Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.5, Oct. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.973

공공부문의 사이버보안 교육격차 해소를 위한 탐색적 연구*

이 송 하,[1†] 전 효 정,[2] 김 태 성[3‡]
[1,3]충북대학교 (대학원생, 교수), [2]충북대학교 보안경제연구소 (박사후 연구원)

Are There Any Solutions for the Cybersecurity Education Gap in the Public Sector?*

Song-ha Lee,[1†] Hyo-Jung Jun,[2] Tae-Sung Kim[3‡]
[1,3]Chungbuk National University (Graduate student, Professor),
[2]Cybersecurity Economics Research Institute (Postdoctoral researcher)

요 약

우리나라는 명실상부한 전자정부 강국으로서 오랜 기간의 경험과 잘 구축된 정보통신 인프라를 기반으로 일찌감치 행정업무의 효율성과 국민의 편의성은 확보했지만, 그만큼 크고 작은 사이버 공격에 항시 노출되어 있다. 행정 및 공공부문의 사이버보안 대응력 및 회복력 확보는 국가경쟁력의 중요한 요소이며, 이를 위해 잘 훈련된 사이버보안 전문인력을 확보하고 재교육을 통해 계속해서 역량개발을 지원해야 한다. 하지만 국가균형발전사업으로 기관과 인력이 지방으로 이전하였음에도 교육시설의 이전이나 확장은 이루어지지 않아, 오히려 재교육을 통한 역량개발의 기회는 박탈되고 있는 것은 아닐지에 대한 논의가 필요한 시점이다. 본 연구는 공공부문 사이버보안 교육기회나 요구사항에 있어 지역, 기관, 인력의 특성에 따라 격차가 있는지 실증하고자 한다. 더불어 실증 결과를 바탕으로 공공부문 사이버보안 인력의 교육격차 해소방안을 제안하고자 한다.

ABSTRACT

South Korea has been guaranteed the efficiency and the convenience of administrative work based on long-term experience and well-established ICT infrastructure. Vice versa, South Korea is always exposed to various scale cyber-attacks. It is an important element of national competitiveness to secure cybersecurity resilience and response in the public sector. For this, the well-trained cybersecurity professionals' retention and support for their capacity development through retraining are critical. As the Special Act on Balanced National Development, most public agencies moved to provincial areas, but the provincial areas are not ready for this, thus the workforce can't get enough retaining courses. We study to analyze whether there is a gap in cybersecurity educational opportunities or needs in the public sector depending on regions, institution type, and personal traits. This paper aims to suggest solutions for the cybersecurity education gap in the public sector based on the empirical analysis results.

Keywords: Cybersecurity, Cybersecurity Training, Education Gap, Special Act on Balanced National Development, Relocation Public Agencies

Received(08. 19. 2021), Modified(09. 09. 2021), Accepted(09. 10. 2021)
* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2018S1A5A2A01039356)
† 주저자, lsh914@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

I. 서 론

전자정부의 추진으로 공공부문의 업무가 대부분 디지털화되면서 행정능률과 국민의 편의성이 눈에 띄게 향상되고 있다. 그러나, 역설적으로 전자정부가 일상생활에 자리 잡을수록 신기술(IoT, AI, Cloud-Computing 등)의 확산에 따른 새로운 보안위협에 대한 대응이 어려워져 전자정부의 신뢰도가 위기에 직면하고 있다. 실제로 국가의 전자정부 운영 수준과 관계없이 전자정부 사이트는 보안에 취약한 것으로 연구된 바 있다. 전자정부 서비스 수준이 높은 호주와 상대적으로 낮은 태국의 전자정부 사이트를 비교한 결과, 두 나라 모두 아주 기본적인 보안 조치조차 지켜지지 않고 있었으며, 두 나라의 전자정부 사이트가 가진 취약점의 수준이 유사한 것으로 도출되어, 강력한 사이버보안 대책 마련이 필요한 것으로 나타났다[1]. 국제연합(United Nations, UN)은 2018년부터 UN전자정부평가에 국제전기통신연합(International Telecommunication Union, ITU)의 사이버보안지수(Global Cybersecurity Index, GCI)를 새로운 평가항목으로 추가하기도 하였다[2].

국가의 사이버보안을 강화하는 방안 중 하나는 '숙련된 사이버보안 인력'의 확보이다. 국제전기통신연합은 사이버보안지수 산정에 법, 기술, 조직, 역량, 협력 등 5가지 영역을 활용한다. 이 중 역량 영역의 세부지표에 사이버보안 전문가에 대한 인증체계, 사이버보안 전문가 교육과정, 사이버보안 학위과정 또는 교육프로그램, 인센티브 체계 등을 포함하고 있어 '사이버보안 인력의 교육·양성·관리'의 중요성을 시사하고 있다[3]〈Table 1.〉.

미국의 회계감사원(Government Accountability Office, GAO)[1]도 국가가 직면한 사이버위협을 완화하고 적절하게 대응하기 위한 핵심 방안으로 공공부문의 숙련된 사이버보안 인력의 확보를 꼽았다. 더불어 사이버보안 관련 업무를 수행하는 재직자들의 기술격차(skills gaps)를 해소하는 것도 중요하다고 지적하였다. 이를 위해 유능한 인재의 신규채용뿐만 아니라 재직자들이 지속적인 재교육을 통해 사이버보안 관련 기술을 유지·개발할 수 있도록 도울 것을 권고하였다[4].

Table 1. Global Cybersecurity Index(GCI) Indicators

Category	Indicators
Legal	• Cybercrime legislation • Cybersecurity regulation • Containment/curbing of spam legislation
Technical	• CERT/CIRT/CSIRT • Standards implementation framework • Standardization body • Technical mechanisms and capabilities deployed to address spam • Use of cloud for cybersecurity purpose • Child online protection mechanisms
Organi-zation	• National cyber security strategy • Responsible agency • Cybersecurity metrics
Capacity Building	• Public awareness campaigns • Framework for the certification of cybersecurity professionals • Professional programs or academic curricular in cybersecurity • Cybersecurity R&D programs • Incentive mechanisms
Cooper-ation	• Bilateral agreements • Multilateral agreements • Participation in international fora/association • Public-private partnerships • Best practices

※ ITU, Global Cybersecurity Index(GCI), 2018 [3]

한국은 전자정부 수출국이자 명실상부한 정보통신 강국이다. 세계경제포럼(World Economic Forum, WEF)의 ICT보급 역량 조사에서 2018년과 2019년 연속으로 1위를 차지할 정도로 정보통신 인프라가 잘 구축되어 있다[5][6]. 또한, 2010년부터 지금까지 국제연합의 전자정부발전지수에서 꾸준히 3위 이내의 순위를 차지할 정도로 전자정부를 안정적으로 추진하고 있다[7]. 하지만 높은 정보통신기술 활용도에도 불구하고 국내 공공부문의 사이버보안 수준은 기대에 부응하지 못하고 있는 것으로 평가된다. 그 원인 중 하나로 감사원[8]은 2016년 국가 사이버안전 관리 실태 감사보고서를 통해 사이버보안 관련 이력이 없는 인력이 내부재배치를 통해 업무를 맡고 있다는 점을 들어 사이버보안 담당인력의 전문성이 낮다고 지적한 바 있다. 2021년 정보보호백서에 따르면 공공부문 127개의 기관 중 사이버보안 담당 인력이 관련 공인 자격증을 소지하고 있는 기관은 약 44%, 관련 석사 이상의 학위를 소지한 인력을 보유

1) GAO는 의회가 정보에 입각한 의사결정을 할 수 있도록 의사결정 주제와 관련된 보고서, 분석, 권고 등을 제공하는 것을 기관 운영의 주요 목표로 함(GAO, 2018)

한 기관은 약 27%에 불과해 수준 높은 인력이 부족한 것으로 나타났다[9].

공공부문 사이버보안 인력의 재교육도 어려운 실정이다. 그 이유로 첫째, 우리나라는 국가균형발전특별법(법률 제7061호, 2004.1.16. 제정)을 마련하여 수도권[2]에 위치한 공공기관이 지방 이전을 추진하였으며, 2019년 153개 기관이 지방 이전을 완료하였다[10]. 공공기관은 이전한 지역의 인재를 채용하고, 재직자들도 이전한 지역 내에서 교육을 받고자 할 것이기에 지방에서 사이버보안과 같은 전문기술교육 수요가 증가하는 것이 당연하다[11]. 그러나, 여전히 사이버보안 관련 교육과정은 일부 지역(수도권, 대전 등)에 밀집되어 있어 지방 재직자들의 접근이 어렵다[12]. 또한, 공공부문 사이버보안 인력이 필요로 하는 실질적인 교육이 부족한 실정이다. 공공부문 재직자 대상의 교육은 형식적으로 운영되어 직무수행능력을 향상시키지 못한다는 지적이 있다[13]. 더불어 공공부문 사이버보안 인력의 업무 범위가 명확하게 정의되지 않은 상태이며, 직무에 적합한 경력개발과 인력관리를 위한 기준도 없어 재교육으로 사이버보안 인력의 수준을 높이기도 어려운 상황으로 관련된 연구가 필요하다는 지적이 있다[14].

공공부문의 정보보호 전문성 강화를 위해서는 전문적인 교육과정 운영역량이 있는 지방 소재의 공공·민간 교육기관에서 지방의 공공부문 재직자들이 실무에 필요한 교육을 받을 수 있도록 연계하는 방안의 마련이 필요하다[12]. 한편으로는 지역 간 교육기회의 차이를 공공부문의 재직자들이 실감하고 있는지, 지역 간의 사이버보안 전문성 차이가 교육격차 때문에 발생하는 것인지, 인력의 근본적인 실력 차이에서 비롯된 것인지에 대해 실증연구가 이루어진 사례는 없다.

본 연구에서는 교육격차 실증을 위해 세 가지의 연구문제를 제안하고 분석한다. 먼저, 지역 간 교육격차 실증을 위해, 지방 소재의 공공부문에서 근무하는 사이버보안 담당자들이 실제로 해당 지역에 교육기회가 부족하다고 인식하는지, 지역에 따라 교육 요구사항에 차이가 있는지 확인한다(연구문제 1).

연구문제 1: 근무지에 따라 교육기회와 교육요구사항에 대한 차이가 있는가?

2) 수도권은 서울특별시, 인천광역시, 경기도를 말함(수도권정비계획법 제2조제1호(시행 2020. 6. 11.) 및 수도권정비계획법 시행령 제2조(시행 2020. 3. 24.) 참고)

우리나라는 인구의 절반이 수도권에 살고 있으며, 자본과 교육, 문화가 수도권에 집중되어 있다. 이에 자연스럽게 수도권에서 더욱 양질의 교육이 이루어질 것이라고 기대한다. 더불어 KTX 등의 발달로 전국이 반나절 생활권 시대에 들면서 수도권으로의 접근이 어렵지 않다. 따라서, 사이버보안 교육이 비수도권인 근무지 내에서 운영될 경우, 실제 참여 의사에 대해서도 실증해보고자 한다(연구문제 2).

연구문제 2: 근무지 내 또는 인접 지역에서 교육이 운영될 경우 참여 의사가 있는가? 교육공급이 부족한 지역이라고 느낄수록 근무지 내 교육 참여 의사가 더욱 높을 것인가?

교육격차가 인력의 특성(전공, 직무, 직급, 재직중인 기관의 분류)에서도 비롯되는지 확인하고, 인력의 특성에 따라 교육 요구사항에 대한 차이가 있는지 확인하고자 한다(연구문제 3).

연구문제 3: 인력의 특성에 따라 교육기회와 교육 요구사항에 대한 차이가 있는가?

본 연구는 세 가지 연구문제를 중심으로 공공부문의 사이버보안 교육격차를 실증하고, 교육격차 해소를 위한 방안을 제안하여, 재교육을 통해 공공부문 사이버보안 인력의 전문성을 높이는데 기여하고자 한다.

II. 문헌고찰

2.1 공공부문 재직자 대상의 사이버보안 교육

빠른 기술변화로 사이버보안 인력은 졸업과 동시에 구식이 된 지식을 가지고 현장에 뛰어들 수밖에 없어, 사이버보안 인력은 지속해서 최신 기술을 학습하고 문제를 해결하려는 의지를 지녀야 한다[15]. 사이버보안과 관련된 전공을 졸업했더라도, 대학에서 배운 내용과 실무 사이에 격차가 발생하기 마련이며, 이러한 격차의 해소는 사이버보안 인력 부족 문제해결의 핵심이다[16][17]. 교육은 인력의 업무 수준을 강화하며 경력개발에 긍정적인 영향을 미치는 중요한 요인이다. 특히, IT 전문가들은 타 직업군에 비해 높은 자기 성장 욕구를 지니고 있으며, 자주 바뀌는 트렌드를 따라잡지 못하거나 새로운 기술을 배우는 것에 대한 걱정이 큰 것으로 알려져 있다[18].

최근 국가 및 공공기관을 대상으로 하는 해킹 공격의 수가 점점 증가하는 추세로 국내 공공부문 종사

자를 대상으로 하는 국가 주도의 사이버보안 교육이 증가하고 있다[19]. 공공부문 재직자의 능력을 제고시키는 방안 중 하나는 재직자를 대상으로 하는 교육의 실효성을 높이는 것이다[20]. 특히, 우리나라의 공공부문 종사자는 타 직무로의 전환 혹은 민간 분야로 이직하는 경우가 적어 재직자를 대상의 교육·훈련이 매우 중요하며, 그 효과가 크다[21][22]. 그러나, 공공부문 재교육은 중요성에 비해 다소 형식적으로 운영되고 있는 것으로 지적받고 있다[13][23][24].

공공부문 재직자 대상의 사이버보안 재교육의 실효성을 높이기 위해 인력의 특성에 따라 차별화되고, 조직의 목표와 인력의 요구사항을 충족하는 교육이 중요한 시점이다[25][26].

2.2 지역 인적자원 개발

인적자원은 조직의 기능수행과 목표달성을 위한 전략적 자본이다. 공공부문의 인적자원 관리는 국가의 경쟁력과 직결되기 때문에 매우 중요하다. 지역 차원의 인적자원개발이란 지방자치단체 주도로 지역사회의 모든 가용할 수 있는 학습자원을 활용하여 지역의 인적자본과 사회자본을 형성하는 활동을 의미한다. 지역 인적자원개발의 효용성을 극대화하기 위해서는 지역 노동시장의 인적자원 수요가 충실히 반영되어야 한다[27].

공공기관의 지방 이전이 지역 인적자원 개발에 미치는 영향으로는 지역에서 양성된 인력 수요의 증가, 그에 따른 대학의 교육과정 변화, 지역 내 신규 직업능력 개발 수요 발생 등이 있다[11]. 특히, 공공기관의 지방 이전이 인적자원 개발에 긍정적인 영향을 미치기 위해서는 지방정부 간 협력적 네트워크를 구축하고 지역 대학 간 전문 인력양성을 위한 협력체계를 마련하는 것이 중요하다. 더불어 이전 공공기관은 지역발전과 인력개발을 위한 지역혁신체계의 핵심주체가 되어야 한다. 장기적으로는 공공기관 지방 이전에 따라 요구되는 노동력에 대응하기 위해 지역에서 자체적으로 수요 기반의 인적자원을 개발할 수 있어야 한다[11].

같은 지방공무원이더라도 광역지자체 소속 공무원이 기초지자체 소속 공무원보다 역량이 높고, 중간관리자급의 역량이 전반적으로 부족한 것으로 조사된 바 있다[22]. 지방 공공부문의 역량 강화를 위해서는 교육 거버넌스 체계의 구축, 교육과 인사과정과의 연계, 지역의 교육 니즈에 부합하는 교육과정의 개발, 각 개인에 대한 역량진단 결과를 바탕으로 하는 맞춤형 교육 등이 필요하다[22].

국가균형발전사업으로 정부·공공기관과 인력이 지방으로 이전하였음에도 교육시설의 이전이나 확장은 이루어지지 않고 있다. 단기적으로는 지방 이전 인력들의 교육수요가 증가하고 장기적으로는 지방으로 이전한 기관에서 지역 내의 인재를 채용하고자 할 것으로 지방에서도 전문적인 사이버보안 교육을 충분히 받을 수 있는 기반이 필요하다. 국가균형발전에 적합한 인적자원 개발을 위해서는 지역과 인력의 특성에 따른 교육 요구사항 분석이 필수적이다.

III. 자료조사 및 분석

분석에 사용한 데이터는 오프라인 설문조사로 수집하였다. 조사대상은 대전광역시, 세종특별자치시, 충청남도, 충청북도 국가·공공기관 정보보호 또는 정보화 담당자 대상의 교육·훈련(2020.6.), 충청북도 사이버보안협의회(2020.10.), 충청권 공공기관 사이버보안협의회(2020.11.), 공공분야정보보호교육센터 교육·훈련(2020. 하반기) 등의 참석자이다.

총 227부를 회수하였으며, 응답 수가 30부 미만인 지자체의 경우 분석대상에서 제외하였다. 최종 분석에는 198부를 활용하였다.

3.1 응답자의 기초통계

응답자의 재직기관은 기타공공기관(28.8%), 지방행정기관(17.2%), 준정부기관(15.7%), 공기업(14.6%), 중앙행정기관(9.1%), 교육청 및 산하기관(8.1%), 군(6.6%) 순이다〈Table 2.〉.

응답자의 근무지는 충청도(충청북도와 충청남도)가 가장 많았으며, 다음으로는 대전광역시, 세종특별자치시, 수도권(서울특별시, 경기도, 인천광역시) 등

Table 2. Current Affiliation

Type of Affiliation	Freq.	Ratio
Other Public Institutions	57	28.8
Local Administrative Agency	34	17.2
Quasi-Governmental Departments	31	15.7
Public Enterprises	29	14.6
Central Administrative Agency	18	9.1
Organization of the Educational Administration	16	8.1
Military	13	6.6
Total	198	100

Table 3. Place of Work

Place of Work	Freq.	Ratio
Seoul Metropolitan Area (Metropolitan)*	33	16.7
Daejeon Metropolitan City (Daejeon)	58	29.3
Sejong City (Sejong)	43	21.7
Chungcheong-do† (Chungcheong)	64	32.3
Total	198	100

* Seoul Metropolitan Area means the Seoul Special Metropolitan City, Incheon Metropolitan City, and Gyeonggi-do.
† Chungcheong-do means Chungcheongnam-do and Chungcheongbuk-do

의 순이다〈Table 3.〉.

응답자의 약 70%는 실무자급이다. 전체 경력이 10년 이상인 경우가 54.5%에 달하지만, 정보보호 경력은 3년 이하인 경우가 47.5%이다〈Table 4.〉.

정보보호 경력이 있는 응답자의 70% 이상이 정보보호 외의 업무 경력이 있으며, 대부분은 정보보호 경력보다 정보보호 이외의 경력이 더 많다고 응답하였다. 정보보호 업무로 경력을 시작하여 정보보호 업무만 수행한 응답자는 24.7% 수준이다. 설문대상에 정보화 담당자도 속해있기 때문에 정보보호 경력이 없는 응답자(4.5%)도 있다〈Table 4.〉. 전체 경력과 정보보호 경력 간의 Pearson 상관분석을 실시한 결과 전체 경력과 정보보호 경력 간에는 낮은 정(+)의 상관관계를 보인다($r=0.394$, $p=0.000$)[3].

Table 4. Current Position and Career

Position/Career		Freq.	Ratio
Current Position	Staff	140	70.8
	Manager	29	14.6
	General Manager	27	13.6
	Executives	1	0.5
	No response	1	0.5
	Sub Total	198	100
Whole Career Year	Under 1 Year	14	7.1
	1~3 Years	21	10.6
	3~5 Years	16	8.1
	5~10 Years	39	19.7
	Over 10 Years	108	54.5
	Sub Total	198	100
Cyber-security Career Year	Under 1 Year	41	20.7
	1~3 Years	53	26.8
	3~5 Years	36	18.2
	5~10 Years	31	15.7
	Over 10 Years	28	14.1
	None	9	4.5
	Sub Total	198	100
Career Charac-teristic	Cybersecurity Career Only	49	24.7
	Cybersecurity Career 〉 the other Career	2	1.0
	Cybersecurity Career 〈 the other Career	138	69.7
	Non-Cybersecurity Career	9	4.5
	Sub Total	198	100

응답자들의 전공은 정보·통신공학 전공자가 가장 많고(36.9%), 정보보호와 전산·컴퓨터 공학(각각 16.7%), 기타(29.8%) 순이다〈Table 5.〉. 전공 구분은 대학알리미의 표준분류체계 소분류[28]를 활용하였다. 단, 표준분류체계에는 정보보호 전공이 소분류 수준에서 드러나지 않지만 본 연구의 대상이 정보보호 인력이기 때문에 정보보호 전공을 구분하였다.

응답자의 현재 직무는 정보보호 업무총괄, 정보보호 정책, 개인정보보호 등을 다루는 '정보보안 관리'가 가장 많다(42.7%). 네트워크 보안, 보안취약점 관리, 시스템 보안, 전산보안, 홈페이지 보안 등을 수행하는 '네트워크 및 전산보안(35.2%)', 보안관제, 사이버 침해대응 등의 업무를 수행하는 '보호 및 대응(15.9%)', '정보통신(6.2%)' 순이다〈Table 6.〉. 정보보호 직무의 분류에는 전효정 등[14]의 분류를 활용하였다.

Table 5. Major

Major	Freq.	Ratio
Computer Science	33	16.7
Information and Computer Engineering	73	36.9
Cybersecurity	33	16.7
Etc.	59	29.8
Total	198	100

Table 6. Current Job Duty (Allowing Multiple Responses)

Job Duty	Freq.	Ratio
Cybersecurity Management	97	42.7
Network and Computer Security	80	35.2
Protect and Defend	36	15.9
IT	14	6.2
Total	227	100

3.2 문항별 기초통계분석

응답자들은 '교육내용의 업무 활용(32.7%)'과 '보안인식 제고(27.2%)'를 주요 수강목적으로 응답하였다. 교육 의무시간 이수를 목적으로 하는 응답도

3) 상관관계 계수 값이 ±0.2 이상 ±0.4 미만일 경우 낮은 상관관계로 정의함[29]

Table 7. Purpose of Retraining (Allowing Multiple Responses)

Purpose of Retraining	Freq.	Ratio
Increasing cybersecurity awareness	80	27.2
Improving cybersecurity technology capabilities	53	18.0
Utilizing retraining contents at work	96	32.7
Completing of compulsory training hours	30	10.2
Getting a promotion	28	9.5
Formatting human networks	2	0.7
Etc.	5	1.7
Total	294	100

10.2% 수준이다〈Table 7.〉.

실무자와 실무자 외로 직급을 구분하였을 때, 두 그룹 모두 교육·훈련 또는 협의회 참석 목적을 '교육 내용의 업무 활용'과 '보안인식 제고'에 두고 있다. 다만, 실무자급에서는 '보안기술능력 향상' 또한 주요 수강목적으로 응답하여, 보안기술능력과 관련된 교육 수요가 있는 것으로 나타났다〈Table 8.〉.

교육기회와 교육요구사항을 확인하기 위한 문항의 평균점수를 확인하였다〈Table 9.〉.

'나의 근무지는 정보보호 교육프로그램 참여기회가 적은 지역이다(이하 V1)'는 보통 수준(평균 3.1점)이지만, 타 항목들에 비해 가장 표준편차가 크다. '나의 근무지와 인접한 지역에서 정보보호 교육프로그램이 운영되면 더욱 자주 교육에 참여할 것이다(이하 V2)'는 높음 수준(평균 4.3점)으로 타 항목들에 비해 표준편차가 가장 작다. '정보보호 교육프로그램이

Table 8. Purpose of Retraining by Current Position (Allowing Multiple Responses)

Purpose of Retraining	Staff		The Others	
	Freq.	Ratio	Freq.	Ratio
Increasing cybersecurity awareness	58	27.6	22	26.8
Improving cybersecurity technology capabilities	45	21.4	8	9.8
Utilizing retraining contents at work	69	32.9	26	31.7
Completing of compulsory training hours	19	9.0	11	13.4
Getting a promotion	13	6.2	15	18.3
Formatting human networks	1	0.5	-	-
Etc.	5	2.4	-	-
Total	210	100	82	100

* Excluding response of 1 respondent who did not respond on current position

Table 9. Educational Opportunities and Needs in Workplace

Questionnaire Variables (5-Point Likert Scale)		Mean	SD
V1	My workplace has few cyber-security education opportunities.	3.1	1.213
V2	If cybersecurity education programs are provided close to my workplace, I will participate more frequently.	4.3	0.805
V3	If cybersecurity education program is linked to a graduate course, I am willing to go on.	3.7	1.063
V4	I am willing to pay for dormitory during cybersecurity program.	3.5	1.121
V5	I wish cybersecurity education program is additionally provided online (Live lectures, VOD, etc.).	3.8	1.109
V6	I prefer hands-on education.	4.0	0.961

학위과정(석·박사)과 연계된다면 진학의사가 있다(이하 V3)'는 보통보다 약간 높은 수준(평균 3.7점)이다. '정보보호 교육프로그램 기간 동안 유료로 사용할 수 있는 기숙사가 있으면 이용하겠다(이하 V4)'는 보통 수준(평균 3.5점)이다. '정보보호 교육프로그램이 온라인(Live 강의, VOD 등)으로도 운영되면 좋겠다(이하 V5)'는 보통보다 약간 높은 수준(평균 3.7점)이다. '나는 실습 위주의 강의를 선호한다(이하 V6)'는 높음 수준(평균 4.0점)이다.

응답자들은 1회당 평균 3.3일(표준편차 1.619) 또는 평균 20시간(표준편차 12.645)의 교육 프로그램을 선호한다. 교육프로그램 참석 시 가장 선호하는 교통수단은 자동차(59.7%), 기차(14.4%), 버스(12.2%), 지하철(7.7%), 대중교통이면 상관없음(6.1%) 순이다. 수도권에서는 자가용(14%)보다 지하철(29%)을 선호하였으나, 수도권을 제외한 지역에서는 자가용에 대한 선호도가 두드러졌다. 교육프로그램 참석을 위해 감내할 수 있는 이동시간은 평균 1.54시간(표준편차 0.723), 최빈값은 1시간으로 주로 1시간~1시간 30분 내외의 이동을 선호한다.

3.3 연구문제 분석

연구문제를 해결하기 위해 통계모형을 활용하여 데이터의 심층분석을 실시하였다. 분석에는 IBM SPSS Statistics 26을 활용하였다.

연구문제 1: 근무지에 따라 교육기회와 교육요구사항에 대한 차이가 있는가?

응답자의 근무지를 수도권(서울특별시, 인천광역시, 경기도)과 비수도권(대전광역시, 세종특별자치시, 충청남도, 충청북도)의 두 집단으로 구분하고 근무지 내의 정보보호 교육기회 및 교육 관련 요구사항에 대한 차이를 t-test로 검증하였다.

교육기회에 있어 수도권(M=2.6, SD=1.475)의 재직자보다 비수도권(M=3.2, SD=1.132)의 재직자가 근무지 내 교육기회가 적다고 인식하고 있으며, 통계적으로 유의미한 것을 확인하였다(V1; t=-2.659, p=.008). 그러나, 교육 요구사항에 있어서는 통계적으로 유의미한 차이를 확인하지 못하였다(V3, V4, V5)〈Table 10.〉. 비수도권 내에서의 근무지 내의 교육기회에 대한 인식 차이를 확인하기 위해 일원배치 분산분석(one-way ANOVA)을 실시하였으나, 통계적으로 유의미한 차이가 없었다(F=2.133, p=.122)〈Table 11.〉.

연구문제 2: 근무지 내 또는 인접 지역에서 교육이 운영될 경우 참여 의사가 있는가? 교육공급이 부족한 지역이라고 느낄수록 근무지 내 교육 참여 의사가 더욱 높을 것인가?

근무지 내에서 정보보호 교육 프로그램이 운영 될 경우 참여하겠다는 응답은 높음 수준(평균 4.3점)이다〈Table 9.〉. 근무지 내에서 운영되는 정보보호 교육에 대한 참여 지역별 의사를 비교하기 위해 t-test 검증 결과, 수도권(M=4.5, SD=.712)과 비수도권(M=4.3, SD=.820) 간에 유의미한 차이를 확인하지 못하였다(V2)〈Table 10.〉.

Table 10. Difference in Cybersecurity Educational Opportunities and Needs by Workplace (t-test)

Variable		Mean	SD	t-value	p-value
V1	Metropolitan	2.6	1.475	-2.659	.008**
	Non-Metropolitan	3.2	1.132		
V2	Metropolitan	4.5	0.712	1.414	.156
	Non-Metropolitan	4.3	0.820		
V3	Metropolitan	3.8	1.103	.507	.613
	Non-Metropolitan	3.7	1.058		
V4	Metropolitan	3.5	1.228	.000	1.000
	Non-Metropolitan	3.5	1.102		
V5	Metropolitan	3.8	1.149	.400	.689
	Non-Metropolitan	3.8	1.104		
V6	Metropolitan	4.1	1.023	.992	.322
	Non-Metropolitan	3.9	0.948		

**p〈.01

Table 11. Difference in Cybersecurity Educational Opportunities by Workplace (one-way ANOVA)

Variable		Mean	SD	F/p
V1	Daejeon[b]	3.0	1.092	2.133/.122
	Sejong[c]	3.2	1.283	
	Chungcheong[d]	3.5	1.038	

*p〈.05

근무지 내 교육기회에 대해 느끼는 정도(V1)와 근무지 내 교육 참여의지(V2) 간에는 상관관계가 없는 것으로 나타났다. 이를 통해 현재 교육기회가 적다고 인식한다고 해서 근무지 인접 지역의 교육훈련 참여 의지가 높아지는 것은 아님을 확인하였다〈Table 12.〉. 이를 통해 응답자들은 근무지 내의 교육훈련 기회가 적다고 생각하고 근무지 인접 지역에서 교육훈련이 있으면 좋겠다는 생각은 있지만, 현재 이수 중인 교육시간을 초과하여 교육프로그램에 참여할 의지는 없는 것으로 보인다.

Table 12. Correlation between Educational Opportunities and Willingness to Participate in Education

Variable	Mean	SD	Correlation	
			1	2
V1	3.1	1.213	1	0.091
V2	4.3	0.806	0.091	1

연구문제 3: 인력의 특성에 따라 교육기회와 교육 요구사항에 대한 차이가 있는가?

인력의 특성인 전공, 직급, 직무, 기관분류[4]에 따라 교육기회에 대한 인식과 교육 요구사항에 대한 차이를 확인하고자 t-test 및 one-way ANOVA를 수행하였으나, 유의미한 차이를 확인하지 못하였다〈Table 13, 14, 15, 16〉.

4) 군(軍)은 표본이 30개 미만이고, 일반적인 기관과 운영 목적이 다르기 때문에 제외. 교육청 및 산하기관은 '지방교육행정기관(지방교육행정기관의 행정기구와 정원기준 등에 관한 규정)'으로 행정기관의 성격을 지닌 것으로 판단하여 행정기관으로 분류함. 「공공기관의 운영에 관한 법률」 제5조에 따라 공기업, 준정부기관, 기타공공기관을 공공기관으로 구분함

Table 13. Difference in Cybersecurity Educational Opportunities and Needs by Affiliation (one-way ANOVA)

Variable		M	SD	t-value	p-value
V1	Administrative Agencies	3.3	1.120	1.234	.219
	Public Institutions	3.1	1.244		
V2	Administrative Agencies	4.3	0.765	-0.485	.628
	Public Institutions	4.3	0.839		
V6	Administrative Agencies	3.9	1.006	-0.840	.402
	Public Institutions	4.0	0.942		

Table 14. Difference in Cybersecurity Educational Opportunities by Major (one-way ANOVA)

Variable		Mean	SD	F/p
V1	Cybersecurity	3.3	1.237	.971/ 0.179
	Computer Science	3.3	1.302	
	Information and Computer Engineering	3.1	1.144	
	Etc.	2.9	1.121	
V2	Cybersecurity	4.1	0.960	1.204/ .408
	Computer Science	4.4	0.810	
	Information and Computer Engineering	4.2	0.808	
	Etc.	4.4	0.692	
V6	Cybersecurity	3.8	0.983	.914/ .309
	Computer Science	4.2	0.986	
	Information and Computer Engineering	3.9	0.947	
	Etc.	3.8	0.906	

Table 15. Difference in Cybersecurity Educational Opportunities and Needs by Job Duty (one-way ANOVA)

Variable		Mean	SD	F/p
V1	Cybersecurity Management	3.2	1.255	.115/ .952
	Network and Computer Security	3.0	1.091	
	Protect and Defend	3.3	1.256	
	IT	3.0	1.569	
V2	Cybersecurity Management	4.4	0.819	.746/ .526
	Network and Computer Security	4.3	0.736	
	Protect and Defend	4.3	0.882	
	IT	4.5	0.650	
V6	Cybersecurity Management	3.9	0.972	.352/ .788
	Network and Computer Security	4.0	0.878	
	Protection and Response	4.1	1.170	
	IT	4.0	0.877	

※Multiple Responses are allowed on job duty.

Table 16. Difference in Cybersecurity Educational Opportunities and Needs by Current Position (t-test)

Variable		Mean	SD	t-value	p-value
V1	Staff	3.1	1.210	-.451	.653
	the others	3.2	1.217		
V2	Staff	4.3	0.811	.014	.989
	the others	4.3	0.801		
V6	Staff	4.0	0.955	1.639	.103
	the others	3.8	0.959		

Table 17. Field of Retraining desired by Respondents (Allowing Multiple Responses)

Field of Retraining		Freq.	Ratio
1	Penetration testing practice	29	12.8
2	Cloud-Computing practice	26	11.5
3	Laws, institutions, guidelines, regulations	22	9.7
4	Information security management assessment	22	9.7
5	Security conformity verification	19	8.4
6	Digital forensics theory&practice	18	8.0
7	Cybersecurity project management	11	4.9
8	Security monitoring practice	10	4.4
9	Computer Emergency Response	9	4.0
10	Cybersecurity Technology Trend	8	3.5
11	Network security	5	2.2
12	System security	5	2.2
13	Secure SW development management	4	1.8
14	Cybersecurity Management (including audit, policy, etc.)	4	1.8
15	IOT security (including policy)	3	1.3
16	Virtualization	3	1.3
17	Privacy	3	1.3
18	Cybersecurity practice	3	1.3
19	Network separation	2	0.9
20	Blockchain practice	2	0.9
21	Malware analysis	2	0.9
22	Visit to related institutions	2	0.9
23	ISMS	2	0.9
24	Guidelines for the establishment and operation of information systems	2	0.9
25	Vulnerability Analysis	2	0.9
26	Training for CCE	1	0.4
27	DB vulnerability guide	1	0.4
28	Wiretapping	1	0.4
29	Deep learning	1	0.4
30	The way to create and teach the lectures for cybersecurity education	1	0.4
31	Manual production for affiliate management	1	0.4
32	ICT policy related to cybersecurity	1	0.4
33	Operation of cybersecurity equipment	1	0.4
Total		226	100

응답자들이 다수 희망하는 재교육 분야는 모의해킹 실무, 클라우드 컴퓨팅 실무, 정보보호 관련 법·제도·가이드라인·규정 등이다〈Table 17.〉.

IV. 결 론

4.1 결론 및 시사점

한국은 전자정부 활용도가 높은 국가인 만큼 크고 작은 사이버위협에 항시 노출되어 있다. 공공부문의 정보보호 대응력 및 회복력 확보는 국가경쟁력과 직결된다. 그 중심에는 '숙련된 정보보호 전문인력'이 있다. 전문인력의 확보에는 신규 채용 못지않게 재교육을 통해 지속적인 역량개발을 지원하는 것이 중요하다. 본 연구는 지방분권과 공공기관 지방 이전이 강조되고 있지만, 여전히 정보보호 교육기회는 수도권에 집중되어 있어 근무 지역에 따라 교육격차가 차이가 있음을 실증하고자 하였다. 더불어 인력의 특성에 따른 교육격차가 있는지도 확인하고자 하였다.

기존의 연구들에서는 지역별 교육기관 수를 통해 근무지 간 교육기회의 차이가 있음을 가늠하는 수준에서 결론을 지었다. 본 연구는 실제 데이터를 가지고 공공부문 정보보호 인력이 근무지에 따른 교육기회의 차이를 체감하고 있음을 실증하였다는 점에서 의의가 있다.

또한, 교육격차 해소를 위한 방안을 제안함으로써 재교육을 통해 공공부문 정보보호 인력의 전문성을 높이고자 하였으며, 주요 분석결과와 분석에 따른 시사점은 다음과 같다.

4.1.1 정보보호 교육격차

근무 지역을 수도권과 비수도권으로 구분하였을 때, 교육기회에 대한 인식의 차이가 통계적으로 유의함을 확인하였다. 이를 통해 정보보호 관련 교육과정이 수도권에 밀집되어 있어 지방 재직자들의 정보보호 교육 접근성이 낮다는 주장[12]을 실제 데이터로 실증하였다〈Table 10.〉. 한편으로 대전광역시, 세종특별자치시, 충청도 간에는 교육기회에 대한 인식 차이가 유의미하지 않은 것으로 나타났다. 이를 통해 수도권을 제외한 경우 광역시 여부와 관계없이 정보보호 교육기회는 유사할 것으로 예상된다〈Table 11.〉.

그러나, 공공부문 재직자의 교육격차 해소를 위해 모든 지역에 공공교육기관을 설치하는 것은 사실상 어렵다. 일반적으로 지역인적자원개발을 위해서는 지방정부, 공공기관, 대학의 협력적 네트워크가 중요하며, 대학은 이미 검증된 교수진과 교육시설을 보유하고 있다는 점에 주목할 필요가 있다[11]. 일례로, 과학기술정보통신부와 한국인터넷진흥원은 신규 사이버보안 인력양성을 위해 대학에 예산을 지원하는 정보보호 특성화대학 지원사업을 운영하고 있다. 교육부는 지역의 대학-지자체-공공기관-산업체 간 연계협력을 통해 지역인재를 양성하고 이들이 공공기관에 취업 할 수 있도록 예산을 지원하는 지역선도대학 육성사업을 운영하고 있다. 이러한 사업 방식을 공공부문 사이버보안 인력 재교육에도 적용하여, 공공부문 사이버보안 인력양성 관련 기관-지자체-지자체에 위치한 행정·공공기관이 대학에 금전적 지원 또는 MOU를 맺음으로써, 공공부문에서 정보보호 업무를 수행하는 재직자의 재교육에 중요한 역할을 하도록 하는 방안도 고려할 수 있다.

4.1.2 근무지 내 정보보호 교육 수요

전공, 직무, 직급, 재직 중인 기관 구분과 관계없이 근무지 내 또는 근무지 주변에서 운영되는 정보보호 교육에 참여하고자 하는 수요와 의지가 뒷받침되는 것으로 나타났다. 그러나, 교육 접근성이 높아진다고 해서 현재보다 더 적극적으로 교육에 참석하지는 않을 것이라는 분석결과에 주목해야 한다.

교육과 인사제도의 연계는 지방 공공부문 인력의 역량을 강화하는 효과적인 방법이다[21]. 그러나, 이미 정보보호 교육 이수를 의무화하거나, 이수시간과 성적을 인사고과 등 평가에 반영하고 있는 기관도 다수 있다[9]. 지방 공공부문 재직자의 정보보호 교육에 대한 참여도를 현재보다 더욱 높이기 위해서는 의무 교육 이수시간 인정, 인사고과 반영 이외에 교육 참여에 따른 강력한 인센티브 마련이 필요하다.

공공부문 재직자 대상의 교육은 형식적으로 운영되어 실제 직무수행능력을 향상시키지 못한다는 지적이 있다. 정보보호 교육도 마찬가지로 교육 자체에 대한 낮은 기대 때문에 교육 접근성의 증가가 더욱 적극적으로 참여하려는 의지로 이어지지 않을 수 있다. 이를 해결하기 위해서는 각 공공부문 정보보호 인력의 교육요구사항에 적합한 교육과정을 운영하여, 그들이 스스로 교육의 필요성과 중요성을 체감하도록 하는 노력도 중요하다.

4.1.3 정보보호 교육 요구사항

정보보호 교육 요구사항에 있어서 근무지, 전공, 직무, 직급, 재직 중인 기관 구분 등에서 모두 통계적으로 유의미한 차이를 확인하지 못하였다. 다만, 기초통계분석 결과를 통해 다음과 같은 시사점을 도출하였다.

첫째, 현재 공공부문에 재직 중인 정보보호 인력의 경우 초기부터 정보보호 분야로만 경력을 쌓기보다는 정보통신을 포함한 타 업무 경력이 정보보호 업무 경력보다 많은 경우가 대부분이다. 교육과정의 설계와 교육생 선발에 있어, 교육생의 수준에 대한 고려가 우선시 되어야 한다.

둘째, 교육의 방법에 있어서, 코로나바이러스감염증-19(COVID-19) 상황에도 불구하고 응답자들의 온라인 교육에 대한 선호도는 보통보다 약간 높은 수준으로 나타났다. 그러나, 표준편차가 1.109로 희망하는 교육의 방법에 대한 의견이 다소 나뉘었다. 그 이유 중 하나는 공공부문의 정보보호 전담인력이 적어 오프라인 교육을 참석을 위해 자리를 비울 경우 대체인력이 부족하여 생기는 업무 공백을 꼽을 수 있다. 2021년 국가정보보호백서에 따르면, 정보보호전담부서의 인원수가 2명 이하인 경우가 약 40% 수준이다[9]. 공공부문 정보보호인력의 교육격차 해소를 위해서는 온라인 교육과 오프라인 교육이 병행되어야 할 필요가 있다.

셋째, 교육의 운영과 분야에 있어서 응답자들은 실습 위주의 교육을 선호하는 것으로 나타났다. 실제로 시뮬레이션을 동반한 정보보호 교육을 받은 경우 실제 보안침해사고 대응에 훨씬 더 대처를 잘하는 것으로 알려져 있다[30]. 교육을 희망하는 분야는 기술적 실무 분야인 모의해킹 실무, 클라우드 컴퓨팅 실무와 관리적 실무 관련 분야인 정보보호 관련 법·제도·가이드라인·규정, 정보보안 관리실태 평가 등이 상위를 차지하였다. 특히, 실무자의 경우 보안기술능력 향상에 대한 수요가 상급자보다 높게 나타났다. 이를 통해 교육생의 수요에 부합하면서 실효성 있는 정보보호 교육을 위해서는 이론보다는 실습, 실무로 구성된 교육과정과 실무경험과 실습 역량을 지닌 강사가 요구된다. 이에 지자체 또는 지역에 위치한 공공기관이 인력의 재교육을 위해 대학과의 협업하거나 교육기관을 설립함에 있어 보유한 기자재로 충분한 실습이 가능한지, 교수진의 실무경험이 풍부한지 등이 필수적으로 검토되어야 한다.

마지막으로 응답자들은 교육 참여를 위해 이동이 필요한 경우, 자가용으로 1시간 내외의 거리를 선호한다. 복수 개의 지역에 재직 중인 공공부문 정보보호 담당자를 교육대상으로 하는 교육기관을 설립하거나 선정할 경우, 주변 지역과의 도로교통망의 편의성과 접근성이 고려되어야 한다. 더불어 교육과정은 3일, 하루 6시간 내외의 교육과정으로 구성된다면 참석률의 향상에 도움이 될 것이다.

4.2 향후 연구

본 연구의 조사대상은 수도권과 충청도에 한정되어 있으나, 세종정부청사, 세종국책연구단지, 대덕연구단지, 오송보건의료행정타운, 충북혁신도시 등이 충청권에 위치하고 있고, 2020년 6월을 기준으로 지방이전대상 공공기관의 약 30%가 충청권으로 이전을 완료하였다[31]. 이에, 공공부문의 다양한 기관 유형과 지리적 위치(수도권/비수도권)를 분석에서 다루고 있다. 그렇지만, 전국의 공공부문의 기관을 충분히 대표하지 못하였다는 한계가 있다. 향후 연구에서는 설문조사의 대상을 전국으로 확대하고, 단순히 수도권과 비수도권이 아닌 각 17개 시·도 간, 광역시 간, 행정구역 간에 교육 현실과 요구사항에 차이가 있는지에 대해 심층적인 연구가 필요하다.

또한, 기관·직무·직급을 세부적으로 분석하기에는 충분한 수의 설문을 확보하지 못하여, 시사점이 제한적이다. 향후에는 전국의 다양한 기관, 직무, 직급의 공공부문 정보보호 인력을 대상으로 조사를 수행하여 기관, 직무, 직급을 다양하게 구분하여 각 유형 간의 교육격차와 교육 요구사항의 차이를 확인하는 노력이 필요하다. 일례로 기관의 설립목적, 업무특징과 주로 취급하는 데이터의 종류 및 양에 따라 기관의 유형을 구분하여 교육의 현실과 요구사항의 차이를 검증할 수 있다.

이를 통해 교육 제공이 우선시되는 지역을 확인하고, 각 지역에서 요구하는 교육수요의 특징을 확인하여야 한다. 또한, 인력의 특성 및 기관의 업무 특성에 따라 어떤 교육이 운영되어야 하는지에 대해 구체적으로 확인할 수 있을 것이다.

References

[1] N. Thompson, A. Mullins, and T. Chongsutakawewong, "Does high

e-government adoption assure stronger security? results from a cross-country analysis of Australia and Thailand," *Government Information Quarterly*, vol. 37, no. 1, Jan. 2020. (https://doi.org/10.1016/j.giq.2019.101408)

[2] United Nations, UN E-government Survey 2018, Jul. 2018.

[3] International Telecommunication Union, Global Cybersecurity Index (GCI) 2018, 2018.

[4] Government Accountability Office, Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions, Jun. 2018.

[5] World Economic Forum, The Global Competitiveness Report 2019, Oct. 2019.

[6] World Economic Forum, The Global Competitiveness Report 2020, Dec. 2020.

[7] e-Nara Index, "UN E-Government Development Index Ranking (Irregular Period, 2002~2020)", http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1027, Mar. 25, 2021.

[8] The Board of Audit and Inspection of Korea, National Cybersecurity Management Status Audit Report, Apr. 2016.

[9] Korea Internet & Security Agency, 2021 National Cybersecurity White Paper, May 2021.

[10] Innovation City Season 2, "Progress" https://innocity.molit.go.kr/v2/submain.jsp?sidx=4&stype=1, Mar. 25, 2021.

[11] Keon-Sup Song, "A study on the HRD effects of public institutions to local moving: focused the manpower demand forecasting," *Korean Policy Sciences Review*, 12(3), pp. 201-217, Sept. 2008.

[12] Tea-Sung Kim, Hyo-Jung Jun, Yeon-Bok Kim, Taek-Young Kim, and Song-ha Lee, Advance Research for Development of National Cyber Security Workforce Management System, Policy Research of Ministry of the Interior and Safety, Jan. 2020.

[13] Chun-Oh Park and Ho-Jin Choi, "An empirical study on the effectiveness of education and training system in korean public sector," *Korean Public Administration Quarterly*, 14(4), pp. 939-959, Dec. 2002.

[14] Hyo-Jung Jun, Tea-Sung Kim, and Ki-Tae Park, "How do we manage the information security workforce of the administrative agencies?," *Journal of Information Technology Services*, 18(4), pp. 55-66, Oct. 2019.

[15] M. Cook, Cyber Acquisition Professionals Need Expertise (But They Don't Necessarily Need to be Experts), Fort Belvoir: Defense Acquisition University, Mar. 2014.

[16] W. Crumpler and J.A. Lewis, The Cybersecurity Workforce Gap. Center for Strategic and International Studies (CSIS), Jan. 2019.

[17] S. Furnell, "The cybersecurity workforce and skills," *Computers & Security*, vol. 100, Jan. 2021. (https://doi.org/10.1016/j.cose.2020.102080)

[18] B.L. Mak and H. Sockel, "A confirmatory factor analysis of IS employee motivation and retention," *Information & Management*, vol. 38, no. 5, pp. 265-276, Apr. 2001.

[19] Dong-Woo Kim, Seung-Woan Chai, and Jae-Cheol Ryou, "A study on domestic information security education system," *Journal of the Korea Institute of Information Security & Cryptology*, 23(3), pp. 545-559, Jun. 2013.

[20] M. Van Wart, Changing Public Sector

Values, New York & London: Garland Publishing, Inc., 1st Ed., Oct. 1998.
〔21〕 Seon-Il Cho, "Training needs analysis for manpower development in local government", *Korean Society and Public Administration*, 16(4), pp. 165-187, Feb. 2006.
〔22〕 Moo-Hyun Choi and Yeong-Woo Kim, "A study on the reinforcement of local public officials' competency : focused on the competency-based curriculum," *The Korean Journal of Local Government Studies*, 13(4), pp. 33-59, Feb. 2010.
〔23〕 Seong-Ho Oh, "Tasks and prospects of HR administration: public officials education and training system and its improvement," *The Korean Journal of Public Administration*, 6(3), pp. 23-40. Fall, 1997.
〔24〕 Cheol-Hyeon Baek, "A study on the development for public officials education and training - focusing on the operation process of education and training for local public officials," *Korean Human Relations Review*, 5(1), pp. 25-44, Oct. 2000.
〔25〕 Song-ha Lee, Hyo-Jung Jun, and Tae-Sung Kim, "Evaluation of public information security training programs : a case study," *Journal of Information Technology Services*, 19(1), pp. 173-185, Feb. 2020.
〔26〕 J. Dawson and R. Thomson, "The future cybersecurity workforce: going beyond technical skills for successful cyber performance," *Frontiers in Psychology*, vol. 9, Jun. 2018. (https://doi.org/10.3389/fpsyg.2018.00744)
〔27〕 Sang-Yong Yi, "The linkage of human resources development and education-industry cooperation for regional development," *The Research Review of Regional Development*, 17, pp. 107-133, Dec. 2005.
〔28〕 Higher Education in Korea, "Department Information" https://www.academyinfo.go.kr/mjrinfo/mjrinfo0460/doInit.do, Jan. 21, 2021.
〔29〕 Ji-Jun Song, SPSS/AMOS Statistical Analysis Method for Paper Writing, 21C Book Inc., Oct, 2015.
〔30〕 M. Jalali, M. Siegel, and S. Madnick, "Decision making in cybersecurity capability development: evidence from a simulation game experiment," *Journal of Strategic Information System*, vol. 28, issue 1, pp. 68-82, Mar. 2019.
〔31〕 Innovation City Season 2, "Targeted Public Agencies", http://innocity.molit.go.kr/v2/submain.jsp?sidx=6&stype=1, Sept. 9, 2021.

〈저 자 소 개〉

이 송 하 (Song-ha Lee) 학생회원
2015년 2월: 충북대학교 경영정보학과 학사
2017년 2월: 충북대학교 경영정보학과 석사
2017년 3월~현재: 충북대학교 경영정보학과 박사과정 수료
〈관심분야〉 정보보호 정책, 정보보호 인력 및 교육, 보인경제성, 개인정보보호

전 효 정 (Hyo-Jung Jun) 정회원
2001년 2월: 충북대학교 경영정보학과 학사
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
2014년 2월: 충북대학교 경영정보학과 박사
2014년 3월~현재: 충북대학교 보안경제연구소 Post-Doc
〈관심분야〉 정보보호정책, 정보보호인력, 정보자원관리, 보안경제성

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월 Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월 Arizona State University 방문연구원
2000년 9월~현재 충북대학교 경영정보학과 정교수, 보안경제연구소장, 보안컨설팅연계전공 및 대학원 융합보안전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, 병무청 정책자문위원,한국전력 정보보안 자문위원, 한국지역정보개발원 선임이사, ISMS-P 인증위원회 위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정