임자(CISO)' 12.0%, '개인정보보호책임자(CPO)' 1.6%로 각각 나타났다[7]. 또한 정보보호 관련 책임자 전담 비율(복수 응답)은 CIO 2.1%, CISO 2.3%, CPO 3.1% 등 전문적 직무에 대한 인식이 매우 낮다[7]. 또한 2019 국내 정보보호산업 실태조사에 따르면 정보보호산업 인력 수(2018년 12월 기준)는 총 46,275명으로 정보보안 인력 13,378명(28.9%), 물리보안 인력 32,897명(71.1%)으로 조사되었다[8]. 국내의 경우 일반적으로 사이버보안 인력의 부족 현상을 인식하고 있고 인력 확보를 위해 정부차원의 정책적 노력은 일부 행해지고 있으나 만족할 만한 수준은 아니라는 것이 일반적인 시각이다.

1.2 연구 내용

본 논문은 지금까지 잘 다루지 못한 기술력을 보유한 사이버보안 전문인력의 역량 기준과 평가를 위한 방법론을 제안하며 다음과 같은 단계로 기술한다.

첫 번째 단계는 "사이버보안 직무 역량 개념 정립" 단계이다. 먼저 사이버보안 역량 모델에 대한 기존 관련 연구(3가지 관점, 국가·조직·개인)들을 분석하여 현황을 파악한다. 이를 통해 기존 모델들이 내재하고 있는 문제점들과 실용적으로 활용하기 어려운 점을 파악한다. 이후 일반적인 직무 및 역량에 대한 개념을 활용하여 사이버보안 직무와 사이버보안 역량에 대해 개별 개념을 정립한 후, 통합적인 관점에서 사이버보안 직무 역량 개념을 규정한다.

두 번째 단계는 "사이버보안 기술적 대응 직무 역량 개념 정립" 단계이며, 세부 내용은 다음과 같다. 첫째 "사이버보안 기술적 대응 직무 식별 및 구성에 대한 방법론 정립"을 위해 NICE 프레임워크의 52개 업무 역할을 분석하여 사이버 위협의 기술적 대응 직무[1]를 식별해낸 후, 하위의 세부 직무를 선별한다. 둘째 "사이버보안 기술적 대응 직무 요구 기술 식별 및 구성에 대한 방법론 정립"을 위해 사이버보안 기술 분류(CTT, cybersecurity technology taxonomy)를 구현하여 사이버 위협에 대한 기술적 대응 역량의 기술 수준을 식별하고 파악한다. 이때 식별된 기술은 IT, 네트워크 등 기술 변화를 반영해야 하므로 필요시 수정 보완되어야 한다. 셋째 "사이버보안 직무·기술 연관 매트릭스(AMCJT, associated matrix of cybersecurity jobs and technologies) 개념 정립"은 식별된 직무와 기술의 상호 연관성을 분석하여 요구되는 기술 수준을 정의한다. AMCJT를 적용하여 기술적 대응 직무 역량 평가가 가능한 "사이버보안 기술적 대응 직무 역량(CtrJC, Cybersecurity technical response Job Competency) 프레임워크"를 제안한다.

1) 이후 capability는 '능력'으로, ability는 '능력(a)'로 구분하여 사용하고자 한다.

세 번째 단계는 CtrJC 프레임워크의 모델링 구현 및 타당성 검증 수행을 위하여, 하나의 구현 사례로, 기술적 대응 직무 중 세부 직무인 실시간 사이버 위협에 대한 기술적 대응 직무에 대해 CtrJC 모델을 구현한다. 구현한 모델을 "실시간 사이버 위협에 대한 사이버보안 기술적 대응 직무 역량(CtrJC-R, Cybersecurity technical response Job Competency against Realtime cyber threats) 모델"이라고 하며, 이 모델에 대한 타당성을 검증하고 활용방안을 제안한다.

II. 관련 동향 분석

2.1 사이버보안 역량 연구 동향

지금까지 사이버보안 역량에 대한 구체적인 개념 또는 정의 없이 관련 연구가 진행되어 온 경향이 있다. 관련 연구들은 주로 국가 관점에서 또는 조직(예, 정부 기관, 기업 등) 관점에서의 사이버보안 능력[2]을 비교 분석하는 모델이 대부분이다. 이와 다르게 인력 관점에서의 참고할 만한 모델은 NICE 프레임워크가 거의 유일하다고 할 수 있다.

사이버보안 분야에서 역량 모델 및 평가 분야에서 국내의 경우 "capability"를 역량으로 번역하여 사용하는 경향이 있다. 엄밀하게 따진다면 능력으로 번역하는 것이 혼란을 줄이는 방법이다(능력과 역량의 엄밀한 차이 및 일반적인 역량 개념 등과 같은 자세한 내용은 관련 3.2.1절 참고).

2.1.1 국가 중심의 사이버보안 역량 모델

사이버보안 역량 모델에 대한 연구들은 사이버보안 능력에 대한 개념을 적용하여 주로 국가, 조직, 인력의 3가지 관점에서 접근하고 있음을 알 수 있다.

국가 차원에서 사이버보안 능력 모델을 제안하는 측면과 국가 간 평가 방법론이 주로 개발되었으며, 정책 연구기관 및 연구자들이 많은 관심을 보이고 있다. 관련 모델은 다음과 같은 것들이 있다[9].

국가 차원의 사이버 능력 평가는 국가 안보・경제 등 포괄적인 분야에 대해 전문가 및 담당자 등의 설문 및 인터뷰, 공개된 정보를 기반으로 작성된다. 전

(1) ASPI Cyber Maturity in the Asia-Pacific Region Index
(2) Cyber Readiness Index 2.0
(3) Cyber Power Index
(4) The Cyber Index
(5) Cybersecurity Policy Making at a Turning Point
(6) Global Cybersecurity Index (ITU)
(7) EU Cybersecurity Dashboard
(8) National Cyber Security Index

문인력의 역량 수준은 반영되고 있지 못하고 있다. 그러므로 국가 중심의 사이버보안 역량 모델을 직무 역량 모델에 직접 반영하는 것은 어려운 상황이다.

2.1.2 조직 중심의 사이버보안 역량 모델

Risto Hansen[9]에 따르면 조직 대상의 사이버보안 능력 평가를 위한 모델로 다음과 같이 4종을 제안하고 있다.

- Information Risk Maturity Index 2014 (IRMI)[10]
- Risk & Responsibility in a Hyperconnected World(RRH)[11]
- Cyber Operations Maturity Framework (COMF)
- Cybersecurity Capability Maturity Mode l(C2M2)

조직 관점에서의 사이버보안 능력 모델들은 다른 조직(기관)과 상대적 비교 없이 대상 조직의 사이버보안 개발 또는 능력 수준을 측정할 수 있는 벤치마크 또는 지침을 제공한다는 측면에서 국가 간 비교 중심의 국가 관점에서의 모델과 차이가 있다. 이러한 유형의 지수는 성숙 모델이라고도 하며 자체 평가 프로세스를 시작하기 위해 조직에 기준선을 제시한다.

옥스퍼드 대학의 글로벌 사이버보안 능력 센터에서 개발한 사이버보안 능력 성숙도 모델(C2M2)은 조직적 관점의 보편적인 모델이다. C2M2는 사이버보안과 관련된 다음의 5가지 능력 차원(①사이버보안 정책 및 전략, ②사이버 문화와 사회, ③사이버보안 교육, 훈련, 스킬, ④법률 및 규제 체계, ⑤조직, 기술 및 표준)을 정의하여 조직의 사이버보안 성숙도를 모델링하며 C2M2는 주로 사이버보안의 정책 및 조직 측면에 중점을 두고 있다[12]. 옥스포드 대학교의 C2M2를 기반으로 여러 기관에서 자체적인 사이버보안 능력 성숙도 모델을 개발하여 활용하고 있다. 다양한 사이버보안 능력 성숙도 모델이 조직 및 개인의 평가에 적용되며, 이들 모델 중 유일하게 NICE만 개별 인력의 능력을 평가하는데 활용이 가능하다고 알려져 있다[13].

2) capability, ability 모두 능력으로 번역되므로, 본 논문에서는 능력, 능력(a)로 구분하고자 한다.

미국 에너지부(DoE)에서 개발한 C2M2는 미국 및 세계 각국의 조직에서 활용 가능한 C2M2 모델을 제안하고 있으므로 조직 대상의 사이버보안 능력 평가의 범주에 포함할 수 있다[14].

조직에 대한 능력 성숙도 모델과 유사한 것이 NIST Cybersecurity Framework(CSF)이다[15]. DoE의 C2M2가 10개의 도메인으로 분류한 반면 NIST CSF는 좀 더 단순하게 5개의 Function으로 구분하여 제시하고 있다.

Function 1. IDENTIFY	Function 2. PROTECT
Function 3. DETECT	Function 4. RESPOND
Function 5. RECOVER	

NIST CSF는 기관들이 자발적으로 도입해서 자체 평가를 통해 사이버보안 위협에 잘 대응하는 조직으로 운영하도록 가이드하는 프레임워크이다[16].

2.1.3 인력 중심의 사이버보안 역량 모델

DoE의 C2M2, NIST CSF 등은 조직의 모든 분야별로 광범위한 상황에 대한 직원 및 전문가들의 의견을 기반으로 정성적인 평가를 통해 조직의 사이버보안 대응 능력 수준을 경영 차원에서 파악하는 것이 가장 중요한 목적이므로, 전담 인력 중심의 개별적인 기술 능력을 식별하는 작업에는 적합하지 않다.

반면에 NICE 프레임워크는 기본적으로 사이버보안 인력의 업무 역할에 대해 정의를 하고 있으며, 필요한 지식, 스킬, 능력(a)을 기반으로 기술하고 있다. 이는 사이버 위협에 대한 실시간 대응 기능을 도출하는 효과적인 방법으로 볼 수 있다.

미국 노동부 산하 고용훈련청(ETA)은 NICE 프레임워크의 사이버보안 인력 업무 역할과 보조를 맞추는 사이버보안 역량 모델을 제안하고 있다. ETA는 다양한 산업 분야에서 고용 활성화를 위하여 분야별 역량 모델을 제시하고 있으며, 이를 취업 준비자 및 채용 기관 등이 활용할 수 있도록 장려하고 있다. 예를 들어 기업 및 기관에서 이 자료를 변경 및 개발하여 인력의 역량을 평가할 수 있도록 지원하고 있다. 사이버보안 역량 모델도 여러 역량 모델 중 하나로 가장 최근 개발되었으며, 다음과 같이 5단계의 단계별 역량으로 구성된다.

1단계에서 3단계까지의 역량들은 주로 직원들이 보유해야 할 기본적인 소양(예, 사교, 의사소통, 팀웍, IT 기술 등)에 관하여 제시하고 있다. 4단계는 사이버보안 전반을 다루는 분야(예, 사이버보안 기술, 정보보안, 위기관리, 탐지, 사고대응 및 복구 등)를 제시하고 있다. 5단계는 NICE 프레임워크의 7개 범주와 52개 업무 역할을 기술하고 있다.

Tier 1: Personal Effectiveness Competencies
Tier 2: Academic Competencies
Tier 3: Workplace Competencies
Tier 4: Industry-Wide Technical Competencies
Tier 5: Industry-Sector Functional Areas

5단계는 NICE 프레임워크의 업무 역할을 제시하고 있으나, 4단계 이하의 역량과의 연관성을 설명하지 않고 있다. 그러므로 NICE 프레임워크에서 요구하는 업무 역할의 역량을 직관적으로 파악하기 곤란하며, 직무에 요구되는 역량이 추상적 레벨에서 단순 나열 형태이므로 현실에서 활용하기에는 다소 어려운 상황이다.

2.2 사이버보안 기술 분류 연구 현황

세계적으로 사이버보안(cybersecurity)이 공통적인 명칭으로 정립되는데 많은 개념적 변화가 있어 왔다. 1980년대에는 컴퓨터보안, 네트워크 보안이 사용되었고, 1990년대에는 IT 용어의 등장과 더불어 정보보안, 정보보증(information assurance) 등의 용어가 사용되었으며, 90년대 후반기 인터넷의 등장 및 초고속인터넷의 발전에 따라 정보전(information warfare)이라는 용어가 등장하였다. 사이버보안이 2000년대에 들어서서 미국 연방 법률에서 공식적으로 처음 등장하였으며, 이후 모든 국가 법·제도·정책 문서의 포괄적인 용어로 정착되어 사용되고 있다. 우리나라의 경우에도 더 이상 혼란을 주지 않도록 용어에 대한 재정립이 필요하다[6].

이처럼 용어가 정립되는데 많은 시간이 요구되었는 것에서 알 수 있듯이, 사이버보안 기술의 분류는 아직도 정립되었다고 보기 어렵다. 하지만, 사이버 위협에 대한 기술적 대응 역량을 객관적이고 정량적으로 측정하고 평가하기 위해서는 관련된 사이버보안 기술을 파악하여야 하며, 이를 효과적으로 관리하기 위해서 사이버보안 기술 분류가 요구된다.

다음의 2.2.1-2.2.4절의 관련 연구에서도 알 수 있듯이 사이버보안 기술 분류에 대한 표준 및 규격화된 방법론은 현재 존재하지 않으며, 일부 기관들이 기술 분류를 시도하기도 하였으나, 대부분 사이버보

안의 광범위한 범위의 틀 안에서 사이버보안 기술을 단위 구성 요소로 바라보는 관점 정도로 기술 분류를 시도하고 있어 한계가 명확하였다. 따라서 본 연구에서는 사이버 위협에 대해 기술적 대응을 하는 직무 역량을 객관적·정량적으로 평가하기 위해 사이버보안 기술적 대응 직무에 요구되는 사이버보안 기술 분류를 새롭게 제안하고자 한다(5.2.절 Table 5 참고).

2.2.1 정보보안 기술 분류(2003, H. S Venter)

2000년대 초는 사이버보안이라는 용어가 일반적이지 않았으며, 주로 정보보안이 사용되고 있었다. H.S Venter는 정보보안 기술 분류를 논문으로 발표하였으며, Fig. 1.과 같이 제시하였다[17].

이 당시만 하더라도 무선, AI, 스마트폰 등이 없었던 때로 IT 기술이 다양하지 않던 상황에서 기술 분류를 너무 단순하게 바라보고 있으므로 현재 반영하기에는 다소 무리가 있다.

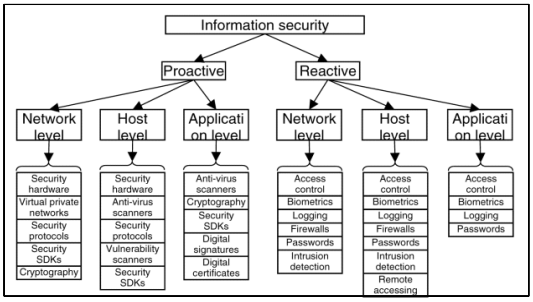


Fig. 1. The case of Information security technology taxonomy

2.2.2 사이버보안 분류(2014, David Klaper)

(1) **Main Taxonomy on Cybersecurity**
- Impact of Cybercrime and Cybersecurity
- Technical Aspects of Cybersecurity

(2) **Operational View Taxonomy on Cybersecurity**
- Actions of People • Systems and Technology Failures
- Failed Internal Processes • External Events

(3) **User-view Taxonomy on Cybersecurity**
- End User Focus • Human Resources Focus
- Permanent Network Administrator Focus
- Temporary Collaboration Network Administrator Focus

Carnegie Mellon 대학교의 Language Technologies Institute에서 제시한 사이버보안 분류는 위와 같이 분류하고 있다[18][19]. 사이버보안의 직관적인 분류를 제시하고 있으나, 기술 중심의 분류로 보기에는 어려움이 있다.

2.2.3 보안 제품, 시스템, 서비스 분류(2016, Vrije Universteit Brussel)

브뤼셀 대학교는 모든 보안 제품, 시스템, 서비스에 관련된 분류 방식을 제안하고 있다[20]. 2014년에 Version 1.0을 발간하였으며, 기술 등의 변화에 따라는 업데이트를 통해 Version 2.0을 2016년에 발간하였다. 이 문서에서는 모든 보안에 관련된 분류로 사이버보안의 경우 일부 구성요소로 포함되고 있다. 다음과 같이 4개 레벨로 유럽의 보안 분류를 시도하고 있다.

(Level 1) Security application areas
(Level 2) Security demands
(Level 3) Security Functions
(Level 4) Security Products and Systems

첫 번째 레벨은 보안 응용 영역으로 다음과 같이 4종으로 구분하고 있다.

- Border security/management • Critical Infrastructure
- Emergency Preparedness Centres/Crisis Management
- Security of the citizens

이러한 응용 역역별로 요구되는 보안 요구(security demand)들을 다음과 같이 8개 분야로 구분하여 세밀하게 분류하고 있고, 보안 요구 사항 중 하나가 사이버보안이다.

- Access control • Asset/freight/cargo security
- Cyber security • Employee/visitor safety
- Loss prevention/shrinkage
- Perimeter/area/building security
- Point of transaction • Situation awareness

브뤼셀 대학교 분류 방식은 국가 안보 차원에서 사이버보안을 작은 구성요소로 보고 있으므로 구체적인 기술 분야를 다루는데 한계를 가질 수밖에 없다.

2.2.4 유럽식 사이버보안 분류 제안(2019, EC JRC)

가장 포괄적인 사이버보안 분류를 다루는 보고서

로 2019년 유로위원회의 Joint Research Centre(JRC)에서 발표한 "A Proposal for a European Cybersecurity Taxonomy"를 들 수 있다[21]. 이 보고서는 다양한 기관 및 조직에서 추진했던 분류 방식을 종합적으로 비교 분석하여 3차원적인 사이버보안 분류를 제안하고 있다.

상기 보고서에서 최신 사이버보안 분야를 포괄적으로 분류할 수 있는 기준을 제시하고 있으며, 도메인 중 "Incident Handling and Digital Forensics", "Network and Distributed Systems", "Software and Hardware Security Engineering"의 기술 분야는 다른 분류 방식 보다 좀 더 사이버 위협 기술적 대응에 활용 가능한 기술 분야를 제시하고 있다.

Table 1. Job classification

Type	Description
Job Family	It is classified into the methods or functions that contribute to value creation in the process of value creation of a cooperationy.
Sub Job Family	The coverage is determined based on the capabilities of the employees in a job classification unit between a job family and a job.
Job	It means the range or size of work that a person can do and consists of a set of similar tasks
Duty	A collection of multiple tasks performed by a particular individual
Task	It is a unit of work activity with a specific purpose and role, and consists of various elements. Tasks are organized tasks that have a certain purpose as a unit of work given to the worker and can be divided or shared.
Element	The smallest units of work (e.g., answering calls, recording, etc.)

III. 사이버보안 직무 역량 개념

3.1 사이버보안 직무 개념

3.1.1 일반적인 직무 개념

실무는 국립국어원의 표준국어대사전에서는 "실제의 업무나 사무"라고 정의하며, 고려대한국어대사전에서는 "실제적이고 구체적인 업무"로 정의하고 있다. 실무는 "현장에서 수행하는 업무"로 보는 것이 일반적으로 받아들 수 있는 개념이라고 볼 수 있다.

실무와 유사한 개념으로 직무를 들 수 있는데, 실무는 현장에서 요구되는 업무이며 직무의 경우 주어진 임무를 달성하기 위해 정해진 업무로 볼 수 있다. 처음 규정된 직무는 실무와 차이가 없으나, 대내외 환경에 따라 실무는 지속적인 변화가 가능하다. 이 변화를 직무에 적절하게 반영하여 현실화하는 것이 중요하다. 만일, 실무의 변화를 직무에 반영하지 못한다면 실무·직무 간 차이가 발생하며, 현장의 실무와 다른 직무체계는 기술력 격차로 변화되는 요인 중 하나가 된다. 결국 직무는 변화하는 실무를 지속적으로 관찰하여 반영하여야 한다. 그러므로 실무와 직무는 동일한 개념으로 사용할 수 있다.

일반적인 직무 분류 방법은 직무를 Table 1.과 같이 "직군(Job Family), 직렬(Sub Job Family), 직무(Job), 책무(Duty), 과업(Task), 요소(Element)"로 분류한다[22, 25](각 세부설명은 Table 1. 내 정의 및 4.1절 설명 참조).

3.1.2 사이버보안 분야의 직무 개념

사이버보안 분야의 경우 IT 기술의 발전과 보조를 맞추어야 하며, 또한 사이버공격에 대응해야 하므로 직무의 변화는 다른 분야보다 매우 크다고 할 수 있다. 즉, 사이버보안 직무에 대한 정의, 설계, 관리 등이 매우 어렵다.

사이버보안 직무에 활용이 가능한 사례는 미국의 NICE 프레임워크의 업무 역할 52종이 대표적이다. NICE의 업무 역할 52종은 연방인사관리처(OPM)에서 연방인력의 인사코드로 부여하고 국가차원에서 관리하고 있으며, 많은 교육기관, 인증기관 등이 활용하고 있다.

국내의 국가직무능력표준(NCS)는 중소기업 등에서 직원 채용 시 활용하도록 권고하였으며, 점차 국가·공공기관의 직원 채용에서도 활용하고 있는 정도이다. 정보보호 분야는 NCS에 별도 분류체계 없이 22개 정보기술(SW) 하위 세분류 중 `보안 엔지니어링`만이 정보보호 직무로 정의돼 다양한 직무 반영이 어려웠다. 2017년 1월 한국인터넷진흥원(KISA) 주관으로 한국정보보호산업협회(KISIA) 등 산업계와 함께 정보보호 분야 직무 3종을 NCS에 신규로 개발하여 추가하였다. 정보보호 분야 직무는 정보보호 관리·운영, 정보보호 진단·분석, 보안사고 분석대응으로 세분화하고 있으나, 전문인력 관리 및 육성 등에서 활용하는 것은 아직 부족한 측면이 있다.

3.2 사이버보안 역량 개념

3.2.1 일반적인 역량 개념

인적자원개발 용어사전에서 "역량(competency)은 특정한 상황이나 직무에 따른 효과적이고 우수한 수행의 원인이 되는 개인의 내재적인 특성으로 개인이 성공적인 수행을 위하여 개별적으로 결합해서 사용하는 특징들"이라고 한다. 역량은 대상 및 관점 단위에 따라서 조직 전체를 유기체로 보고 기업의 경쟁력 강화를 위한 전략의 관점에서 조직의 역량과 조직 구성원의 관점에서 우수한 성과를 내는 개인의 역량으로 나눌 수 있다. 조직의 역량은 해당 조직을 이끌어 왔으며 적절하게 전환되거나 축적되면서 조직의 성장을 이끌어 가도록 조직 내부에 공유되고 있는 특유의 총체적인 능력, 기술, 지식을 의미한다. 조직의 역량은 연구자에 따라 다양하게 정의되었다[23].

일반적인 역량은 교육학과 인적자원관리 측면에서 바라본다고 한다면, 핵심 역량(core competency)은 기업과 같은 조직에서 경쟁력 확보를 위해 필수적인 요소가 된다. 특히 IT 기업 및 사이버보안 분야의 조직은 급변하는 기술에 적절한 대응하기 위해서는 핵심 역량의 확보가 타 분야에 비해 더 중요하다.

Javidan, M.[24]은 Fig. 2.와 같이 기업은 핵심 역량, 역량, 능력, 자원의 계층적 구조를 갖는다고 주장하였다.

자원은 역량의 구성 요소다. 자원은 조직의 가치 사슬에 투입되는 투입물로서, 공장, 장비, 장소, 자산과 같은 물리적 자원, 인력, 관리팀, 교육 및 경험과 같은 인적 자원, 문화 및 명성과 같은 조직 자원으로 분류한다.

능력은 기업의 자원을 활용하는 제반 능력(a)으로, 자원 간의 상호 작용을 관리하는 일련의 비즈니스 프로세스로 구성된다. 프로세스는 입력을 출력으로 변환하는 활동 집합이다.

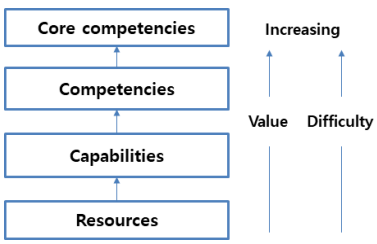


Fig. 2. Competencies hierarchy

역량은 기능 간 통합 및 능력 조정이다. 예로 다종 사업을 하는 기업에서 역량은 전략사업부(SBU, Strategic Business Unit)에 수용되는 일련의 스킬과 노하우이며, SBU의 기능적 능력들 간의 인터페이스와 통합에서 비롯된다.

핵심 역량은 SBU 경계를 넘나들며, 서로 다른 SBU의 역량들 사이의 상호작용에서 비롯된다. 핵심 역량은 비즈니스 단위에서 공유되고 SBU 역량의 통합과 조화로 인해 발생하는 기술과 지식 영역이다.

3.2.2 사이버보안 역량 개념 정립

앞 절에서 제기된 일반적인 역량, 능력, 자원의 계층 구조를 사이버보안 역량 개념에 적용할 수 있다. 역량은 자원을 활용하는 능력을 기반으로 주어진 목표를 달성하는 성과를 보이는 것으로 정의하고 있으므로 사이버보안 역량도 능력과 자원으로 구성이 가능하다. 사이버보안 역량을 정립하기 위해서는 목표를 정의하고, 능력 및 자원을 정의하는 것이 기본적으로 요구되나, 사이버보안의 많은 부분이 변화하고 있으며 학문적 또는 실용적 관점에서 명확한 정의가 어려운 분야이다. 그러므로 사이버보안 분야 전체를 포괄하기에는 한계가 있으므로, 본 논문에서는 사이버보안 중 사이버 방어에 해당되는 업무를 중심으로 적용하고자 한다.

사이버보안 능력을 구체적으로 식별하기 위해서는 직무별로 구성하는 기능을 식별하여 해당 기능을 수행할 수 있는 제반 지식, 스킬, 능력(a) 등을 갖추어야 한다. 이와 같은 기능을 식별하여 정량 및 정성적으로 인정할 수 있는 지표 등을 마련하여야 조직 및 개인의 역량 측정이 가능하다고 할 수 있다. 본 논문에서 역량 관련 용어들을 다음과 같이 정의한다.

- **사이버보안 역량(competency)** 사이버보안 역량을 달성하는데 요구되는 능력들의 집합(set of capabilities)
- **사이버보안 능력(capability)** 사이버보안 관련 특정 기능을 수행할 수 있는지에 대한 정도
- **사이버보안 기능(function)** 사이버보안 관련 특정 목적을 달성하는데 필요한 활동들의 집합(set of activities)
- **사이버보안 활동(activity)** 특정 기능을 실행하는데 요구되는 업무 행위

3.3 사이버보안 직무 역량 정립

3.3.1 일반적인 직무 역량 개념

직무 역량은 앞 절에서 논의한 바와 같이 여러 가지 능력으로 구성된다. Fig. 3.은 직무 역량을 구성하는 능력들의 계층적 구조를 보여주고 있다.

본 논문에서는 직무 역량을 구성하는 능력을 성과 달성 능력(performing capability), 직무 수행 능력(job capability), 기술 보유 능력(technology capability)으로 구분한다. 첫째, 성과 달성 능력은 조직의 목표에 부합하는 성과를 내기 위한 능력으로 정량적으로 표현하기 어려운 요소 중 하나이다. 둘째, 직무 수행 능력은 직무별로 요구되는 업무 수행 능력으로, 일반적으로 일 잘한다는 평가를 내릴 수 있는 요소로서 상세한 업무 수행 절차 및 행위 정의가 요구된다. 셋째, 기술 보유 능력은 업무 수행에 요구되는 기술을 보유하고 있는 능력으로서, 정량적인 표현이 가능하며 사이버보안 분야의 기술력 격차의 원인이 되는 능력에 해당된다.

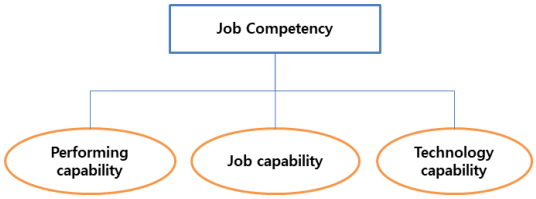


Fig. 3. General job competency and its capabilities

3.3.2 사이버보안 직무 역량 개념

앞 절에서 정립한 직무 역량 개념을 사이버보안 분야에 적용한다면 다음과 같이 재정립할 수 있다.

- **사이버보안 직무 역량** : 사이버보안 분야에서 목표 달성에 요구되는 직무 수행하여 성과를 내는 것이며, 사이버보안 직무 역량을 달성하는데 요구되는 능력들의 집합
- **사이버보안 성과 달성 능력** : 조직의 목표에 부합하는 사이버보안 분야의 성과를 내기 위한 능력
- **사이버보안 직무 수행 능력** : 직무 별 요구되는 실무 수행 능력이며, 상세한 업무 수행 절차 및 행위 정의가 필요함
- **사이버보안 기술 보유 능력** : 직무 수행에 요구되는 기술을 보유하고 있는 능력

Fig. 4.는 사이버보안 직무 역량의 계층적 구조를 보여주고 있다. 의미는 일반적인 직무 역량의 개념과 유사하게 적용할 수 있다.

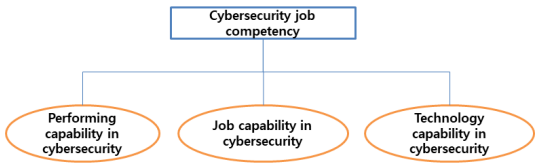


Fig. 4. Cybersecurity job competency and its capabilities

IV. 사이버보안 기술적 대응 직무 역량 프레임워크 제안

NICE 프레임워크의 52개 직무 역할에서 보듯이 사이버보안 직무 역량은 다양한 능력을 포함하고 있다. 본 논문에서는 효과적인 전달의 목적을 달성하기 위함과 동시에 객관적, 정량적 평가가 가능한 방법을 개발하는 것을 목표로 사이버보안 직무 중에서도 경영, 관리 등의 비기술적 요소를 배제하고 변별 가능한 기술적 직무에 초점을 두고자 한다.

3.3.2에서 제안한 사이버보안 직무 역량 정의 개념을 활용하여 사이버보안 기술적 직무 대응 역량(CtrJC)을 기술적 대응 직무 수행에 필요한 성과달성 능력, 직무 수행 능력, 기술 보유 능력의 집합으로 정의한다(Fig. 5.).

사이버보안 기술적 대응 직무 역량을 평가하기 위해서는 3가지 능력(성과 달성 능력, 직무 수행 능력 기술 보유 능력)에 대한 평가가 모두 요구되나, 기술력 격차 관점과 효과적인 직무 역량 평가 방법론을 기술하기 위해서 본 논문에서는 3가지 능력 중 하나인 기술 보유 능력 및 이에 대한 평가를 예시로 사용하여 초점을 두고 기술하고자 한다.

사이버보안 기술적 대응 직무 역량 평가를 파악하는 프레임워크는 (단계1)직무 식별·구성, (단계2) 기술 식별·구성, (단계3)AMCJT 구현, (단계4)평가의 4 단계로 구성된다(Fig. 6.).

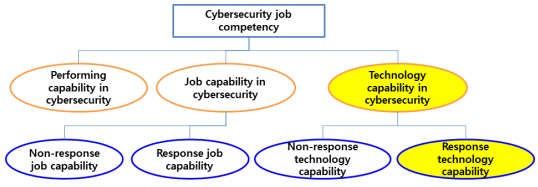


Fig. 5. Cybersecurity technical response job competency

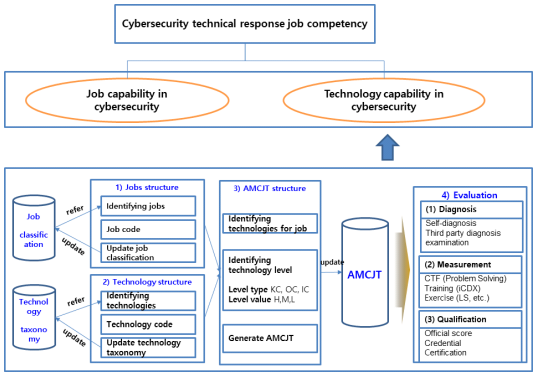


Fig. 6. CtrJC framework

4.1 (단계1)직무 식별·구성 단계

사이버보안 기술적 대응 직무에 대한 명확한 분류, 규정 등이 미흡한 관계로 사이버 공격 대응을 수행하는 보안관제 업무 특성과 NIST CSF[11] 개념을 적용하여 다음과 같이 5개 분야로 구분한다. 이 직무들을 최상위 레벨의 직무로 식별하여 하위 직무로 분류하는 것을 원칙으로 한다.

① **예방(protect) 직무** : 사이버 위협 및 공격을 미연에 방지할 수 있는 역량이 요구되는 직무
② **탐지(detect) 직무** : 실시간 침입 시도 및 사고를 빠른 시간 내에 인지할 수 있는 역량이 요구되는 직무
③ **초동(initial-response) 직무** : 탐지된 실시간 침입 시도 및 사고에 대해 긴급 대처 역량이 요구되는 직무
④ **분석(analysis) 직무** : 침입 시도 및 사고의 분석을 통해 원인 및 방안을 식별해 내는 역량이 요구되는 직무
⑤ **대응(response) 직무** : 침입 시도 및 사고 분석을 통해 방어 조치를 취하여 동일 및 유사 사고에 대처할 수 있도록 조치하는 역량이 요구되는 직무

다음 장에서 구현할 모델에 요구되는 실시간 사이버 위협 및 공격 대응을 위한 직무 및 역량은 정책 직무 및 사무 역량을 제외하고 운영·기술 역량이 요구되는 업무로 식별할 수 있다.

앞에서 일반적인 직무에 대한 분류(3.3.1절 Table 1 참조)와 유사하게 사이버보안 기술적 대응 직무를 다음과 같이 구분한다. 기본적으로 레벨 5 수준으로 직무를 구분하여 요구되는 기술력을 보다 구체화하려고 하는 것이다.(Table 2.)

본 연구에서는 범위가 매우 넓은 직군(job family)에 해당하는 직무 수준은 정의하지 않고, 직렬 이하 직무에 대해서 레벨을 정의한다. 직렬(sub job family)은 직군과 직무 사이에 두는 직무분류

Table 2. Cybersecurity jobs classification

Type	Level	Contents
Job Family	N/A	N/A
Sub Job Family	Level 1 Job	① Protect job ② Detect job ③ Initial-response job ④ Analysis job ⑤ Response job
Job	Level 2 Job	high level job
Duty	Level 3 Job	duty level job
Task	Level 4 Job	task level job
Element	Level 5 Job	job at unit function and behavior level

단위로 직원들의 전문성을 향상시키기 위하여 이동의 범위를 결정하는 직무이다[22, 25]. 앞서 구분한 NIST CSF의 5개 분야(예방, 탐지, 초동조치, 분석, 복구)로 분류된 최상위 레벨의 직무가 이에 해당한다고 판단하였으며, 본 연구에서는 직렬을 레벨 1 직무라 정의한다.

직무(job)는 한 사람 정도가 수행할 수 있는 일의 범위나 크기를 의미하며 유사한 과업들의 집합으로 구성된다[22, 25]. 이는 높은 수준의 직무에 해당하며, 본 연구에서는 레벨 2 직무로 정의한다.

책무(duty)는 특정 개인이 수행하는 여러 가지 과업의 집합이다[22, 25]. 책무 수준의 직무를 본 연구에서는 이를 레벨 3 직무로 정의한다.

과업(task)은 특정 목적과 역할을 가지고 있는 작업활동 단위로서 여러 가지 요소들로 구성되며 과업은 작업자에게 부여된 일의 한 단위로 일정한 목적을 가지고 있으며 분업이나 분담이 가능한 정리된 일을 말한다[22, 25]. 과업 수준의 직무를 본 연구에서는 레벨 4 직무로 정의한다.

요소(element)는 업무의 가장 작은 단위(예: 전화 받음, 기록함 등)를 의미 한다[22]. 요소 수준의 직무를 본 연구에서는 레벨 5 직무로 정의한다.

본 논문에서는 편의상 직무를 레벨1 ~ 레벨5로 분류하는 방식을 적용하며, 다음과 같이 레벨 5 직무 식별이 가능하도록 직무 코드(job code, JC)를 부여한다. 레벨별 코드는 10진수 2자리로 "01"이상의 값을 가지며 마지막 자리를 기준으로 직무 레벨을 파악할 수 있다.

레벨 1직무명		레벨 2직무명		레벨 3직무명		레벨 4직무명		레벨 5직무명	
dd	dd	dd	dd	dd	dd	dd	dd	dd	dd

다음 사례는 "JC_01_01_01"인 경우의 예이다.

예방		보안시스템 운영		네트워크 방화벽 운영		미사용		미사용	
0	1	0	1	0	1	*	*	*	*

4.2 (단계2)기술 식별·구성 단계

특정 직무가 요구하는 기술은 사이버보안 기술적 직무 역량에 적용하기 위한 사이버보안 기술 분류(CTT)의 구현이 요구된다. 2.2절에서 살펴보았듯이 사이버보안 기술 분류는 정형화된 방법이 없으므로 적용 가능한 CTT 구현도 중요한 연구 분야이다. 앞에서 살펴본 사이버보안 기술 분류 연구 현황에서 보듯이 사이버보안 분야의 기술 분류는 실질적으로 비존재를 알 수 있다. 그러므로 사이버보안 기술적 대응 실무 역량에 요구되는 기술들을 기준으로 식별하여 기술 분류표를 구성하는 것이 필요하다.

직무별로 요구되는 세부 기능은 기술력을 필요로 하며, 기술력은 정의된 CTT에 의거하여 하위 직무 또는 직무를 구성하는 기능별로 요구되는 기술들을 식별해 나갈 수 있다. 본 논문에서 제안하는 사이버보안 기술 분류는 1차 분류 **12**종, 2차 분류 **34**종, 3차 분류 기술 **85**종을 기반으로 기술을 식별하였다. 세부 내용은 5.2절에서 확인할 수 있다.

향후 확장성을 고려하여 기술 코드(technical code, TC)는 다음과 같이 규정한다. 레벨별로 코드에서 식별 가능하도록 부여하며, 레벨별 코드는 10진수 2자리로 01이상의 값을 가지며 마지막 자리를 기준으로 주어진 레벨을 파악할 수 있다.

레벨 1기술명		레벨 2기술명		레벨 3기술명		레벨 4기술명		레벨 5기술명	
d1	d2	d3	d4	d5	d6	d7	d8	d9	d10

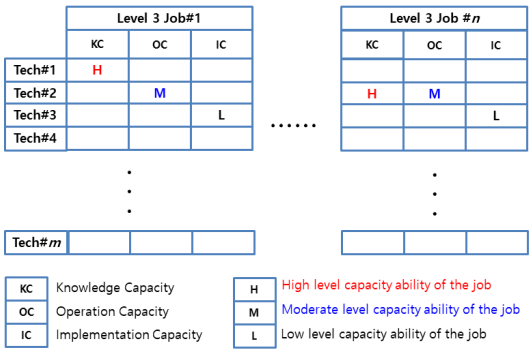


Fig. 7. AMCJT concept

다음 사례는 "TC_02_01_01"인 경우의 예이다.

정보보호 시스템		네트워크 보안		방화벽		미사용		미사용	
0	7	0	1	0	1	*	*	*	*

4.3 (단계3)AMCJT 구현 단계

기술적 직무 역량은 기술보유능력을 평가하여 역량을 표현하고자 한다. 이러한 역량 평가를 위해서는 Fig. 7.에서 보여주는 사이버보안 직무·기술 연관 매트릭스(AMCJT)를 구현해야 한다. AMCJT는 직무에 요구되는 기술을 식별하여 요구 수준까지 정의하는 방법이다.

사이버위협 대응 기술력은 사이버보안 기술의 지식 능력(knowledge capability, KC), 운영 능력(operation capability, OC), 구현 능력(implementation capability, IC) 등의 3가지 부분 기술력 수준 형태로 분류할 수 있다. 각각의 능력은 3단계의 난이도 수준(high(H), middle(M), low(L))으로 표현한다.

- **KC :** 기술에 대해서 이론적 지식 보유 능력이며, 실제 운영 중인 시스템의 기능의 직접 조작 등은 부족한 능력
- **OC :** 기술에 해당되는 시스템 운영을 담당하며 일부 설정 등의 조치가 가능한 정도의 운영 기술 보유 능력
- **IC :** 해당 기술 관련 분야의 시스템을 구현하는 능력

4.4 (단계4)평가 단계

사이버보안 직무·기술 연관 매트릭스를 구성하게 되면 직무 역량 평가 가능한 기반을 마련한 것이다. 평가는 다음과 같이 3 단계를 활용할 수 있다.

1 단계 : 진단(diagnosis)
① 자가 진단(설문) ② 제3자 진단(인터뷰) ③ 자격증 여부
2 단계 : (자동)측정(assessment)
① 해킹대회 : CTF(문제풀이), King-of-the-hill 등
② 훈련(사이버훈련장)[26] ③ 연습(Locked Shields 등)[27]
* 자동화 플랫폼 기반의 직무 수행 결과를 측정
3 단계 : 자격(qualification)
① 점수(score) ② 인정(authorization) ③ 인증(certification)
* 자격 부여는 정책 및 제도가 요구되는 분야

본 논문에서는 평가 단계를 식별하는 정도이며, 구체적 구현은 추후 연구로 남겨둔다.

V. 실시간 사이버 위협에 대한 사이버보안 기술적 대응 직무 역량 모델 구현

CtrJC 프레임워크의 기술 보유 능력 또한 적용 범위가 넓기 때문에 효과적인 연구 방법론 구현을 위하여 기술 보유 능력을 세부 능력으로 분류하고, 범위를 좁혀 예시를 제시한다.

사이버보안 기술 보유 능력은 비대응 / 대응 기술 보유 능력으로 분류한다. 또한 대응 기술 보유 능력은 사이버위협에 대해 실시간 대응이 필요한지 아닌지 기준으로 비실시간 / 실시간 대응 기술 능력으로 구분한다(Fig. 8.). 본 논문에서는 사이버보안 기술 보유 능력 중 해킹과 같은 실시간 사이버 위협 대응 기술 보유 능력에 대해 역량 평가 모델을 제안한다. 이를 실시간 사이버 위협에 대한 사이버보안 기술적 대응 직무 역량(CtrJC-R)으로 명명하며, 실시간 위협 대응기술 보유 능력 중심으로 제안된 모델을 구현하여 결과에 대한 타당성을 확인한다.

Fig. 9.는 CtrJC-R 모델을 구현하는 4단계 방식의 방법론을 보여주고 있다. 이와 같은 구현 절차는 직무와 기술을 적용함으로써 사이버보안 인력의 역량에 대한 평가가 가능한 모델을 구현할 수 있다. 다음 절에서 단계별로 세부 구현 내용을 설명한다.

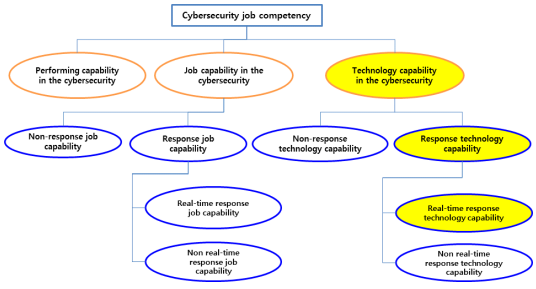


Fig. 8. Cybersecurity technical response Job Competency against Realtime cyber threats

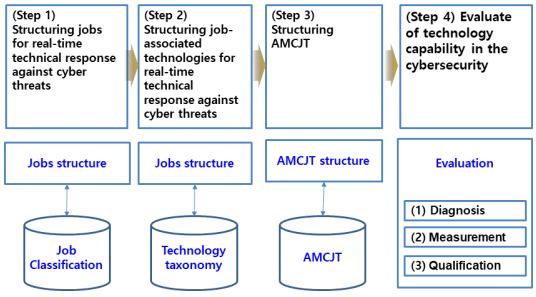


Fig. 9. Implementation of CtrJC-R Model

5.1 (단계1)직무 식별·구성

Fig. 10.은 실시간 사이버 위협에 대한 기술적 대응에 관련된 직무를 개발하는 단계를 보여준다. 본 논문에서는 3레벨의 직무를 식별하는 직무 개발 방법을 적용하도록 한다.

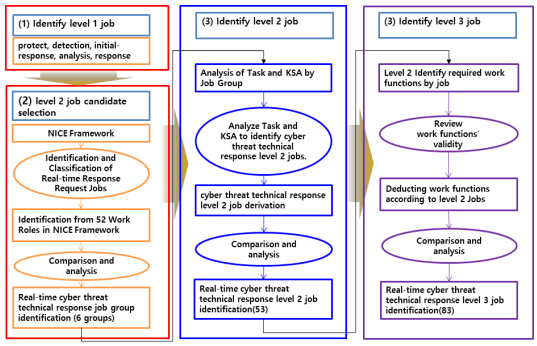


Fig. 10. (Step 1) Structuring jobs for real-time technical response against cyber threats

5.1.1 레벨1 직무 식별

레벨 1 직무는 사이버보안 기술적 대응 직무 능력 프레임워크에서 제안하듯이, "예방, 탐지, 초동, 분석, 대응"의 5개 직무로 정의하여 적용한다.

5.1.2 레벨2 직무 식별

NICE 프레임워크가 정의하는 52개 업무 역할을 검토하여 실시간 사이버 위협 기술적 대응 관련 업무 역할을 식별하여, 레벨 2 직무의 후보를 도출한다. 실시간 사이버 위협 기술적 대응 직무에 직접적으로 관련된 업무 역할은 다음과 같이 6종이 해당된다.

① PR-CDA-001 사이버 방어 분석가 Cyber Defense Analyst
② PR-INF-001 사이버 방어 인프라구조 지원 스페셜리스트 Cyber Defense Infrastructure Support Specialist
③ PR-CIR-001 사이버 방어 사고대응담당관 Cyber Defense Incident Responder
④ PR-VAM-001 취약점 평가 분석가 Vulnerability Assessment Analyst
⑤ AN-TWA-001 위협/경고 분석가 Threat/Warning Analyst
⑥ AN-EXP-001 익스플로잇 분석가 Exploitation Analyst

업무 역할들은 관련된 작업(task) 항목과 지식, 스킬, 능력(a)으로 구성된 KSA를 가지고 있다. 업

무 역할은 담당자가 해야 할 업무를 정의하고 있으므로 세부적인 직무는 작업 항목과 KSA 정보로부터 도출할 수 있다. "실시간 사이버 위협 및 공격 직무" 6종의 개별적인 업무 역할이 확보해야 하는 NICE 프레임워크의 작업 항목과 KSA를 면밀히 분석하여 직무로 식별하여, 그 직무가 실시간 사이버 위협 기술적 대응 직무인가를 판별한다. 이와 같은 과정을 거쳐 각 업무 역할로부터 식별된 직무를 최종적으로 레벨 2직무로 식별한다.

첫 번째 업무 역할인 사이버 방어 분석가는 다양한 사이버 방어 도구 (예 : IDS 알림, 방화벽, 네트워크 트래픽 로그)에서 수집한 데이터를 사용하여 위협 완화를 위해 해당 환경에서 발생하는 이벤트를 분석한다. 사이버방어 분석가 직무 분석을 위해 해당되는 작업 항목 및 KSA를 세부적으로 분석하여, 적용 가능한 직무 내용에 대해서 다음과 같이 작업 항목 및 KSA 번호를 식별하였다(24종). 세부 내용은 NICE 프레임워크 문서를 참조할 수 있다.

(1) 사이버방어 분석가
- **Tasks** T0020, T0023, T0043, T0164, T0166, T0178, T0214, T0258, T0259, T0293, T0295, T0296, T0297, T0310, T0503
- **KSAs** S0020, S0025, S0027, S0057, S0063, S0078, S0096, S0167,S0370

이와 같은 방식으로 나머지 5개 업무 역할을 분석하여 연관된 작업 항목과 KSA를 다음과 같이 식별하였다.

(2) 사이버 방어 인프라 지원 스페셜리스트
- **Tasks** 없음
- **KSAs** S0079

(3) 사이버 방어 사고 대응담당관
- **Tasks** T0161,T0163,T0164,T0175,T0214,T0233,T0278,T0503
- **KSAs** S0003, S0047, S0078, S0079, S0080, S0173

(4) 취약점 평가 분석가
- **Tasks** T0010
- **KSAs** S001, S0025, S0044, S0051, S0052, S0081, S0120

(5) 위협/경고 분석가
- **Tasks** T0749, T0751, T0752
- **KSAs** S0285, S0289

(6) 익스플로잇 분석가
- **Tasks** T0028, T0266
- **KSAs** S0184, S0199, S0245, S0258, S0286, S0294

상기와 같이 NICE 프레임워크로부터 식별된 58종의 직무를 예방, 탐지, 초동, 분석, 대응으로 구성되는 사이버대응 단계로 분류하였으며, 최종적으로 기술적 및 실시간적 연관성이 부족한 6종의 제외하

Table 3. Identification of real-time technical response job against cyber threats(level 2, 52)

Level 1 jobs	Level 2 jobs
Protect (7)	operation of security system
	development of cyber defense contents
	penetration test for network target
	operation of cyber defense applications/systems
	penetration test for applications
	treatment of intrusion artifact
	operation of network device
Detection (15)	vulnerability scan and recognition
	utilization of penetration test tools and technology
	Identification, capture, acquisition and reporting of malware
	monitoring and analysis of detection events
	data collection
	analysis of detection rules
	vulnerability recognition
	application of network visualization SW
	utilization of search engine
	verification of network alert
	receiving and analyzing network alerts
	monitoring and analysis tools for abnormal behavior
	monitoring and identifying security issues with control data
	monitoring of open source websites
	monitoring of operation environments
Initial-response (6)	maintenance of integrity of evidence
	processing of real-time cyber defense incidents
	detection, identification, alerting
	verification of IDS alert
	isolation and removal of malware
	monitoring and reporting of threat activity
Analysis (20)	malware analysis
	imitation of threat behavior
	utilization ion of social engineering techniques
	utilization of protocol analysis tool
	analysis of vulnerability/attack relation
	performing of damage assessment
	utilization of Network Analysis Tools
	analysis of intrusion-associated log
	packet-level analysis
	utilization of security event correlation tools
	analysis of traffic - identification of network devices
	analysis of packets-extract important information
	analysis of traffic - perception and analysis of malicious activities
	utilization of database
	utilization of path tracking tool
	analysis of network traffic
	log analysis
	review of cyber defense accident
	tracking and documenting cyber defense incidents
	identification and analysis of abnormal behaviors
Response (4)	development and distribution of detection rules
	protection of malware response networks
	query write-up
	update rules and signatures

여 최종적으로 레벨2에 해당하는 52종의 직무를 선정하였다.(Table 3.)

5.1.3 레벨3 직무 식별

레벨 2 직무 52종을 선정하였으며, 이 직무들을 보다 세분화하여 확장한 83종의 레벨 3 직무는 Table 4.와 같다. 레벨 3 직무부터는 NICE 프레임워크로부터 차용하지 않고, 직관적으로 기술적 직무에 요구되는 세부 직무로 확장 도출하였다.

Table 4. Identification of real-time technical response job against cyber threats(level 3, 83)

Job code	Job capability (level 3 job)
JC_01_01_01	operation of Network Firewall
JC_01_01_02	operation of Network IDS/IPS
JC_01_01_03	operation of web firewall
JC_01_02_01	development of contents for network firewall
JC_01_02_02	development of contents for network IDS/IPS
JC_01_02_03	development of web firewall contents
JC_01_03_01	design of network penetration test
JC_01_03_02	execution of network penetration test
JC_01_03_03	analysis&evaluation of network penetration test
JC_01_04_01	operation of cyber defense applications
JC_01_04_02	operation of cyber defense system
JC_01_05_01	design of application pen. test
JC_01_05_02	execution of application pen. test
JC_01_05_03	analysis&evaluation of the application pen. test
JC_01_06_01	collection of intrusion artifacts
JC_01_06_02	analysis of cyber defense incidents
JC_01_06_03	establishment and implementation of a mitigation plan for cyber defense incidents
JC_01_07_01	operation of hub/switch
JC_01_07_02	router operation
JC_01_08_01	vulnerability scan
JC_01_08_02	analysis of vulnerability scan results
JC_01_09_01	utilization of public penetration test tools
JC_01_09_02	utilization of commercial penetration test tools
JC_01_09_03	development and utilization of other penetration test tools
JC_02_01_01	malware collection
JC_02_01_02	malware report
JC_02_02_01	monitoring of detection events
JC_02_02_02	analysis of detection events
JC_02_03_01	identification & operation of cyber defense resources
JC_02_03_02	data collection of cyber defense resources
JC_02_04_01	analysis of detection rules
JC_02_05_01	scanning of vulnerabilities in security systems
JC_02_05_02	recognition of vulnerability in security system
JC_02_06_01	utilization of network nisualization SW
JC_02_07_01	utilization of search engine
JC_02_08_01	verification of network alert
JC_02_09_01	receive and analysis of network alarms
JC_02_10_01	utilization of network firewall
JC_02_10_02	Utilization of Network IDS/IPS
JC_02_10_03	web firewall utilization
JC_02_11_01	monitoring of control data
JC_02_11_02	identification of security issues
JC_02_12_01	monitoring of open source websites
JC_02_13_01	monitoring of operating environment
JC_03_01_01	retaining of evidence integrity
JC_03_02_01	correlation and tracking of intrusion
JC_03_02_02	analysis of incident threat
JC_03_02_03	treatment of incident-related system
JC_03_03_01	detection of intrusion, abnormality, misuse activity and issuance of alarms
JC_03_04_01	verification of IDS/IPS alert
JC_03_05_01	isolation and removal of malware
JC_03_06_01	monitoring and reporting of threat activity
JC_04_01_01	malware analysis
JC_04_02_01	imitation of threat behavior
JC_04_03_01	utilization of social engineering technology
JC_04_04_01	utilization of protocol analysis tool
JC_04_05_01	analysis of vulnerability/attack relation
JC_04_06_01	performance of damage assessment
JC_04_07_01	use of network analysis tools and identification of vulnerabilities
JC_04_08_01	log Analysis for identifying intrusion evidence
JC_04_09_01	packet level analysis
JC_04_010_01	use of security event correlation tools
JC_04_011_01	analysis of traffic for network device
JC_04_012_01	generating and extracting important information through packet capture
JC_04_013_01	recognition and analysis of malicious network activity in traffic
JC_04_014_01	utilization of DB for target-related information identification
JC_04_015_01	analysis and reconfiguration of tracking path tool-based networks
JC_04_015_02	analysis of tracking path tool-based results
JC_04_016_01	analysis of network traffic characteristics
JC_04_016_02	identify abnormal activity and potential threats to network resources
JC_04_017_01	identification of host log-based threats
JC_04_017_02	network traffic log-based threat identification
JC_04_017_03	identify firewall and IDS log-based threats
JC_04_018_01	developing cyber defense incident Review Plan
JC_04_018_02	implementation of cyber defense incident review
JC_04_019_01	tracking and documenting cyber defense cases
JC_04_020_01	identification and analysis of metadata-based abnormal network traffic
JC_05_01_01	development and deployment of signatures
JC_05_02_01	protect your network from malware
JC_05_03_01	build a Boolean operator-use query
JC_05_04_01	update of IDS/IPS detection rules
JC_05_04_02	update of virus vaccine
JC_05_04_03	update of contents blacklist

5.2 (단계2)직무 요구 기술 식별·구성

사이버 위협 대응 기술 보유 능력을 평가하기 위해서는, 이와 연관된 기술을 식별해야 한다. 하지만 연관된 사이버보안 기술이 너무나 많기 때문에 효과적인 관리를 위해서 체계적인 분류 방법이 필요하다.

사이버보안기술분류를 활용하여 직무별로 요구되는 기술을 식별하고, 만일 해당 분류표에 없는 기술이 식별된 경우, 기술 분류표에 추가하여 확장하도록 한다.(Fig. 11.) 본 연구에서 제안하는 사이버보안 기술분류는 Table 5.와 같으며, 이는 사이버보안 직무를 수행할 때 요구되는 기술을 구성하였다.

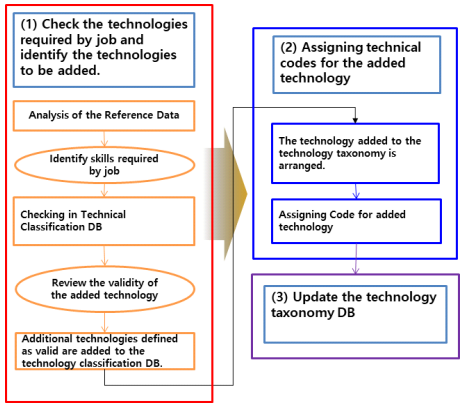


Fig. 11. (Step 2) Structuring job-associated technologies for real-time technical response against cyber threats

Table 5. Cybersecurity technology taxonomy

Name of level 1 tech.	Name of level 2 tech.	Code of level 3 tech.	Name of level 3 tech.
Network	Network equipment	TC_01_01_01	Router
		TC_01_01_02	Switch/hub
	Wireless network equipment	TC_01_02_01	Wireless router
Cyberse curity system	Network security	TC_02_01_01	Firewall
		TC_02_01_02	IDS/IPS
		TC_02_01_03	UTM
		TC_02_01_04	VPN
		TC_02_01_05	DDoS equipments
		TC_02_01_06	ESM/SIEM
		TC_02_01_07	NMS
		TC_02_01_08	NAC
	Wireless network security	TC_02_02_01	WIPS
	System security	TC_02_03_01	Antivirus
		TC_02_03_02	DLP
		TC_02_03_03	DRM
	Web security	TC_02_04_01	web firewall
Network security	Detection rule management	TC_03_01_01	firewall policy
		TC_03_01_02	IPS/IDS detection rule
		TC_03_01_03	Detection Profile (SIEM-related)
		TC_03_01_04	thresholds(traffics, etc.)
	Event analysis	TC_03_02_01	packet level analysis
		TC_03_02_02	traffic statistics analysis
		TC_03_02_03	network status analysis
	Development of Detection Signature/Pattern	TC_03_03_01	Detection Signature/ Pattern Development (Utilization of PCRE)
Operati ng system security	Windows server OS security	TC_04_01_01	Windows Server OS Security Operation
		TC_04_01_02	Windows Server OS Security Configuration
	Linux server	TC_04_02_01	Linux server OS security operation
	OS security	TC_04_02_02	Linux server OS security configuration
	UNIX server OS security	TC_04_03_01	UNIX server OS security operation
		TC_04_03_02	UNIX server OS security configuration
	Windows user OS security	TC_04_04_01	Windows user OS security
	Linux user OS security	TC_04_05_01	linux user OS security
	UNIX user OS security	TC_04_06_01	UNIX user OS security
Web security	Web application security	TC_05_01_01	web vulnerability response
		TC_05_01_02	script dyslexia
DB security	DBMS security	TC_06_01_01	DBMS security ops.
		TC_06_01_02	DBMS security configuration
	DB query security	TC_06_02_01	DB query security design
		TC_06_02_02	DB query security implementation
Vulnera bility	Vulnerability diagnosis	TC_07_01_01	network equipment vulnerability diagnosis
		TC_07_01_02	PC vulnerability diagnosis
		TC_07_01_03	A server (Windows/Linux/Unix) vulnerability diagnosis
		TC_07_01_04	Diagnosing WEB/WAS server vulnerability
		TC_07_01_05	DBMS vulnerability diagnosis
		TC_07_01_06	information security system vulnerability diagnosis
		TC_07_01_07	mobile application vulnerability diagnosis
		TC_07_01_08	simulated hacking
	Vulnerability analysis	TC_07_02_01	static analysis
		TC_07_02_02	Dynamic analysis
		TC_07_02_03	Mobile vulnerabilities Analysis
		TC_07_02_04	Web vulnerability analysis
	Unknown vulnerability study	TC_07_03_01	1-day vulnerability
		TC_07_03_02	0-day vulnerability
Digital forensic	Information collection	TC_08_01_01	Windows Volatility Information Collection
		TC_08_01_02	Windows nonvolatile information collection
		TC_08_01_03	Linux/Unix Volatility Information Collection
		TC_08_01_04	Linux/Unix nonvolatile information collection
		TC_08_01_05	network system log collection
		TC_08_01_06	information security system log collection
		TC_08_01_07	IT system log collection

		TC_08_01_08	Online imaging
		TC_08_01_09	Offline imaging (Use of Expert Equipment)
	Information analysis	TC_08_02_01	Timeline manual analysis (such as xslx)
		TC_08_02_02	Timeline Automatic Analysis
Malware	Malware management	TC_09_01_01	malicious code information collection
		TC_09_01_02	malicious code registration and management
	Malware analysis	TC_09_01_01	malicious code information collection
		TC_09_02_02	Static analysis
		TC_09_02_03	Dynamic Analysis
Programming	web programming	TC_10_01_01	Client side language (Javascript etc.)
		TC_10_01_02	Server side language (Python, php, jsp etc.)
	application programming	TC_10_02_01	User level language (C#, Java, Python etc.)
		TC_10_02_02	kernel level language (C, .NET, etc.)
	script	TC_10_03_01	Linux/Unix bash shell
		TC_10_03_02	windows catch
	DB language	TC_10_04_01	MySQL/MSSQL
		TC_10_04_02	Oracle
		TC_10_04_03	Others (MonoDB, etc.)
	embedded programming	TC_10_05_01	assembly/crosscompile
		TC_10_05_02	embedded system
Virtualization & cloud tools	Vmware/Virtualbox	TC_11_01_01	Vmware/Virtualbox
	AWS	TC_11_02_01	AWS
	Azure	TC_11_03_01	Azure
Etc	Search engine utilization	TC_99_01_01	Use search result filter options
		TC_99_01_02	Analysis of English Results

85종의 레벨3 기술은 기본적인 사이버보안 기술 분류로 적용하여 직무·기술 연관 매트릭스 및 이를 기반으로 직무 역량 평가 구현에 적용한다.

5.3 (단계3)직무·기술 연관 매트릭스 구현

5.3.1 직무·기술 연관 매트릭스 구현 방법

CtrJC 프레임워크에서 제안된 방법론인 사이버보안 직무·기술 연관 매트릭스(AMCJT)를 구현하는 것은 앞에서 식별한 직무와 기술의 연관성을 분석하여 요구되는 기술력 수준을 판별할 수 있는 기반을 구현하는 것이다.(Fig. 12.)

AMCJT를 제대로 구현하기 위해서는 직무와 기술 분야에 대한 전문가적인 관점에서 식별해야 하므로 이 자체도 복잡하고 어려운 연구 주제이다. 본 논문에서는 레벨3 직무 1종을 선정하여 AMCJT를 구현하고 CtrJC-R모델을 검증하는데 활용한다.

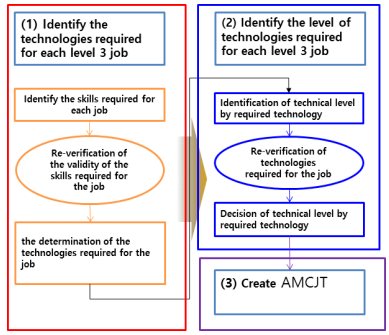


Fig. 12. (Step 3) Developing AMCJT for real-time technical response job against cyber threats

Table 6. AMCJT(Operation of network firewall, JC_01_01_01)

Level 3 technology code	Level 3 technology name	KC	OC	IC
TC_01_01_01	router	M	M	
TC_01_01_02	switch/hub	M	M	
TC_02_01_01	firewall	M	H	
TC_02_01_02	IDS/IPS	M	H	
TC_02_01_03	UTM	M	M	
TC_02_01_04	VPN (virtual private network)	M	M	
TC_02_01_05	DDoS equipments	M	M	
TC_02_01_06	ESM/SIEM	M	H	
TC_02_01_07	NMS	M	M	
TC_02_01_08	NAC	M	M	
TC_02_02_01	WIPS	M	M	
TC_02_03_01	antivirus	M	H	
TC_02_03_02	DLP	M	M	
TC_02_03_03	DRM	M	M	
TC_02_04_01	web firewall	M	H	L
TC_03_01_01	firewall policy	M	H	L
TC_03_01_02	IPS/IDS detection rule	M	H	L
TC_03_01_03	Detection Profile	M	M	
TC_03_01_04	thresholds of traffics	L	M	
TC_03_02_01	packet level analysis	L	M	
TC_03_02_02	traffic statistics analysis	L	M	
TC_03_02_03	network status analysis	L	M	
TC_03_03_01	Detection Signature/Pattern Development	M	H	L
TC_04_02_01	Linux server OS security operation	M	H	L
TC_04_02_02	Linux server OS security configuration	M	H	L
TC_04_03_01	UNIX server OS security operation	M	H	L
TC_04_03_02	UNIX server OS security configuration	M	H	L
TC_04_05_01	Linux user OS security	M	H	L
TC_04_06_01	UNIX user OS security	M	H	L
TC_05_01_01	web vulnerability response	L	L	L

TC_05_01_02	script obfuscation	L	L	L
TC_07_01_01	network equipment vulnerability diagnosis	L	L	L
TC_07_01_02	PC vulnerability diagnosis			
TC_07_01_03	A server (Windows/Linux/ Unix) vulnerability diagnosis	L	L	L
TC_07_01_04	Diagnosing WEB/WAS server vulnerability	L	L	L
TC_08_01_03	Linux/Unix Volatility Information Collection	L	L	L
TC_08_01_04	Linux/Unix nonvolatile information collection	L	L	L
TC_08_01_05	network system log collection	L	L	L
TC_08_01_06	information security system log collection	L	L	L

5.3.2 직무·기술 연관 매트릭스 구현 사례

레벨3 직무 중 대표적으로 네트워크 방화벽 운영(JC_01_01_01)에 요구되는 기술(Table 4의 첫 번째 항목)은 Table 5의 사이버기술분류표의 매핑을 활용하여 40종 별로 요구 기술 수준을 식별하였다(Table 6.).

Table 7.에서 보듯이 네트워크 방화벽 운영에 요구되는 특성을 살펴보면, 대체로 높은 운영 능력이 요구되며, 지식 능력은 H(높음) 수준을 요구하지 않고, 구현 능력은 H(높음), M(중간) 수준을 요구하지 않고 있다.

Table 7. Capacity for operation of network firewall

	H		M		L		계	
Knowledge capacity (KC)	0	0%	25	29%	15	18%	40	47%
Operation capacity (OC)	14	16%	15	18%	11	13%	40	46%
Implementation capacity (IC)	0	0%	0	0%	21	25%	21	25%

5.4 (단계4)직무 기술 보유 능력 평가

직무별로 직무·기술 연관 매트릭스가 작성되면 직무 역량을 평가할 준비가 된 것이다. 물론 평가는 객관적인 방법론이 요구되나 본 논문에서는 세부적으로 다루지 않고 향후 연구가 요구되는 분야이다.

5.4.1 직무 기술 보유 능력 평가 방법

직무 역량 평가를 위해 요구되는 방법론은 진단, 측정, 자격의 과정으로 구성된다. 본 논문에서는 다음과 같이 구현한다.

(1) 직무별 직무·기술 연관 매트릭스에 가중치 점수 부여
직무별로 요구되는 기술 수준을 점수화하여 역량 평가를 수행 할 수 있다. 본 논문에서는 "H : 3, M : 2, L : 1"과 같이 점수화하여 적용하기로 한다.

(2) 직무별 요구 기술력의 진단 또는 측정
직무별로 요구되는 기술력에 대해 0~3점을 적용하는 자가 진단을 수행한다. 자가 진단은 지식 능력(KC), 운영 능력(OC), 구현 능력(IC) 별 점수와 총점을 산정할 수 있다. 또한 직무별로 요구되는 기술력 점수를 100점 만점으로 환산하여 등급을 적용할 수 있다. 예를 들면 100점 만점으로 측정하여 A, B, C, D, F 등급으로 산정 가능하다.

(3) 진단/측정 결과에 대한 직무별 기술력 비교 분석 수행
자가 진단 결과 완성된 자가 진단 매트릭스를 기반으로 해당 직무를 수행하는데 필요한 기술력이 어느 정도인지 분석하여 평가를 수행하는 단계이다. 기초적인 진단 데이터를 직무별 직무·기술 연관 매트릭스를 기준으로 부족한 기술 및 그 수준에 대해 정량적으로 평가하는 단계이며 세부 방법론은 별도 연구가 요구되는 분야이다.

5.4.2 직무 평가 구현 사례

앞에서 제안된 5종의 직무·기술 연관 매트릭스 중 네트워크 방화벽 운영(JC_01_01_01)의 가상적인 진단 결과를 적용하여 비교 분석하고자 하며, 다음 표는 자가 진단 결과 파악된 가상의 전문인력의 보유 기술 능력의 사례로 항목별로 수준에 따른 가중치 점수를 부여한 결과를 보여주고 있다.(Table 8.)

Table 8. Required capability and diagnosis result

	Required technology capability			technology capability diagnosis result		
Level 3 technology code	KC	OC	IC	KC	OC	IC
TC_01_01_01	2	2		1	1	
TC_01_01_02	2	2		1	2	
TC_02_01_01	2	3		1	2	
TC_02_01_02	2	3		1	2	
TC_02_01_03	2	2		1	2	
TC_02_01_04	2	2		1	1	
TC_02_01_05	2	2		1	2	
TC_02_01_06	2	3		1	2	
TC_02_01_07	2	2		1	2	
TC_02_01_08	2	2		1	2	
TC_02_02_01	2	2		1	2	
TC_02_03_01	2	3		1	3	
TC_02_03_02	2	2		1	2	
TC_02_03_03	2	2		1	1	
TC_02_04_01	2	3	1	1	3	1
TC_03_01_01	2	3	1	1	2	1
TC_03_01_02	2	3	1	1	2	1
TC_03_01_03	2	2		1	2	
TC_03_01_04	1	2		2	1	
TC_03_02_01	1	2		0	1	
TC_03_02_02	1	2		2	2	
TC_03_02_03	1	2		0	1	
TC_03_03_01	2	3	1	1	0	1
TC_04_02_01	2	3	1	2	3	1
TC_04_02_02	2	3	1	3	2	1

TC_04_03_01	2	3	1	2	1	0
TC_04_03_02	2	3	1	2	2	1
TC_04_05_01	2	3	1	3	2	1
TC_04_06_01	2	3	1	2	1	1
TC_05_01_01	1	1	1	1	1	0
TC_05_01_02	1	1	1	1	0	1
TC_07_01_01	1	1	1	1	1	1
TC_07_01_03	1	1	1	1	0	1
TC_07_01_04	1	1	1	1	1	1
TC_08_01_03	1	1	1	1	1	1
TC_08_01_04	1	1	1	1	1	0
TC_08_01_05	1	1	1	1	0	1
TC_08_01_06	1	1	1	1	1	0
TC_10_03_01	1	1	1	1	1	1
TC_99_01_01	1	1	1	1	1	1

Table 9. Evaluation result of technology capability of Operation of network firewall(JC_01_01_01)

	Knowledge capacity (KC)			Operation capacity (OC)			Implementation capacity (IC)			Total		
	R_S	A_S	C_S	R_S	A_S	C_S	R_S	A_S	C_S	R_S	A_S	C_S
H	0	6		42	9		0	0		42	15	
M	50	12		30	34		0	0		80	46	
L	15	30		11	16		21	17		47	63	
Sum	65	48	74	83	59	74	21	17	81	169	124	74
G			C			C			B			C

* R_S: Required Score, A_S: Acquired Score, C_S: Conversion Score

부여된 점수와 기준 점수 비교를 통해 지식능력(KC), 운영능력(OC), 구현능력으로 분류하여 점수 및 등급을 분석한 결과는 Table 9.와 같다.

5.4.3 (종합)직무 평가 사례 종합 분석

앞에서 분석한 1개 사례 외에 4개 직무를 추가하여 분석한 결과를 적용하여 분석한 5개 사례의 직무로 구성된 전담 부서의 보유 기술 능력을 종합적으로 분석하는 관점에서 Table 10.과 같이 정리하였다. 여기서는 개별적인 직무의 KC, OC, IC 수준별로 보유 능력을 파악할 수 있다.

Table 10. Comprehensive evaluation result of technology capability for 5 jobs(I)

	Knowledge capacity (KC)				Operation capacity (OC)				Implementation capacity (IC)			
	R_S	A_S	C_S	G	R_S	A_S	C_S	G	R_S	A_S	C_S	G
#1	65	48	74	C	83	59	71	C	21	17	81	B
#2	52	40	77	C	60	39	65	D	6	4	67	D
#3	25	21	84	B	26	19	73	C	2	1	50	F
#4	39	32	82	B	48	29	60	D	0	0	-	-
#5	87	55	63	D	84	40	48	F	6	2	33	F
Sum	268	196	380		301	186	317		35	24	231	
Avg	**54**	**39**	**76**	**C**	**60**	**37**	**63**	**D**	**7**	**5**	**46**	**F**

* G : Grade

Table 11. Comprehensive evaluation result of technology capability for 5 jobs(II)

	Total five jobs			
	Required Score	Acquired Score	Conversion Score	Grade
#1	169	124	73	C
#2	118	83	70	C
#3	53	41	77	C
#4	87	61	70	C
#5	177	97	55	F
Sum	604	406	346	
Avg	121	81	69	D

또한 Table 11.은 직무별 전체 등급 및 직무 종합 등급을 확인할 수 있다. 이와 같이 실시간 사이버 위협 대응 기술적 직무 역량 모델 구현을 통해 개별 직무 및 여러 직무의 종합적인(예, 특정 전담 부서) 기술 보유능력을 정량적으로 확인할 수 있다.

5.5 실시간 사이버 위협 기술적 대응 직무 역량 모델의 활용성 검토

본 논문은 사이버보안 기술 분야의 직무 역량 모델을 설계하여 제시하였으나, 기존의 유사 방법론이 부재한 관계로 상호 비교가 어려운 상황이다. 유사하게 국내의 직무능력표준(NCS)의 정보보호 분야를 거론할 수 있으나, 독자적인 채용 조직 및 체계를 갖추기 어려운 중소기업 대상의 적용을 가정하여 시작하였다. 또한 정보보호 분야의 정확한 기술적 수요 및 공급 등의 분석이 부족하여 현실성이 부족하며, 신규 채용에만 적용한다는 한계점이 존재한다. 미국 NICE 프레임워크는 연방기관의 직무에 준하는 업무 역할 52종을 선정하여 작업, KSA를 제시하고 있으나, 그 수준이 추상적인 관계로 해당 기관은 자체적인 인력 채용 및 유지 방법론을 갖추어야 한다.

여기서 제안하는 모델은 NICE 프레임워크를 세부적으로 분석하여 기술적인 역량을 평가하는 방법론을 제시하고 가상적 데이터를 기반으로 객관성이 보장되는 정량적인 역량 평가 결과를 보여주는 방법을 확인할 수 있다. 이 모델이 갖는 의미는 크게 3가지로 분류해서 설명할 수 있다.

첫째, 새로운 사이버보안 기술 역량 모델 구현 방안을 다음과 같이 제시하고 있다.

- 실현 가능한 기술적 직무 역량 모델 개발
- 기존 역량 및 능력 모델의 비정형성, 주관적, 지속성 등의 문제를 극복하는 방법론 개발

- 구성원의 기술적 역량을 정확히 파악하는 이 모델을 적용하여 조직의 인적 역량을 기존 조직 능력 모델에 연계하는 방법론 개선

둘째, 기술 격차 및 부족 해결을 위한 기본 모델로서 산업계에서 요구하는 역량과 학계에서 교육하는 역량과의 격차를 극복하기 위해서는 상호 바라보는 공통된 관점 및 개념이 중요한데, 이에 대한 방법론으로 활용할 수 있다.

셋째, 국가차원의 전문인력 육성 제도화의 기본틀을 다음과 같이 제시하고 있다.

- IT기술 및 보안기술의 끊임없는 변화 및 복잡성으로 인하여 규격화하기 어려운 사이버보안 기술에 대해 기술 분류를 통한 규격화 시도
- 국가 차원의 인력 양성 정책의 새로운 방향에 활용 가능한 방법론

VI. 결 론

사이버 위협이 국가 안보에서 개인의 사생활까지 침해하는 수준으로 진화되어 왔다. 이에 대한 대응책은 모든 국가들의 핵심 방어 정책으로 다루어지고 있으며 많은 예산과 인력이 투입되고 있으나, 급증하는 위협에 비해서 사이버보안 전문인력 양성 속도가 늦어 전문인력의 부족 문제가 심각한 실정이다. 또한 학교에서 배출하는 인력과 산업 현장에서의 전문성 사이에서 발생하는 기술 격차 문제도 역시 심각한 상황이다.

이와 같은 문제점을 해결하기 위해서 요구되는 전문인력의 역량을 정확히 식별하여 갖춰야할 역량을 제시하고 보유 역량을 정확히 평가할 수 있는 방법론이 요구된다.

본 논문에서 제시한 사이버보안 직무 역량의 개념적인 검토를 통해 “사이버보안 기술적 대응 직무 역량(CtrJC) 프레임워크”를 제안하여 기술적 대응 직무에 요구되는 역량에 대해 정의하고 평가할 수 있는 모델을 만들어 낼 수 있는 방법론을 제시하였다. 이 프레임워크의 효과를 확인하기 위해 “실시간 사이버 위협 대응 기술적 직무 역량(CtrJC-R) 모델”을 구현하였다.

사례로 구현된 모델은 사이버 위협에 대응하는 기술적인 역량을 식별, 평가가 가능한 모델로서 정부, 산업계 및 학계에서 사이버보안 전문인력 역량을 확인 및 양성하는 기초로 활용할 수 있는 방법론이다. 여기서 구현된 분야는 NICE 프레임워크의 52개 업무 역할 중 6개 정도로 제한될 정도로 일부를 구현한 모델이다. 사이버보안 인력의 역량 평가를 위해서 본 논문의 프레임워크를 도입하여 자체 모델을 만들어 낸다면 전문가들이 공감하고 인정할 수 있는 역량 평가가 가능할 것으로 기대하며, 추후 연구의 주제로 남겨둔다.

References

[1] Oltsik, J. “The cybersecurity skills shortage is getting worse”. ESG Blogs, 10 Jan. 2019. Accessed Nov. 2020. www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse

[2] (ISC)2, “Strategies for building and growing strong cyber security teams: (ISC)2 Cybersecurity Workforce Study”, 2019. Accessed Nov. 2020. https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

[3] NIST, SP 800-181, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework”, Aug. 2017,

[4] Cyberseek, “cyberseek”, https://www.cyberseek.org/ accessed Nov. 2020.

[5] ENISA, “Cybersecurity Skills Development in the EU”, 26 Mar. 2019.

[6] Soonjwa Hong, “A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S.”, Journal of the Korea Institute of Information Security & Cryptology 28(1), pp. 249-267, Feb. 2018.

[7] Korea Information Security Industry Association, “Survey on Information Security”, Jan. 2020.

[8] Korea Information Security Industry Association, “Survey for Information Security Industry in Korea: Year 2019”, Dec. 2019.

[9] Risto Hansen, "Cyber security capability assessment", Master's Thesis of Tallinn University of Technology, Nov. 2016.
[10] PwC & Iron Mountain, "Beyond Cyber Threats: Europe's First Information Risk Maturity Index" Mar. 2012.
[11] McKinsey Digital, "Risk and responsibility in a hyperconnected world", Jan. 2014. Accessed Nov. 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises
[12] Global Cyber Security Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition", Mar. 2016. accessed Nov. 2010. https://gcscc.ox.ac.uk/the-cmm
[13] Rafael Dean Brown, "Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework" Jornal of International Review of Law, Vol. 2018 No. 4, Mar. 2018. DOI https://doi.org/10.29117/irl.2018.0036
[14] US Department of Energy, "Cybersecurity Capability Maturity Model (C2M2) Program". Accessed Nov. 2020. https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program
[15] NIST, "Cybersecurity Framework Version 1.1". Accessed Nov. 2020. https://www.nist.gov/cyberframework/framework
[16] NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1", Apr. 2018.
[17] H. S Venter and J. H. PE loff, "A taxonomy for information security technologies", Computers & Security Volume 22, Issue 4, pp. 299-307, May 2003.
[18] Language Technologies Institute of Carnegie Mellon University, "Cybersecurity Taxonomy". accessed Nov. 2020. http://www.cs.cmu.edu/~dklaper/cybersecurity/website/
[19] David Klaper, Eduard Hendrik Hovy, "A taxonomy and a knowledge portal for cybersecurity", Proceedings of the 15th Annual International Conference on Digital Government Research, pp. 79-85, June 2014.
[20] Vrije Universteit Brussel, "Taxonomy of Security Products, Systems and Services.", Deliverable 1.2 CRISP project, Apr. 2014. accessed Nov. 2020. https://www.trilateralresearch.com/wp-content/uploads/2018/09/CRISP-D1.2-Taxonomy-of-Security-Products-Systems-Services_REVISED.pdf
[21] European Commission, Joint Research Centre(JRC), "A Proposal for a European Cybersecurity Taxonomy", 2019. accessed Nov. 2020. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf
[22] Kyoo-wang Kyeong, "A Study on the Performance-based job Analysis Method based on NCS", Doctorial Thesis of Graduate School of Korea National University of Transportation, pp. 8-9, Dec. 2018.
[23] Lee, Min Kyung, "A Study on Improvement of Project Competency for Small IT Companise through SWOT-AHP Analysis", Master's Thesis of Hanayang University, pp 5-6, Aug. 2018.
[24] Javidan, M. "Core competence: What Does it Mean in Practice?", Long Range Planning, 31(1), pp. 60-71. Feb. 1988. https://doi.org/10.1016/S0024-6301(97)00091-5

[25] The Korean Association For Regional Information Society, Development of job analysis techniques for efficient organization management, Prism of Ministry of the Interior and Safety, pp. 5-6, Dec. 2008. accessed Nov. 2020.

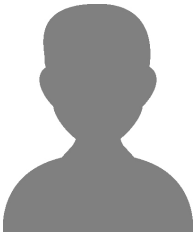
[26] Younghan Choi, Insook Jang, Inteck Whoang, Taeghyoon Kim, Soonjwa Hong, Insung Park, Jinsoek Yang, Yeongjae Kwon, Jungmin Kang, "Design and Implementation of Cyber Range for Cyber Defense Exercise Based on Cyber Crisis Alert", Journal of the Korea Institute of Information Security & Cryptology 30(5), pp. 805-821, Oct. 2020.

[27] The NATO Cooperative Cyber Defence Centre of Excellence, "Locked Shields," accessed Nov. 2020. https://ccdcoe.org/exercises/locked-shields/

〈저자소개〉

홍 순 좌 (Soonjwa Hong) 정회원
1989년 2월: 숭실대학교 전산학과 졸업
1991년 2월: 숭실대학교 전산학과 석사
2005년 8월: 충남대학교 컴퓨터과학과 박사
1991년 2월~2000년 1월: 국방과학연구소(ADD) 선임연구원
2000년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 사이버보안 인력양성 정책, 미래 IT・보안기술, 사이버보안 기술・위협 분석, 국내외 정보보호 법・정책

박 한 진 (Hanjin Park) 정회원
2007년 2월: 연세대 컴퓨터·산업공학과(컴퓨터과학 심화 전공) 졸업(공학사)
2015년 2월: KAIST 전산학과 박사(석·박사 통합) 졸업(공학박사)
2015년 1월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 사이버보안 인력양성 정책, 사이버보안 기술·위협 분석, 국내외 정보보호 법·정책, 미래 IT·보안기술



최 영 한 (Younghan Choi) 정회원
2002년 2월: 한양대학교 전자공학과 졸업(학사)
2004년 2월: KAIST 전자공학과 졸업(공학석사)
2015년 2월: 고려대학교 정보보호대학원 졸업(공학박사)
2019년 2월: 한국방송통신대학교 법학과 졸업(학사)
2004년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
2020년 2월~현재: 사이버안전훈련센터(실장)
〈관심분야〉 사이버보안, 사이버훈련, 사이버법률

강 정 민 (Jungmin Kang) 정회원
2003년 6월~현재: 사이버안전훈련센터(센터장)
2015년 3월~2016년 2월: UCSD QI(Qualcomm Institute) 방문연구원
2014년 4월: 고려대학교 컴퓨터교육학과 졸업(박사)
2011년 7월: NATO 국제회의 한국대표단
2005년~2011년: UN GGE(정보보호 정부전문가그룹) 국제회의 한국대표단
2002년 2월~2003년 5월: 삼성SDS 근무
2002년 2월: 광주과학기술원(GIST) 정보통신공학과 졸업(석사)
〈관심분야〉 사이버교육훈련, 사이버보안 및 회복력, 기반시설보호, 국제동향과 사이버분쟁