반도체디스플레이기술학회지 제20권 제3호(2021년 9월)
Journal of the Semiconductor & Display Technology, Vol. 20, No. 3. September 2021.

# 사이버 보안 분야 전문가 프로파일 관리 시스템 연구

안준영[*]·이승훈[*]·박희민[*]·김현철[*†]
[*†]상명대학교 소프트웨어학과

# Development of a Cybersecurity Workforce Management System

**Jun-young Ahn[*], Seung-hun Lee[*], Hee-min Park[*] and Hyun-chul Kim[*†]**
[*†]Dept. of Software, Sangmyung University

**ABSTRACT**

According to the trend of increasingly sophisticated cyber threats, the need for technology research that can be applied to cyber security personnel management and training systems is constantly being raised not only overseas but also in Korea. Previously, the US and UK have already recognized the need and have been steadily conducting related research from the past. In the United States, by encouraging applications based on related research (NICE Cybersecurity Workforce Framework) and disclosing successful use cases to the outside, it is laying the groundwork for profiling cyber security experts. However in Korea, research on cyber security expert training and profiling is insufficient compared to other countries. Therefore, in this study, in order to create a system suitable for the domestic situation, research and analysis of cases in the United States and the United Kingdom were conducted over the past few years, and based on this, a prototype was produced for the study of profiling technology for domestic cyber security experts.

**Key Words** : NICE Cybersecurity Workforce Framework (NICE Framework), Chartered Institute of Information Security (CIISec), Cyber Security Expert

## 1. 서 론

지능정보사회의 정보보호 위협이 빠르게 증가하고 있고 정보보호의 대상이 개인정보에서부터 민감한 군사정보에 이르기까지 매우 광범위해져, 숙련된 사이버 보안 전문 인력의 중요성이 더욱 커지고 있다. 연구[1]에 따르면 사이버 침해 대응 전담팀을 별도로 운영하는 것이 데이터 유출로 인한 피해를 감소시키는 가장 효과적인 방법으로 제기되고 있으며, 이러한 까닭에 전문 역량을 보유한 사이버 보안 인력의 관리와 양성이 중요시 되고 있다. 이에 미국, 영국 등은 정보보호 업무(또는 직무)를 표준화하고 업무 역할과 필요 수준에 부합하는 인력을 양성하기 위한 기반을 마련하기 위해 오랜 기간 꾸준히 연구를 진행해왔다[2].

미국의 경우, 2017년 사이버 보안 분야 업무 표준분류체계인 NICE Cybersecurity Workforce Framework(이하NICE Framework)[3]를 개발했으며 영국의 경우, CIISec(Chartered Institute of Information Security / 기존 IISP)를 중심으로 한 CIISec Skills Framework[4], IISP Knowledge Framework[5], CIISec Roles Framework[6] 등 다양한 사이버 보안 분야 업무 표준 체계를 연구하고 이를 활용해 사이버 보안 전문가 관리·양성에 대한 연구를 진행하고 있다.

우리나라의 경우 사이버 보안에 특화된 프레임워크는 아니지만, 산업 전반에 걸친 NCS라는 프레임워크가 존재한다. 그러나, 앞선 국가들만큼 사이버 보안 전문가에 특화되어 있지 않고, 조사 기관이나 조사 시기별로 각기 다

[†]E-mail: hkim@smu.ac.kr

른 업무 분류를 사용하고 있어 사이버 보안 인력에 대한 데이터의 수집, 관리는 물론 이를 활용한 정책 및 시스템을 개발하기 위한 데이터로 활용하는 데 한계가 있다[2].

본 연구에서는 사이버 보안 인력 관리·양성을 목적으로 하는 국내·외의 선행 연구와 사례들을 조사, 분석하고 국가 단위의 표준화된 업무 체계 연구를 활용한 사이버 보안 전문 인력 관리·양성 시스템의 사례를 조사 및 분석한다.

## 2. Related Work

### 2.1 NICE Framework (US)

2010년 3월 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 주도로 연구 조직이 설립되었고, NICE Framework[3]의 첫 번째 버전은 2012년 9월에 공개되었다. 이후 크고 작은 업데이트가 있었으며 2017년 8월에 현재의 NICE Framework가 만들어졌다. 2021년 현재까지 수정 버전을 내는 등 지속적인 업데이트를 하는 중이다.

NICE Framework에는 7개의 카테고리 (Category), 33개의 전문 영역(Specialty Area), 및 52개의 직무(Work role)가 있으며 각 직무에 따라 필요한 스킬, 지식, 능력 등이 명시 및 설명되어 있다.

Fig. 1은 이에 대한 구성도이며, Table 1은 Cyber Defense Analyst를 예시로 각 직무를 수행할 땐 담당업무가 무엇인지, 어떤 기술, 지식, 능력을 갖추고 있어야 하는지 설명이 되어 있다. Table 2는 NICE Framework의 직무들을 구성하는 1,006개의 업무, 377개의 기술, 634개의 지식, 177개의 능력들에 대한 설명의 예시이다.

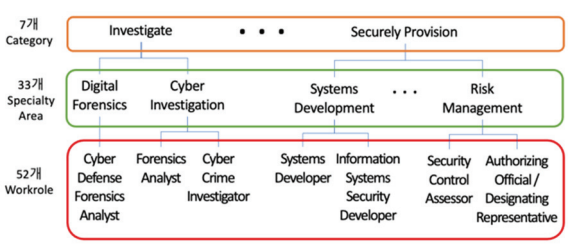


**Fig. 1.** Diagram of NICE Framework.

### 2.2 CIISec Skills Framework (UK)

CIISec의 모체 IISP는 2006년 영국의 사이버 보안 연구를 주 목적으로 하는 비영리기관으로 설립되었다. 2012년에는 NCSC (National Cyber Security Center)로부터 UK 정부 명의로 발급하는 Information Assurance Professionals의 인증기관으로 임명되고, 2019년 6월부 영국 왕실에서 Royal Charter 칭호를 획득하여 국가연구기관으로서 자리매김하였다.

**Table 1.** An example of NICE Framework Work role description and required resources (Cyber Defense Analyst)

| 직 무 | Cyber Defense Analyst | | |
|---|---|---|---|
| 전문영역 | Cyber Defense Analysis (CDA) | | |
| 카테고리 | Protect and Defend (PR) | | |
| 직무설명 | 다양한 사이버 방어 도구 (예 : IDS 경보, 방화벽, 네트워크 트래픽 로그)에서 수집된 데이터를 사용하여 사이버 위협의 완화를 위해 환경 내에서 발생하는 이벤트를 분석 | | |
| 담당업무 | T0020, T0023, … | 지 식 | K0001, K0002, … |
| 기 술 | S0020, S0025, … | 능 력 | A0010, A0015, … |

**Table 2.** An example of Knowledge, Skill, Ability

| I D | 설 명 |
|---|---|
| K0001 | 컴퓨터 네트워킹 개념과 프로토콜, 네트워크 보안 방법론에 대한 지식 |
| S0001 | 취약성 스캔을 수행하고 보안 시스템의 취약성을 인식하는 기술 |
| A0001 | 취약성 및 구성 데이터 분석을 기반으로 시스템 보안 문제를 식별하는 기능 |

IISP가 발간한 Framework로는 Skills Framework[4], Knowledge Framework[5]가 있으며, CIISec로 승격되면서 Roles Framework [6]가 추가되었다. IISP 핵심 업무 중 하나라고 볼 수 있는 Framework연구와 관련해서, 2007년에는 IISP Skills Framework를 발표, 꾸준한 개정을 거쳐 2018년 3월에는 버전 2.2를 발표했고, CIISec 출범 이후는 CIISec Skills Framework (Fig. 2)로 계승되었다. 역량 레벨은 총 6단계로 구성되어 있으며 버전 2.2 발표당시, 11개의 업무 섹션, 33개의 스킬 그룹으로 세분화하였고 현재까지도 꾸준히 업데이트 중이다.


**Fig. 2.** CIISec Skills Framework.

Skills Framework는 A부터 K까지 총 11개의 섹션으로 이뤄져 있으며, 섹션 A부터 I는 사이버 보안에서 필요한 기술을 다루고, 섹션 J는 효과적으로 일하는 데 필요한 대인관계 및 공동 기술을 정의하며 섹션 K는 개인 경력 개발을 지원하고 직업을 발전시키는 데 필요한 기술을 정의한다.

CIISec Skills Framework에서는 사용자가 각 스킬에 대하여 어떤 수준의 능력을 가지고 있는지를 파악할 수 있도록 스킬별 수준에 따른 정의를 달리하며, Table 3은 그 정의를 이용하여 만든 CIISec Skills Framework에서 스킬과 수준에 대한 정의의 예시이다.

**Table 3.** An example of skill definition and levels in the CIISec Skills Framework (Forensics)

| ID | F3 | |
|---|---|---|
| Skill Name | Forensics | |
| Skill Description | · 적절한 전문 장비를 사용하여 현장을 보호하고 법적 지침에 따라 가장 효과적인 방식으로 비즈니스 중단을 최소화 및 증거 가중치를 유지하는 증거를 캡처<br>· 증거를 분석하여 맬웨어의 존재를 포함하여 정책, 규정 또는 법률 위반을 식별<br>· 필요 시 전문가 증인 역할을 하는 적절한 증거를 제시 | |
| Level Description | Lv.1 | 디지털 포렌식의 기본 원칙을 설명하고 조사를 지원하는 포렌식의 능력을 인식 |
| | Lv. 2 ~ Lv. 5에 대한 설명 | |
| | Lv.6 | · 대규모 조직 내에서 또는 여러 고객에 걸친 포렌식 작업을 담당.<br>· 까다로운 법의학 운영을 이끌고 있다. 관련 법규를 깊이 이해하고 있음 |

### 2.3 CyBOK (UK)

CyBOK[7]은 국가 차원의 보안 인력 양성을 위해서 2017년에 National Cyber Security Programme의 투자를 바탕으로 University of Bristol이 중심이 되어 시작한 프로젝트이다. 공식적으로는 2020년에 공표되었으며 현재는 NCSC로부터 그 지위를 인정받아 국가적 보안 인력 양성 프로그램에서의 기본 요소로 사용되고 있다.

CyBOK은 이미 확립된 지식 체계를 중복된 내용 없이 새롭게 정의하는 것을 목적으로 한다. 따라서 CyBOK의 Knowledge를 구성할 때 Fig. 3과 같이 기존의 연구가 진행된 IISP Skills Framework, IEEE Symposium on Security & Privacy 등 사이버 보안과 관련된 다수의 문건을 수집하고 자연어 처리 기법(NLP)을 사용하여 사이버 보안의 큰 주제들을 5개의 카테고리와 19개의 상위 지식 영역으로 분류했다.

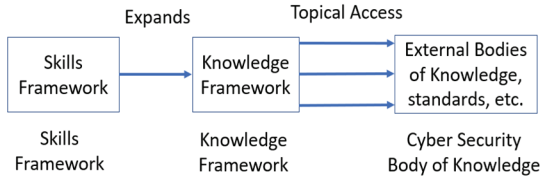


**Fig. 3.** Relationship between Skills&Knowledge Framework and CyBOK.

### 2.4 NCS (Korea)

미국과 영국의 사례처럼, 한국에도 국가직무능력표준(NCS, National Competency Standards)[8]이라는 업무 표준 분류 체계가 있다.

NCS는 2019년 6월을 기준으로 24개의 직업 분야와 1,001개의 직무(NCS), 12,405개의 능력 단위로 구성되어 있다. 직무는 NCS 분류표의 세분류를 의미하고, 이 세분류의 하위 단위인 능력단위는 NCS의 기본 구성요소에 해당한다. 능력 단위는 능력 단위 분류 번호, 능력 단위 정의, 능력 단위 요소(수행 준거, 지식, 기술, 태도), 적용범위 및 작업 상황, 평가 지침, 직업 기초 능력 등으로 구성되어 있다.

NCS는 산업 현장 직무의 수준을 체계화하여 수준 체계를 제시하는데 '산업현장-교육훈련-자격'연계, 평생 학습 능력 성취 단계 제시, 자격의 수준 체계 구성에서 활용되며, NCS 개발 시에는 8단계의 수준 체계에 따라 능력 단위 수준을 평정하여 제시한다.

NCS 직무 체계에서 정보보호 분야의 세분류, 능력 단위 요소는 Table 4와 같이 구성되어 있다.

**Table 4.** An example of NCS job hierarchy subdivision

| 세분류 | 보안사고 분석대응 | |
|---|---|---|
| 능력요소 | 디지털포렌식 | |
| 능력단위 요소 | 디지털 포렌식 분석하기 | |
| 수행준거 | 업무 | 사고 발생 시 법정에서 요구하는 절차에 의거하여 증거로서의 효력이 발생할 수 있도록 수집된 자료를 분석할 수 있다. |
| | | (중략) |
| | 지식 | 디지털 포렌식에 대한 동향 |
| | | (중략) |
| | 기술 | 디지털 포렌식 도구 활용 기술 |
| | | (중략) |
| | 태도 | 디지털 포렌식 최신 동향을 습득하려는 태도 |
| | | (중략) |

### 2.5 Use Cases (iQ4, Career Framework)

1) iQ4 - NICE Framework

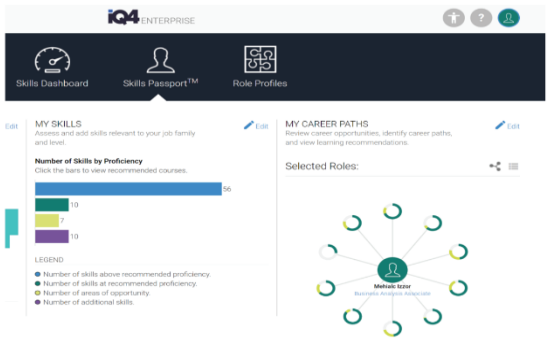


**Fig. 4.** Skills Passport of iQ4 which shows analysis results according to user's skills score.

NICE Framework는 각 기업/단체들이 국가 표준에 맞는 인재들을 양성하고, 인적 자원 관리 및 커리어 관리 등을 하는 형태로 사용이 된다.

iQ4[1]는 이를 실행하고 있는 미국의 대표적인 기업으로써 Fig. 4와 같은 자사만의 시스템을 바탕으로 개인의 역량과 직무별 요구 사항(기술, 지식 등) 들을 분석하여 어느 부분이 부족하고 어느 부분이 뛰어난 지 비교하는 서비스를 제공해주고 있다.

2) Career Framework[2] – CIISec Frameworks, CyBOK

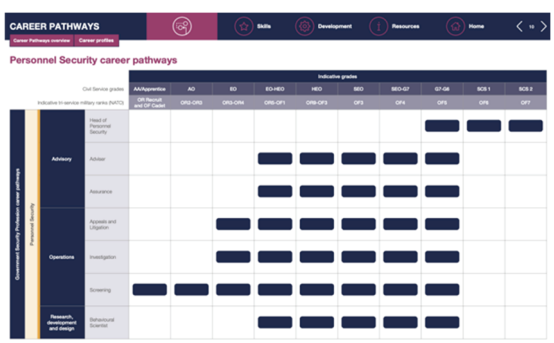


**Fig. 5.** Job proficiency required by the government for public service.

영국 또한 미국의 iQ4와 마찬가지로 커리어에 대한 설계 및 분석을 해줄 수 있는 서비스가 존재한다. NCSC의 Career Framework가 그 대표적인 예이다. Career Framework는 CIISec Frameworks, IISP Frameworks, CyBOK 등의 내용을 바탕으로 국가 차원에서 관련 서비스를 제공하고 있다. Career Framework에서는 사이버 보안의 직군별로 필요한 능력에 대하여 확인할 수 있으며 Fig. 5와 같이 정부 부처에서 요구되는 직무 숙련도를 확인할 수 있다.

[1] iQ4 website : https://www.iq4.com/

[2] https://www.gov.uk/government/publications/the-government-security-profession-career-framework

## 3. Proposed System

### 3.1 시스템 아키텍처

Fig. 6은 사이버 보안 전문가를 프로파일링하기 위하여 전문가가 가지고 있는 기술을 확인하는 기능의 흐름도이다. 붉은 박스는 사이버 보안 전문가의 기술과 개인정보를 조사하여 프로파일링 하는 과정이고, 파란색 박스에서는 사이버 보안 전문가의 프로파일링 과정 이후에 진행되는 과정으로 사이버 보안 전문가가 활동할 직무를 선택하는 과정이다. 사이버 보안 전문가가 선택한 KSA와 NICE Framework에서 직무의 KSA 조건과 비교하여 가장 근접한 직무 후보들을 출력하고 사이버 보안 전문가가 직접 선택한다. 선택된 직무는 유저 정보를 관리하는 DB에 추가된다.

### 3.2 시스템 구현

가. 프로파일링 시스템 시작 화면

Fig. 6 흐름도를 기반으로 제작한 프로토타입 구현 결과물에 대해서 설명하자면, Fig. 7은 NICE Framework 기반 사이버 보안 전문가 프로파일링 시스템의 시작 화면이다. 시작 화면에는 3가지의 기능이 있다. ①과 ②는 사이버 보안 전문가가 자신이 보유하고 있는 지식, 스킬, 능력(KSA)을 선택하기 위하여 사용하는 탐색 기능, ③은 선택이 완료된 후 사이버 보안 전문가와 근접한 직무와 프로파일링 결과를 보기 위한 기능이다.

나. KSA 선택을 위한 탐색

①은 키워드 기반 탐색 기능이다. 사이버 보안 전문가가 자신이 보유하고 있는 KSA의 키워드를 입력하면 Fig. 8-1과 같이 해당 키워드가 삽입된 KSA가 출력된다. 키워드 검색을 통해 출력된 KSA 중 사이버 보안 전문가가 보유한 KSA를 선택한다.

②는 NICE에서 명시된 카테고리, 전문 영역, 직무 기반의 탐색 기능이다.

사이버 보안 전문가가 자신과 관련 있거나 관심 있는 항목을 선택하면 Fig. 8-2처럼 NICE Framework에서 정의한 직무의 KSA 집합을 출력한다.

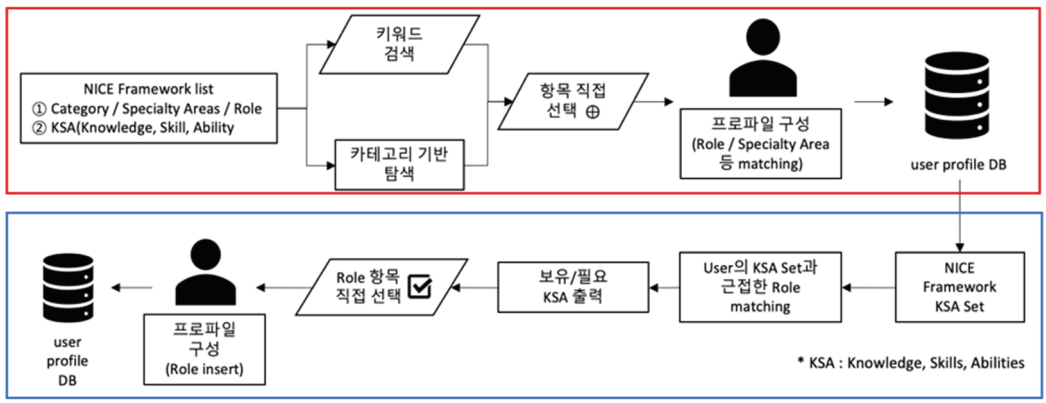


**Fig. 6.** Flowchart of Cyber Security Expert Profiling System.

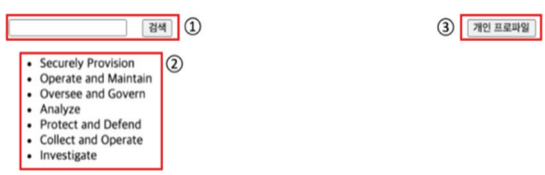


**Fig. 7.** Profiling System Startup Screen.

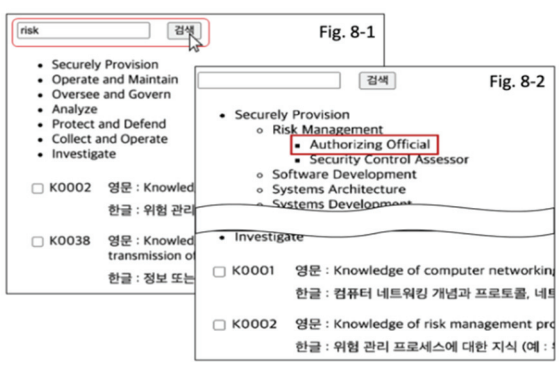


**Fig. 8.** Navigation screen for selecting KSA.

Fig. 8-1과 Fig. 8-2의 화면에서 사이버 보안 전문가는 자신이 보유하고 있는 KSA를 모두 선택한 다음 본인의 개인 정보(아이디, 이름 소속기관/부서)를 입력 후 저장 버튼을 누르면 DB에 자신의 개인 정보와 KSA를 저장할 수 있다

### 다. 사이버 보안 전문가 직무 매칭 및 직무 표시

Fig. 7에서 ③ 버튼을 누르면 검색 창 화면으로 전환된다. 이 때, Fig. 9의 ① 검색창에 사이버 보안 전문가가 자신의 아이디를 입력하면 저장된 프로파일 데이터를 기반으로 현재 가지고 있는 KSA와 근접한 직무를 Fig. 9와 같이 매칭한다. 시스템에서는 사이버 전문가의 KSA와 NICE Framework 직무의 KSA를 비교하여 가장 많이 보유하고 있는 직무 순서대로 추천한다. 시스템 사용자는 Fig. 9의 ②에서 자신이 원하는, 할 수 있는 직무를 선택할 수 있고 Fig. 10은 시스템에서 매칭된 직무와 사이버 보안 전문가의 KSA 비교 결과이다. 붉은색으로 표기된 정보는 현재 사이버 보안 전문가가 보유하고 있는 KSA이며 검은색으로 표기된 정보는 사이버 보안 전문가가 해당 직무로 활동하기 위해 필요한 KSA이다. 표 왼쪽 부분에는 매칭된 직무에 대해 사이버 보안 전문가가 보유하고 있는 KSA의 개수를 표기하여 보여준다.

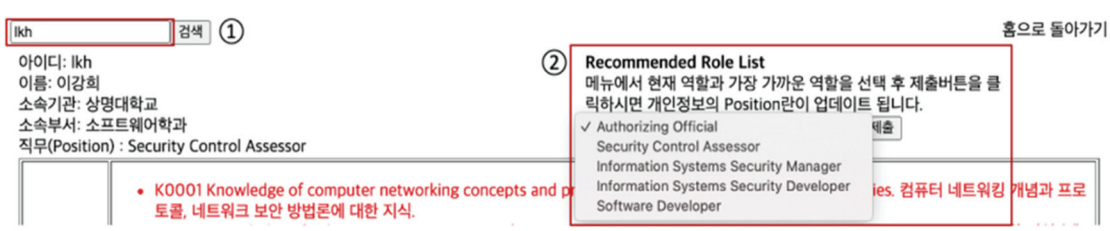


**Fig. 9.** Work role matching result of Cyber Security Expert.

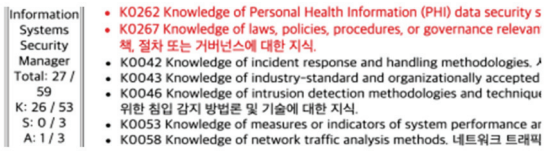


**Fig. 10.** Comparison result of matched work role and Cyber Security Expert's KSA.

### 라. 기관 및 부서별 요약 통계

Fig. 11은 조직 구성원들의 프로파일링 자료를 바탕으로 취합한 부서 및 기관별 직무 또는 KSA 분포에 대하여 요약하여 출력하는 기능이다. 상단에서 요약 정보를 보고 싶은 기관/부서를 선택하면 해당 기관의 직무의 분포 또는 배치 현황과 기관/부서 단위로 보유하고 있는 KSA를 출력한다.

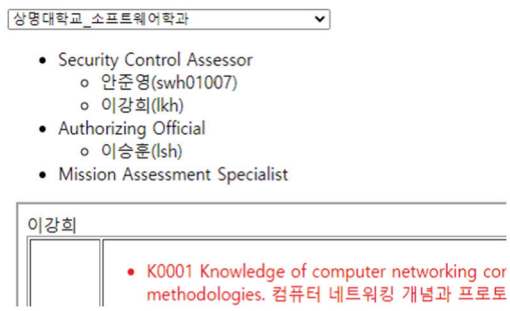


**Fig. 11.** Statistics screen for each organization in the profiling system.

## 4. Conclusions

본 연구에서는 미국(NICE), 영국(CIISec)의 사이버 보안 업무 체계 관련 선행 연구를 포함해 국내·외에서 진행되고 있는 사이버 보안 인력 양성, 직무체계 분류 및 기반 지식에 대해 어떤 식으로 정의를 내리고 있는지 조사했다. 두 국가 (미국, 영국) 모두 과거부터 체계적인 보안 인력 관리에 대한 필요성을 인지하고 오랜 기간 연구를 진행해온 만큼 사이버 보안 인력양성을 위한 프레임워크 연구가 상당히 진행되어 실제로 활용되고 있는 것(iQ4, Career Framework)을 확인할 수 있었다. 국내의 경우, 산업의 전반적인 부분에서 직무를 정의하긴 했으나, 사이버 보안 분야에 집중한 연구는 아니기에 국가 단위에서 사이버 보안 인력양성을 위한 연구와 국내 실정에 맞는 업문 분장의 정의가 필요하다고 볼 수 있다. 그러하기에, 본 연구에서는 미국의 NICE Framework를기반으로 사이버 보안 전문가를 프로파일하는 시스템 구조를 설계하고 프로토타입을 제작해봤다. 이러한 연구·조사 결과들을 통해, 이 연구가 향후 국내 사이버 보안 전문가 관리·양성 체계 및 시스템 개발을 위한 기초 제언 자료로 활용될 수 있을 것으로 기대된다.

## 참고문헌

1. Ponemon Institute LLC, "2018 Cost of Data Breach Study: Impact of Business Continuity Management", IBM, 2018.
2. T.S. Kim, H.S. Jeon, Y.B. Kim, T.Y. Kim, S.H. Lee, "Prior research for development of national cyber security manpower management system", The Korea Society of Management Information Systems, 2020.
3. William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", National Institute of Standards and Technology, USA, 2017.
4. CIISec, "CIISec Skills Framework V2.4", Chartered Institute of Information Security, UK, 2019.
5. CIISec, "IISP Knowledge Framework V1.1.1", Chartered Institute of Information Security, UK, 2019.
6. CIISec, "CIISec Roles Framework V0.3", Chartered Institute of Information Security, UK, 2019.
7. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, and Andrew Martin, "The Cyber Security Body of Knowledge V1.0", CyBOK, 2019.
8. Ministry of Employment and Labor, Human Resources Development Service of Korea, "2020 National Competency Standards (NCS) Development and Improvement Manual", 2020.

접수일: 2021년 8월 27일, 심사일: 2021년 9월 13일, 게재확정일: 2021년 9월 16일