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.2021.31.5.1083

국내 정보보호 교육 표준 프레임워크 개발; 연령 및 직무 맞춤의 이원화(Two-track) 교육과정을 중심으로*

박 민 정,[1†] 이 기 혁,[2] 채 상 미[3‡]
[1,3]이화여자대학교 (강사, 교수), [2]중앙대학교 (교수)

Development of a Standardized Framework for Domestic Information Security Education; Focusing on a Two-Track Curriculum Customized by Age and Job*

Minjung Park,[1†] GI Hyouk Lee,[2] Sangmi Chai[3‡]
[1,3]Ewha Womans University (Lecturer, Professor), [2]Chung-Ang University (Professor)

요 약

최근 사용자의 인터넷 의존성 증가와 각종 IT 디바이스의 보급과 확산에 따라, 과거에 비하여 개인 생활 전반에 정보보호가 미치는 영향력이 확대되었다. 이와 더불어 보안을 위협하는 침해 요인들이 지속적으로 복잡, 다양해지고 가짜뉴스 확산, 온라인 신분 도용, 사이버 불링 등을 비롯한 개인의 안전한 온라인 환경을 위협하는 요소들이 사회적으로 증가함에 따라, 정보보호 전문 인력 양성의 필요성이 증가하고 있다. 나아가 기업의 정보보호 업무 종사자 이외에 사회의 모든 구성원이 정보보안의 위협에서 자유로울 수 없게 됨에 따라, 개인의 정보보호에 대한 인식 제고와 자발적인 정보보호 행동을 유도하기 위한 다양한 정보보호 교육 과정의 마련이 필요하다. 따라서, 본 연구에서는 현재 이루어지고 있는 국내·외 정보보호 교육 과정의 현황과 특징에 대하여 분석한다. 이를 통하여 정보보호 교육 필요성과 교육 체계 수립의 전략을 모색하여 본 연구에서는 국내 환경에 적용 가능한 정보보호 교육 표준 프레임워크를 제시하고자 한다. 이는 개인의 정보보호 인식과 지식 수준을 제고하여 국내 정보보호 전문 인력 양성과 더불어 개인과 조직, 사회 전반의 정보보안 수준을 향상시켜 국가 경쟁력 향상에 기여할 것으로 판단된다.

ABSTRACT

With the recent increase in users' dependence on the Internet and the spread of various IT devices, the influence of information security on the users' has expanded compared to the past. Therefore, it is expected to have an increased influence on information security in personal life. In addition, as the intrusion factors that threaten security continue to become more advanced and diversified (eg., fake news, cyberbullying, identity theft), the need for nurturing information security experts is increasing. Furthermore, not only corporate information security workers, but also all individuals, cannot be free from the threat of information security. Therefore, it is necessary to prepare various information security education to improve information security awareness and induce proactive information security behaviors. In this study, characteristics of domestic and foreign information security education courses are analyzed and provide a standardized framework for information security education applicable to the domestic environment.

Keywords: Information Security Curriculum, Information Security Education, Information Security Education Framework, Information Security Training

Received(08. 27. 2021), Modified(09. 07. 2021), Accepted(09. 07. 2021)

* 이 논문은 2020년 대한민국 교육부와 한국연구재단의 인문사회분야 중견연구자지원사업의 지원을 받아 수행된 연구임(NRF-2020S1A5A2A01046634), This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2020S1A5A2A01046634)

† 주저자, mjpark6767@ewha.ac.kr
‡ 교신저자, smchai@ewha.ac.kr(Corresponding author)

I. 서 론

최근에 형성된 COVID-19 팬데믹의 상황으로 전 세계적으로 교육기관의 비대면 수업과 기업의 재택근무 비중이 증가하게 되었다[12]. 이러한 팬데믹 이후의 시대에서는 업무 및 교육 공간의 경계가 사라지게 되었으나 다양한 IT 디바이스를 비롯하여 클라우드, IoT 서비스 이용 증가 등에 따라, 사용자들은 새로운 보안 취약점에 노출되었다[13]. 이에 국내 정부는2020년 '디지털 뉴딜 정책'의 과제 중 하나로 글로벌 정보보호 역량 강화를 제시하며 보안 혁신 인재 양성을 위한 전략으로 정보보호 특성화 대학 선정 등의 정보보호 교육을 강화하기 위한 다양한 노력을 하고 있다. 그러나 2020년 과학학기술정보통신부에서 실시된 '국내정보보호산업실태조사'의 결과에 따르면, 국내 정보보호 인력은 15,655명에 불과하여 적절한 인력 수급이 이루어지지 않는 것으로 나타났다[1]. 이와 더불어 국내를 비롯하여 전세계적으로 현재, 기업의 정보보호 예산 대부분이 정보보호 시스템 구축, 유지·보수 등의 기술 분야에 책정되어 실제 정보보호를 수행하는 조직 구성원들의 교육·훈련 등의 인적·관리적 보안에 대해서는 소홀한 것으로 밝혀졌다[40].

과거에 비하여 복잡, 다양해지는 보안 침해 위협에 대한 선제적 보안 방안 마련과 사이버 레질리언스 구축을 위해서는 사용자 중심의 보안 구축을 위한 정보보호 교육이 필요하다. 나아가 최근 들어, 가짜뉴스 확산, 사이버불링, 온라인 신분 도용 등의 증가는 개인의 안전한 온라인 환경을 위협하게 되었다. 이와 같이 온라인 환경에서 발생하는 다양한 사회적 범죄의 증가는 개인정보 탈취 등의 사용자의 정보보안을 위협하는 문제로 직결됨에 따라, 올바른 정보보호에 대한 인식을 형성하고 상황에 따른 적절한 정보보호 행동을 수행할 수 있는 정보보호 교육의 필요성이 중요해지고 있다. 따라서, 본 연구에서는 교육기관, 공공기관, 민간기관에서 현재 진행 중인 정보보호 교육 체계의 현황에 대하여 살펴본 뒤, 정보보호 인식 교육을 넘어 전 구성원의 보안 내재화를 통한 사용자 중심의 보안 문화를 형성할 수 있는 정보보호 교육 표준 프레임워크를 제시하는 것을 목적으로 한다.

본 논문의 구성은 다음과 같다. 2장에서는 국내·외 정보보호 교육 과정 현황 및 교육 체계 현황을 분석하고, 3장에서는 정보보호 교육 및 정보보호 지식 강화의 필요성에 대하여 제시한다. 이를 바탕으로 4장에서는 앞서 논의된 국내·외 사례를 바탕으로 국내 환경에 최적화된 정보보호 교육 표준 프레임워크를 제안한다. 이를 통하여 마지막 5장에서는 제안된 국내 정보보호 교육의 적용과 활용 전략에 대한 논의를 통하여 결론을 맺는다.

II. 국내·외 정보보호 교육과정

2.1 국내 정보보호 교육과정

2.1.1 국내 정규교육기관 정보보호 교육과정

현재 국내 정규교육기관으로 분류되는 전문대학, 4년제 대학교, 대학원에서 이루어지는 정보보호 교육의 주된 목적은 정보보호 전문인력 양성이다. 2019년 2월 기준, 국내 2~3년제 전문대학 및 4년제 대학교에는 총 47개의 정보보호 및 정보보안 관련 학과가 설치되어 운영중이다[2]. 대학의 각 해당 학과에서 편성된 정보보호의 교과과정을 살펴보면, 공통적으로 1~2학년 과정은 주로 프로그래밍, 컴퓨터 구조 등의 일반 공학 기초 소양 분야를 중심으로 구성되어 있으며 3~4학년 과정은 암호학, 시스템 및 네트워크 보안, 디지털포렌식 등을 비롯한 실습 비중이 높은 것으로 나타났다[14]. 해당 교과목들은 대부분 공학 기초 전공 학습을 중심으로 구성되어 졸업 후 학생들이 학습 내용을 실무에 즉각적으로 반영하기 어려운 단점이 존재한다[3]. 또한, 정보보호 관련 해당 전공 학생이 아닌 타 학과 학생이 정보보호와 관련된 강의를 의무적으로 수강하여야 하는 대학은 존재하지 않았다[14]. 대부분의 국내 대학에서는 현재, 교양 영어, 글쓰기, 글로벌 사고와 의사소통 능력 등과 같은 필수 기초 소양 과목에 대해서는 교양 필수 과목으로 개설하여 학생들의 사회화 및 기초 역량 증진을 지원한다. 그러나 정보보호와 관련된 교과목의 필수 지정은 찾아보기 어렵다는 점에서 대학을 비롯한 국내 정규교육기관에서는 정보보호를 학생들의 향후 사회화 과정 및 졸업 후 업무 능력 함양을 위한 필수 역량으로 인식하고 있지 않음을 추론할 수 있다. 즉, 현재 국내 대학의 정보보호 교육 과정 대부분이 관심이 있는 학생 중 해당 학과에 선발된 학생에 한하여 정보보호 교육 기회를 제공하기 때문에 타 학과 학생들의 정보보호 관련 교육 이수에 대한 접근 장벽이 높다. 이에 따라, 대부분의 학생들은 정보보호 관련 지식을 습득하지 못한 채 대학을 졸업하게 되어 실제 업무 현장에서 반드시 필요한 기본적인

정보보호 지식을 갖추지 못한 채, 정보를 다룸에 따라 보안의 위협과 취약점에 그대로 노출될 수 밖에 없게 된다.

국내 정보보호 관련 대학원은 대학 학사의 형태와 동일하게 단일전공 형태의 일반대학원 및 전문.특수대학원에 개설되는 경우와 학연산협동과정 및 다양한 학과의 융합학과 형태로 운영되는 특징이 있다.

대학원에 설치된 정보보호 전공은 석,박사 중심의 정보보호 전문 인력 양성을 목적으로 한다는 점에서 기초 공학, 수학 등의 지식을 바탕으로 암호 알고리즘 개발, 시스템 및 DB 보호 기술 개발 등과 같은 과목을 커리큘럼에 포함한다. 이외에 정보보호 기술 표준화, 응용 서비스 개발, 적용 등과 같이 심화 교과목을 중심으로 구성된다[14]. 특히, 정보보호 분야의 대학원은 심층 전공 지식 습득 기반의 주체적인 연구 수행이 가능한 전문 석,박사 배출을 목표로 한다는 대학원의 교육과정 목표에 따라 정보보호 관련 학위 취득 후, 졸업생의 정보보호 관련 분야로의 진출 비율이 상당히 높은 것으로 나타났다[15]. 이를 러한 통계 결과를 통하여, 국내 정보보호 대학원은 정보보호 분야의 전문 연구 인력 양성의 개설 취지에 비교적 부합하여 현재 운영되는 것으로 볼 수 있다. 그럼에도 불구하고, 아직까지 대학을 비롯한 국내 정규교육기관에서는 정보보호 관련 교과목을 수강하거나 교육과정을 이수하기 위해서는 제한 사항이 많음에 따라, 원활한 인력 수급을 위한 정보보호 전문가를 양성하기에는 한계가 존재한다. 이와 더불어 정보보호 관련 교과목의 수강이 가능한 학생들이라 하여도 소속 대학 및 학과 내에 접근 가능한 교과목의 설치 범위와 그 수가 다양하지 않다. 이에 국내 정보보호 인력 양성 및 국내 사회에 조성된 정보보호의 전반적인 인식 수준을 제고하기 위해서는 교육과정의 재편을 비롯하여 교육 프로개름 확대 개설 등의 노력이 지속적으로 요구된다.

2.1.2 국내 공공기관 정보보호 교육과정

대학 이외에도 국내 공공기관 중 대표적으로 한국정보기술연구원(KITRI)과 과학기술정보통신부에서는 각각 "Best of the Best(이하 BoB)"와 "케이쉴드 주니어(K-Shield Jr.)"를 통해 정보보호 교육 프로그램을 정기적으로 운영하고 있다. 먼저 BoB와 케이쉴드 주니어 모두 정보보호에 관심 있는 지원자를 대상으로 필기시험과 면접 등의 자체 평가 절차에 따라 교육 대상자를 선발하여 교육 프로그램을 제공하고 있다.

2012년 1기를 시작으로 2020년 9기까지 약 1,200여명의 정보보호 인력을 배출한 BoB의 경우, △보안 컨설팅, △보안제품개발, △취약점 분석, △디지털 포렌식의 4가지 트랙을 중심으로 운영된다[16]. BoB의 전체 교육 과정은 총 3단계로 구성된다. 첫 번째, 1단계는 정보보호에 관한 기본 소양과 기반 지식을 습득하기 위한 과정으로 트랙별 구분 없이 공통 교육으로 이루어진다. 이후 2단계에서는 4개의 트랙 과정중, 지원자가 사전에 선택한 트랙에 맞추어 각 트랙별 심화 교육을 이수한다. 따라서, 정보보호에 대한 기초 전반적인 지식을 습득하는 1단계와 해당 지식을 바탕으로 세부 분야에 대한 전문지식을 함양하는 2단계로 구성된다. 이후 최종 3단계에는 1,2단계 과정의 종합 평과 결과 선발된 30여명의 인원에 한하여 참여 가능하도록 하였다. 이러한 과정을 거쳐 최종 선발된 인원은 상금, 프로그램 이수 인증서를 비롯하여 선정된 팀의 창업 및 기술 사업화를 지원한다.

케이쉴드 주니어는 과학기술정보통신부가 주최하고 한국인터넷진흥원이 주관하는 교육과정으로 2018년 1기를 시작으로 2021년 현재 6기까지 운영되었다[17]. 케이쉴드 주니어는 수강생이 프로그램 이수 후, 정보보호 업무 현장 실무에 바로 투입 가능한 수준의 인력 양성이 주된 목적임에 따라, 주로 실무 능력을 함양 시킬 수 있는 교육 과정으로 구성되어 있다. 구체적으로 케이쉴드 주니어의 교육과정은 △정보보호 관리진단, △ 보안사고 분석대응 두가지로 분리하여 교육생을 선발하여 교육한다. 정보보호 관리진단 과정은 정보보안 컨설턴트, 기업 보안담당자, 모의해킹 분야로의 인력 양성을 위한 교육 과정으로 구성되었다. 보안사고 분석대응 과정에는 실제 보안사고에 대한 대응 이해 능력을 향상시키기 위하여 침해사고 분석, 악성코드 분석, 보안솔루션 개발, 보안관제(Computer Emergency Response Team, CERT) 등의 분야를 중점적으로 교육한다[18].

앞서 제시한 바와 같이, 국내 공공기관에서 이루어지는 BoB과 케이쉴드 주니어 교육 프로그램 모두 국내 정보보호 전문인력 양성의 목표를 가지고 자체 평가제도에 따라 선발된 수강생을 대상으로 이루어지는 교육 프로그램이라는 공통점이 있다.

앞서 제시한 바와 같이, 국내 대학과 공공기관에서 시행하는 정보보호 교육 프로그램의 주된 취지는

정보보호에 대한 수강생들의 관련 지식 습득 기회를 제공하고 국내 정보보호 시장의 원활한 인력 수급을 위한 관련 분야의 전문 인력 양성이다. 그러나 이러한 취지와 달리 대학과 공공기관의 교육 프로그램 모두 학생들의 자발적인 의지를 바탕으로 지원한 뒤, 각 기관의 자체 평가 절차를 통하여 선발된 수강생들에 한하여 프로그램을 이수할 수 있다는 점에서 교육 프로그램의 접근성이 낮다. 따라서, 국내 교육기관을 비롯한 공공기관에 정보보호 교육 과정이 운영되고 있는 것에 반하여 개인의 정보보호 지식 향상과 사회 전반에 미치는 긍정적 파급효과는 미미하다.

2.1.3 국내 민관기관 정보보호 교육과정

공공기관 중심의 교육 운영 프로그램 이외에 국내 민간기관에서는 코어시큐리티, 씨드젠, 라온 화이트햇센터, 라이지움, 인섹시큐리티 등에서 정보보호 전문 교육을 시행하고 있다[4]. 이러한 민간기관의 정보보호 교육 프로그램은 주로 정보보호 교육을 희망하는 기업 및 조직 혹은 정보보안 종사자를 주로 대상으로 정보보호 교육이 시행된다. 해당 교육은 조직의 정보보호 수준 제고를 목적으로 조직 구성원의 정보보안 인식 향상 및 기초 역량 강화를 주로 목적으로 이루어진다.

코어시큐리티의 경우, 조직의 보안기술 역량 향상을 위한 집체교육과정 등을 제공하며 씨드젠은 조직원을 대상으로 보안 인식을 강화 및 실무에 적용 가능한 온/오프라인 교육을 제공한다. 마지막으로 라온화이트햇센터는 CTF와 실시간 공방 등의 실전 교육을 통한 조직 정보보호 인력의 역량 강화를 목적으로 한다. 이외에 인섹시큐리티, 라이지움 등은 정보보안 직무 종사자를 주로 대상으로 CISSP, CISA 등의 관련 자격증 취득 지원 및 해킹보안, 디지털포렌식 등의 전문성 확보를 위한 다양한 프로그램을 운영 중이다[19]. 즉, 민간기관의 정보보호 교육은 조직 전체를 대상으로 하는 인식 교육과 정보보호 인력을 대상으로 정보보호 전문 심화 교육으로 분류할 수 있다.

민간기관의 경우, 정보보호에 관심이 있는 조직에서 구성원의 정보보호 인식 강화와 정보보호인력의 전문성 향상을 목적으로 교육을 시행하고 있다. 그러나 대부분 기업 혹은 조직의 신청에 따라 정보보호 교육이 이행되기 때문에 민간기관에서의 정보보호 교육 대상의 범위가 넓지 못한 실정이다. 또한, 민간기관에서 이루어지는 교육은 대부분 유료 교육 과정으로 수강자의 수강 비용에 대한 경제적 부담이 발생하는 동시에 다양한 교육 과정이 마련되지 않은 점 또한 문제점으로 존재한다.

2.2 해외 정보보호 교육과정

2.2.1 해외 정기교육기관 정보보호 교육

미국은 정보보호 전문 지식을 가진 인력의 수요 증가에 따라, NSA(National Security Agency)의 NSTISS(National Security Telecommunications and Information Systems Security Committee)가 5개로 구성된 정보보호 표준 교육과정을 제정하였다[20,21]. 해당 표준교육과정은 무엇이 중요한지에 대한 '인식(Awareness)'과 실무(Performance)' 의 레벨로 제시하여 각 레벨에 따른 범위와 내용 등을 제시한다[21]. '인식'에 해당하는 레벨에서는 시스템 운영 환경, 운영체제, 통신이론 등의 보안에 대한 전반적인 개론을 학습하고 '실무'의 레벨에서는 각 보안 정책과 거버넌스, 침해 대응, 취약점 평가, 위기 관리 등에 대해서 학습한다. 해당 표준교육과정은 파트너십을 맺은 대학을 비롯한 정규교육기관에 보급한다[21].

미국의 NSA는 표준교육과정 이외에 정보보호 전문 인력 네트워크를 구축하고 국가 보안을 향상시키기 위한 CAE(National Centers of Academic Excellence (CAE) in Cyber Operations Program)를 운영 중이다. CAE는 미국 국가의 사전 허가를 받은 2년제, 4년제 대학 수준의 기관이 NSA에 의하여 교육과정을 인증 받아 정보보안 교육과정 기관으로 지정받아 운영된다[22]. 해당 교육과정에서는 데이터 분석 기초, 각종 프로그래밍 언어, 사이버 방어, 사이버 위협, 보안설계 원칙의 2년 과정과 데이터베이스, 네트워크 일반, 네트워크 보안, 운영체제 개론, 확률과 통계, 프로그래밍의 4년 과정으로 구성된다. 해당 기본교육 내용을 바탕으로 암호학 심화, 법회계학, 알고리즘, 클라우드 컴퓨팅, 아날로그 통신 등의 선택 심화를 이수하게 된다[22]. 이외에 카네기멜론대학교, 펜실베니아주립대학교, 조지메이슨대학교, 캘리포니아주립대학교 등 많은 대학에서 사이버보안, 정보보호 등의 다양한 명칭으로 독립된 정보보호 학위 과정을 운영중이다. 이와 같이 독립된 정보보호 관련 학위 뿐만 아니라, 컴퓨터 공

학, 데이터 사이언스 등 다양한 학과에서 운영되는 정보보호와 관련된 세부 학위 과정도 다수 존재한다.

영국은 사이버 공격에 대응하여 'CERT'를 창설하여 정보보안 인재 양성을 위하여 영국 공학기술원과 파트너십을 체결하여 우스터대학, 드몽포르대학, 벨파스트퀸즈 대학에 사이버 보안 관련 학위과정을 개설하였다[23]. 또한, Royal Holloway 대학, Buckingham 대학, Napier 대학에서는 정보보호학,석,박사의 학위 과정을 운영중이다[21]. 특히, Royal Holloway 대학은 직장인을 주로 대상으로 하는 단기 석사 학위 과정을 운영하여 정보보안 업무 종사자의 전문성 향상을 위한 교육체계를 갖추었다[21].

일본은 2009년 시행된 국가 IT 전략인 'i-Japan Strategy 2015' 일환으로 국민의 정보보안 인식 강화를 위한 노력으로 '정보보안 인재 육성'에 관한 프로그램을 개발하였다. 해당 프로그램은 일본 내, 국가 정보보안 경쟁력을 향상시키기 위하여 일반 국민 전체를 교육 대상자로 하여 전체 국민의 정보보안 인식 수준을 균형 있게 향상 시키기 위한 병렬식의 프로그램으로 구성된 특징이 있다[21]. 특히, 대부분의 국가 정책은 대학 등의 고등 교육기관을 중심으로 정보보호 교육을 이행할 것을 권고하고 성인 대상의 정보보호 교육 과정을 주로 개발하였다. 그러나 이와 달리 일본은 초·중학교 청소년을 대상으로 하여 정보보안의 기초적 소양을 함양시키고자 했으며 나아가 고등학교에서는 정보보호 교과를 필수 과목으로 포함하였다 는 점에서 주목할 만하다[21].

2.2.2 해외 공공기관 정보보호 교육과정

미국은 급증하는 사이버공격에 대비하기 위하여 정보보호 전문 인력을 양성하기 위하여 관련 교육 과정을 국가 차원의 정책 마련을 통하여 일찍이 시행중이다. 대표적으로, 2011년 8월 '사이버보안 교육을 위한 국가 계획 (NICE: National Initiative for Cybersecurity Education)'을 발표하였다[19,24]. NICE는 정보보호 업무 종사자나 전공자뿐만 아니라 전국민을 대상으로 정보보호에 대한 지식 수준의 향상을 목표로 한다.

NICE의 전체적인 운영은 국토안보부에 주관하나, 실무적인 내용은 미국 국립표준기술연구소(NIST: National Institute of Standards and Technology)에서 운영하여 교육과정의 전문성 유지를 위한 지속적 노력을 이행하고 있다. NICE는 전연령대를 대상으로 이루어짐에 따라, 연령대에 맞추어 세분화된 정보보호 교육 커리큘럼이 존재하며 이에 따른 교육 달성 목적이 다르다[24]. 먼저, 유치원 및 초·중·고 학생에게는 정보보호의 기반이 될 수 있는 과학, 기술, 수학, 공학 등의 이공계 기초 관련 교육의 중요성을 강조한다. 이와 같은 교육과정은 주로 교육부와 국가과학재단에서 주도를 하여 교육 프로그램을 개발하여 학교 등의 공식 교육기관에 배포하게 된다. 나아가, 대학, 대학원생을 비롯하여 정보보호 관련 업무 종사를 대상으로는 보다 전문적인 교육을 제공한다. 이는 전문성이 요구되는 교육 과정인 만큼 주요 대학, NIST 등에서 참여하여 교육 강좌가 구성된다. 마지막으로 일반인을 대상으로는 정보보호 관련 기초 지식 및 정보보호 필요성에 대한 인식 향상에 주로 주안을 두고 있다. 이는 '인터넷 사용과 사이버보안 인식 향상을 위한 대국민 캠페인 활동 및 강좌'와 같이 국민이 쉽게 접근 가능한 다양한 교육 자료의 제공을 통하여 주로 이루어진다[19]. 이와 같이 연령대에 따른 NICE의 교육 체계는 사이버 위험에 대한 미국민의 정보보호 인식 수준 향상, 정보보호 업무에 투입 가능한 숙련된 전문 인재 양성, 정보보호 분야의 국가 경쟁력 확보의 각 단계에 따른 달성하고자는 목표의 차이에서 기인한 것으로 볼 수 있다.

영국은 국가 사이버보안 중추 기구인 사이버보안센터(National Cyber Security Center)를 2016년 설립하여 개인, 기업, 정부기관의 정보보안 사고 대응을 비롯하여 국가 차원의 국민 정보보안 교육을 총괄하고 있다. 구체적으로, 11세~19세의 학생을 대상으로 이루어지는 정보보안 육석 프로그램인 'CyberFirst', 영국 내 세계적인 정보보안 우수 대학 지원 프로그램(ACE-CSR), 정보보안 산업계 인력 교육 프로그램인 'Industry 100', 정보보안 전문가 교육 프로젝트인 'CyBOK(Cyber Security Body of Knowledge)' 등을 개발하여 운영중이다[23].

III. 정보보호 교육과정 강화 필요성

앞서 살펴본 바와 같이, 국내 정규교육기관을 통하여 정보보호 분야를 전공하거나 별도의 교육기관 등을 통하여 정보보호 교육을 수강하지 못한 성인들은 정보보호에 대한 충분한 지식을 습득하지 못한 상

황에서 조직 구성원이 된다. 그러나 점차 보안을 위협하는 공격 유형은 지속적으로 복잡 및 다양해지는 동시에 공격의 발생 빈도 증가와 피해 범위가 확대됨에 따라, 조직은 이에 대응하기 위한 조직 구성원들의 정보보호 교육 필요성에 대한 인지가 최근 증가하기 시작하였다[26]. 따라서, 조직 구성원을 대상으로 내부 정보보호 교육 시행, 외부 전문기관을 통한 정보보호 교육 수행, 사내 정보보호 전담 인력 배치 등 조직 내 정보보안 수준 향상을 위한 다양한 노력을 시도하고 있다[27]. 이를 통하여 조직의 객관적인 정보보호 수준 향상을 비롯하여 조직 내부의 보안 문화를 활성화함에 따른, 조직원들이 능동적인 보안 활동 참여를 유도하고 있다[5]. 그러나 조직 구성원들에게 시행되는 정보보호 관련 교육 프로그램이 항상 정보보안 침해사고의 발생 가능성을 줄이거나 구성원의 보안 의식 강화에 직접적인 영향을 주는 것이 아님이 밝혀졌다[6].

정보보호 교육과 관련된 선행연구 결과를 종합하면, 정보보호의 교육 유형과 방식, 교육 수강생들의 정보보호에 대한 관련 기초 지식 습득 여부 및 인식 및 성별, 연령, 개인정보침해 경험 등의 특징에 따라, 개인의 정보보호 교육 프로그램 사전 수강 여부가 정보보호 행동과 태도에 미치는 영향은 상이한 것으로 밝혀졌다[29~31]. 특히, 시간과 공간의 물리적 제약 사항을 해결해주는 다양한 온라인 교육 프로그램의 등장과 COVID-19의 확산과 더불어 비대면 교육 방식의 필요성 증가는 교육 방식에 따른 정보보호 대한 사람들의 태도에 영향을 미친다. 특히, 오프라인 교육 방식에 비하여 온라인 교육 방식이 개인의 정보보안 행동을 향상시키는데 영향력이 큰 것으로 나타났다[28]. 이외에도 조직은 구성원의 정보보안 정책 준수 및 정보보호 행동을 유도하기 위하여 보상 및 처벌의 제도를 운영하여 조직 내부의 정보보안 수준 향상을 위한 노력을 오랜시간 진행하여왔다[26]. 그럼에도 불구하고, 최근 들어 대부분의 정보침해 사고의 원인이 보안 기술의 결함 보다 조직 구성원 내부의 보안 정책 준수 소홀, 관리 태만, 수동적 정보보호 행동 이행 등의 구성원의 결여된 자율성에서 기인하는 것으로 밝혀짐에 따라, 구성원의 자발적 정보보호 행동을 유도하기 위한 교육 과정의 필요성이 증가하고 있다[33]. 이를 위한 방법으로, 조직 구성원의 능동적인 정보보호 정책 준수 유도를 위한 방안으로 정보보안 정책에 대한 개인의 내재화 강화 전략, 정보보호 중요성 인식 향상이 구성원의 자발적인 정보보안 행동을 유도하는 것으로 밝혀졌다[32].

앞서 제시된 선행연구를 통하여 밝혀진 정보보호 교육의 역할과 기대효과 및 정보보호 행동에 미치는 영향을 살펴보면 실제 2장에서 대부분의 국내외 대학, 공공 및 민간 기업에서 정보보호 교육 프로그램 개설의 취지인 정보보호 전문 인력 양성이 실제 기업 현장에서는 실효성을 갖지 못하는 것으로 볼 수 있다. 따라서, 현재 정보보호 교육 과정의 실효성을 향상시키기 위해서는 정보보호 중요성에 대한 개인의 인지 수준을 높이기 위한 방법으로 정보보호에 대한 내재화 향상 전략이 교육과정에 반영될 필요가 있다. 특히, 최근에는 정보보호 관련 업무 종사자 뿐만 아니라 대부분의 조직 구성원이 정보를 다룰 수 밖에 없음에 따라, 정보보호교육 수강 범위를 확대 시켜야 한다. 한편, 현행 교육과정에는 초등 실과 교육 및 중·고등학교 정보 과목에 정보보호에 관한 내용이 존재한다. 초등 실과와 중학교 정보 교육 과정의 경우 개인정보보호 관련 내용만을 다루며, 고등학교 정보는 정보보안과 관련된 법규를 다루고 있다[7]. 이러한 교육의 성과로 '2020년 개인정보보호 실태조사' 결과에 따르면, 청소년의 93.1%가 개인정보보호의 중요성을 인식하고 있는 것으로 나타났다. 그러나 50.6%가 개인정보 침해를 경험하였으며 이 중, 32.7%가 개인정보 침해 후 조치를 하지 않는 등 정보보호에 대한 인식이 실천으로까지 이어지지 못하는 것으로 밝혀졌다. 이는 정보보호 교육의 비율이 전체 초등 실과 교과목의 1%, 중등 정보의 경우 3~6%에 그칠 정도로 적으며 [7] 다양한 분야의 지식이 필요한 정보보호 교육임에도 불구하고충분하게 정보보호에 대한 지식 습득의 기회가 제공되지 못했기 때문이다. 그러므로 초·중등 과정에서는 정보보호 인식을 강화하고, 학습자의 정보보호에 대한 이해가 가능한 고등 교육 및 대학 교육과정에서의 정보보호 지식 교육을 강화 필요성이 존재한다. 이와 같은 교육 과정을 통하여 국내 사회 구성원 전체가 정보보호에 대한 인식을 향상시키는 것을 넘어 정보보호에 대한 내재화를 통한 능동적인 정보보호 행동으로 견인할 수 있어야 한다.

IV. 국내 정보보호 교육 표준 프레임워크

개인의 정보보호 내재화 실현 및 국내 사회의 보안문화 활성화를 위한 전략으로 본 연구는 다음과 같은 정보보호 교육 표준 프레임워크를 제시한다. 해당

교육 표준 프레임워크는 국내 대학, 공공 및 민간 기관에서 정보보호 교육 프로그램을 개발 및 운영하기 위한 기본 지침의 의미를 갖는다. 현재 국내에서 운영되는 정보보호 교육 프로그램은 대부분 일관적인 기준 없이 각 기관의 자체적인 커리큘럼을 구성하여 교육을 이행함에 따라, 수강생들의 교육 연속성을 확보하기 어렵다. 국내 정보보호 지식교육 강화를 위해서는 단발성의 교육 과정이 아니라 수강생이 본인의 보유 역량, 교육 수강 목적 등에 맞추어 효율적으로 강좌를 수강할 수 있는 기반이 조성되어야 한다. 이를 위해서 본 연구에서 제안하는 교육 표준 프레임워크는 각 기관에서 이를 기반으로 하여 정보보호 교육 프로그램을 자체적으로 활용하여 운영할 수 있도록 하여 다양한 프로그램의 개발에 기여한다. 이와 동시에 수강생들의 교육 연속성과 기본 역량에 대한 교육 기회를 확장하게 된다. 이는 국가 차원에서 국민 전체의 정보보호 인식 수준을 제고하는 동시에 국내 경쟁력 향상을 위한 정보보호 전문 인력 양성을 위한 교육 과정 개발을 도모하게 된다.

현재까지 선행연구를 통하여 주로 제시된 정보보호 교육 과정은 대부분 정보보안 업무 종사자를 대상으로 구성되었다[19,34~36]. 따라서, 기업 규모, 기업의 산업 분류 형태, 기업의 개인정보처리 규모 등 주로 기업의 특징에 따라 교육 과정이 제시되었다. 이는 기업 내, 정보보호 수준을 높이고 정보보호 업무 종사자의 전문성 강화에는 긍정적인 영향을 줄 수 있는 것에 반하여 사회 전체의 정보보안 수준까지 향상시키는데에는 역부족이다. 이에 공공기관을 비롯하여 국가 차원에서 정보보호 교육의 중요성을 강조한 연구가 진행되었음에도 불구하고[19], 최근 들어 확장된 비대면 기반의 생활 방식과 고도화된 정보보호 침해 유형이 반영된 교육 프레임워크에 대한 연구는 미미한 실정이다. 따라서, 본 연구에서 제안하는 정보보호 표준 교육 프로그램은 전국민을 대상으로 적용할 수 있도록 연령별 특화 기본 교육 및 정보보호 전문가 양성을 위한 직무 맞춤형 심화 교육의 투트랙(two-track)의 중장기 교육 로드맵으로 구성된다.

모든 사회 구성원에게 정보보호 지식을 교육하기 제공하기 위해서는 기본 교육 과정에서 관련 교육이 선행될 필요가 있다. 따라서 초등학교부터 대학교까지 전 과정에서 정보보호 교육을 시행하여 정보보호 지식을 단계적으로 강화한다. '2015 교육 과정'에서 시행되고 있는 초등 및 중등 교육은 개인정보보호에 대한 교육을 통한 정보보호 인식 함양을 목적으로 하고 있다. 해당 연령대에서는 일반적인 교육보다 부모와 함께 진행하는 교육이 교육의 효과를 극대화할 수 있다[8]. 따라서, 본 시기에는 기존의 주입식 교육보다 부모와의 동반 교육을 통해 정보보호 인식을 함양하고 실생활에서 실천할 수 있는 정보보호의 훈련에 익숙해지기 위한 교육이 필요하다. 이와 같이 청소년기부터 정보보호 교육에 대한 개인의 접근성을 높여 정보보호에 대한 익숙함과 기초 소양을 습득할 수 있도록 토대를 제공한다.

청소년기에 학습한 기본 정보보호 지식을 바탕으로 이후에는 학생들의 자발적 의지에 따라, 정보보호에 대한 심층 교육을 이수할 수 있는 교육 프로그램을 확대하여 운영한다. 구체적으로, 교육부에서 현재 지원하는 중·고등학교 재학생을 대상으로 시행하는 화이트해커 양성사업인 '정보보호 영재과정'와 같은 전문 인력 양성 과정을 권역별로 확대 개편한다. 고등 교육에서는 정보 과목을 통해 주로 정보보호 교육을 시행하고 있지만, 대학 입시에 반영되지 않아 교육에 대한 집중도가 감소하는 단점이 존재한다. 이에 학생들의 수업 참여도에 대한 의지와 지식 습득에 대한 동기를 고취시키기 위하여 다양한 교수법이 활용된다. 일례로 한국정보기술연구원 주관의 '사이버 가디언즈' 사업은 방과후 학교, 동아리 활동, 체험학습 등을 지원하여 정보보호 교육의 질을 향상하고 있다. 또한, 스마트교육 모형 등의 체험형 교육을 사용하여 기존의 강의식 수업보다 효과적인 정보보호 지식교육을 수행하도록 한다[9]. 이를 통하여 학생들의 정보보호 관련 고등교육 과정 이수 경험을 바탕으로 향후, 대학 진학 및 진로 계획 설정 과정에서 정보보호 관련 분야로의 진출을 지원하는데 기여하게 된다.

정규 교육과정에서 정보보호 지식을 습득하더라도 이를 실무에 바로 적용하기 위해서는 응용 역량이 요구된다. 그러므로 각 대학의 정보보호 수업은 관련 이론과 더불어 실무에 적용 가능한 교육 훈련 과정을 포함하여 커리큘럼이 구성되어야 한다.

정보보호 혹은 컴퓨터 공학 등 정보보안과 직접적인 관련이 없는 전공이라 하여도, 졸업 후 각 분야에서 적절한 정보보호 행동을 수행하기 위한 기초 지식 및 실천 방법 등에 대하여 습득할 수 있는 정보보호 관련 교양 과목 등의 개설 및 의무 수강에 대하여 고려해볼 필요가 있다. 이와 같은 정보보호 교육 방식의 개선을 통하여 국내 정보보안 전문 인력 양성 및 국내 다양한 정보보안 전문가의 적재적소 배치가 이

Table 1. Information Security Education Framework

		Contents	Benefits
Formal Educational Institution	Elementary / Middle school	Acquiring information security behaviors and strengthening awareness through shared education with parents	Reinforcement of information security awareness and necessity
	High School	Providing high-quality information security education by developing new teaching methods	Strengthening information security knowledge
	Undergraduate / Graduate school	Opening of information security and practical training elective courses applicable to each major	Acquisition of convergence information security knowledge based on various majors
Speciality Area	Securely Provision	Research and Development of software assurance, security engineering and new technology	Estabilsh new security workstations
	Operate and Maintain	Defense analysis of computer network and infrastructure support	Design fundamental security principles and keep safety
	Oversight and Development	Provide legal advice and advocacy, strategic planning and policy development	Develop Chief Security Manager & Security Strategy Specialist
	Digital Forensic Specialist	Investigate cybercrimes and data administartion	Understand data management
	Security Consultant	Analyze threats and manage whole information security risks	Plan information security strategy
Public Institutions		Evaluation of the quality of information security education and development and distribution of various free education programs	Improving all individuals' access to information security education

루어질 것으로 예상된다. 단순히 기술적 보안 위주의 정보보호 교육만으로는 COVID-19 이후 뉴노멀 시대의 보안 위협에 대응하기 어렵다. 그러므로 현재 진행되는 인식 강화 및 기술적 보안 위주의 정보보호 교육에서 벗어나 물리적, 관리적 보안 등의 융합보안을 통한 다양한 정보보호 교육이 도입되어야 한다[10]. 따라서, 대학 과정 이후에서의 정보보호 교육은 정보보호 인식을 넘어 융합보안에 대한 지식 학습을 통한 정보보호 실천으로 이루어질 수 있도록 진행되어야 한다. 본 연구에서 제시하는 교육 표준 프레임워크는 앞서 제시한 바와 같이, 연령대별 정보보호 교육 이외에 정보보호 업무 종사자의 맞춤화된 필수 및 심층 교육과정을 분류하여 함께 포함한다. 이는 실제 업무 현장에서 적용 가능한 실무 중심의 교육 훈련을 포함하여 교육 이수 후, 수강자가 바로 실효성있는 정보보호 지식의 활용을 위해서이다. 이를 위하여 NICE의 Workforce Framework에서 제시한 정보보호 직무체계[37]와 국내 정보보호 분류체계를 바탕으로 전문 인력 양성을 위한 세분화된 직무의 기준을 설계하였다.

포스트 코로나 시대의 등장에 따라, 온라인 기반의 비대면 강의에 대한 사용자의 친밀감 증가 및 플립 러닝(flipped learning)이 확대되고 있는 추세이다[38]. 각종 IT 디바이스를 활용하여 수강자가 필요에 따라 능동적인 교육 수강 의지에 따라 이루어지는 플립 러닝은 기존의 오프라인 중심의 교육 형태를 온라인으로 전환시켰다[39]. 따라서, 본 연구에서 제안하는 프레임워크는 대면 중심의 수업을 넘어 다양한 온라인 동영상 교육 콘텐츠가 개발될 수 있도록 하는데 주안을 두고 있다. 먼저, 수강자가 필요한 정보보호 분야의 핵심에 대한 동영상 콘텐츠를 제공할 수 있도록 하여야 한다. 이러한 동영상 콘텐츠는 물리적, 시간적 공간의 제한 없이 수강생의 의지에 따라, 수강할 수 있다는 점을 바탕으로 정보보호 교

육에 대한 사용자의 접근성을 높이고자 한다. 나아가, 지식의 사전 이해 후, 이를 업무 종사자가 바로 실전에서 적용할 수 있도록 하는 플립 러닝의 취지를 극대화 하는 방식으로 추진된다. 이와 같은 온라인 교육 동영상 콘텐츠는 교육기관과 공공분야에서의 원활한 협력 체계 구축을 통하여 다양한 방식으로 개발될 수 있어야 하며 이의 배포 및 관리에 대한 공공기관의 역할이 요구된다. 이와 같이 본 연구에서 제시한 정보보호 교육 표준 프레임워크를 다음의 Table 1.을 통하여 제시한다.

Table 1.은 각각의 연령대에 따른 교육 과정의 특징과 교육 이수에 따른 수강효과에 대하여 자세히 나타내고 있다. 연령대에 따른, 각 단계별 교육의 특징을 키워드 중심으로 살펴보면 먼저, 초등 및 중등의 청소년 대상의 교육 특징은 정보보안의 중요성을 고취시키고 정보보안의 인식 자체를 개선하기 위하여 부모와 함께 실생활에서 이루어지는 특징이 있다. 특히, 해당 과정에서는 수강생의 연령을 고려하여 부모와 함께 수강생이 정보보안에 대한 인식을 강화하기 위한 과정이 주로 마련된다. 이는 청소년기의 수강생 특징을 반영하여 가정에서 부모와 함께 생활에서 실천할 수 있는 정보보호 활동부터 주로 습득하게 된다. 이후, 고등학교 과정에서는 이전 단계에서 학습한 내용을 바탕으로 정보보안과 관련된 보다 심화된 지식을 학습하고 정보보안 인식을 강화한다. 대학 및 대학원의 단계에서는 현재와는 다르게 정보보호 교육을 필수 과목으로 개설하여 학생들의 정보보안에 대한 기초 지식을 배양하고 이를 바탕으로 사회 진출 후, 각 분야에 맞는 정보보호 활동을 능동적으로 수행할 수 있도록 지원한다. 또한 각 전공별로 필요한 정보보호 지식과 각 전공에 적용 가능한 정보보호 활동을 훈련하는 것이 해당 단계의 주요 목적이다.

V. 결 론

본 연구는 정보보호 교육 표준 프레임워크를 제시함에 따라, 이를 통한 개인의 정보보호 인식 제고 및 전문 인력 양성을 통한 국가 보안 수준 향상에 기여하고자 한다. 특히, 현재 이루어지는 조직의 정보보호 교육은 대부분 단기적인 임시방편에 그치는 경우가 많아 교육 효과가 지속되지 못하는 문제점이 있다[11]. 따라서, 본 연구에서 제안하는 교육 표준 프레임워크는 중장기적 관점에서 교육이 이루어질 수 있도록 구성하였다. 이와 더불어 현재까지 주로 정보보안 업무 종사자를 중심으로 설계된 정보보호 교육 과정과 달리 전연령대로 교육 수강 대상이 확대될 수 있도록 하였다. 이를 통하여, 각 연령 시기별에 맞춤화된 정보보호 교육을 제공하고 정보보안 업무 종사자의 세분화된 직무 특징에 따른 교육 제공을 통하여 정보보안 전문가 양성의 효율성을 극대화하고자 한다.

국내 '정보보안 마스터플랜'에 따르면, 정보보호 기반 강화를 위하여 정부기관의 정보보호 인력 증원 및 국가 핵심기반시설 운영기관의 보안전담인력 확보 방안 등을 제시하고 있다. 그러나 대부분 공공기관의 정보보호 전문 인력 확충 방향에만 중점을 두고 있으며, 이를 위한 인력 양성 확보에 대한 중장기적인 교육 계획은 포함하지 않고 있다[19]. 그리고 정부에서 시행중인 정보보호 교육은 대부분 관련 자격증 취득을 위한 지식 습득의 교육 과정에 편중됨에 따라, 실질적인 전문가의 양성에는 한계가 있다. 이에 따라, 본 연구는 표준 프레임워크를 설계하는 과정에서 전 연령 대상의 정보보호 교육 접근성 향상과 각 직무별 전문성 강화에 중점을 두었다. 이는 단기의 정보보호 교육이 아닌 중장기의 관점에서 국민이 지속적인 정보보호 교육 수강을 위한 다양한 교육 프로그램 제공 개발 및 운영과 관련된 정책의 추진 필요성을 시사한다.

현재 국내 정보보호 관련 교육 과정의 공식화된 표준 커리큘럼의 부재로 상이한 교육 프로그램임에도 불구하고 중복된 교육으로 인한 강의 비효율성, 검증되지 못한 부실한 교육 내용에 따른 수강생의 불만족 등의 문제가 발생한다. 이를 해결하기 위하여 국내 정보보호교육에 대한 총괄 기관 혹은 전담 부서의 설치를 통하여 체계적인 교육 운영 관리 및 강의 평가 등이 이루어질 필요가 있다. 나아가, 정보보호 관련 교육에 대한 업무 종사자의 수강 부담을 완화하기 위하여 국가 차원의 무료 혹은 실비 제공의 교육이 이루어질 수 있도록 정보보호 관련 예산 정책이 개선될 필요가 있다.

포스트 코로나 시대 도래에 따른 ICT 기술의 의존성 증가와 급변하는 보안 위협에 대처하여 국가 경쟁력 확보를 위해서는 일부 연령대 혹은 관련 직무 담당자만을 대상으로 이루어져서는 국내 사회의 정보보호 역량 강화를 유도하기에는 한계가 존재한다. 이러한 한계점에 착안하여 본 연구는 정보보안에 대한 국민 전체의 인식을 제고하여 국내 사회 전반의 정보보호 문화 형성 조성 방안을 정보보호 교육 전략을

통하여 제시하였다. 이에 본 연구에서 제안한 국내 정보보호 교육 표준 프레임워크를 기반으로 중장기 관점에서의 정보호호 교육 정책의 추진 필요성을 시사하였다. 이를 위한 구체적인 전략으로 국내 정규교육기관의 정보보호 관련 설치 교과목, 관련 학과에 대한 재검토와 다양한 학위 운영 과정 개설, 교육 프로그램의 확대 설치 등의 방안에 대하여 논의하였다.

본 연구는 국내·외 대표적인 정보보호 교육 과정의 분석을 통하여 표준 교육 프레임워크를 제시하였으나, 향후에는 산업보안 등 세분화된 보안 분야별 교육 과정에 대해서도 지속적으로 강구되어야 할 필요가 있다. 또한, 본 연구에서는 미국 NICE의 Workforce Framework를 바탕으로 정보보호 교육 표준 프레임워크의 직무를 주로 분류하였다. 직무를 분류하고 이에 따라 요구되는 교육 과정을 구성하는 단계에서 본 연구는 국내 대학 등의 정규교육과정에서 이루어지는 정보보호 커리큘럼과 공공기관의 교육 이수 체계를 반영하였으나, 국내 환경과 정보보호 관련 법률 체계는 미국과 상이하다는 점에서 향후, 연구에서는 국내 환경의 상세한 특징이 추가로 적용되어야 한다. 특히, 직무 유형을 단계적으로 구성하여 분류하는 표준인 국가직무능력표준(NCS, National Competency Standards)은 국내에서 널리 활용됨에 따라, NCS의 분류체계를 본 연구에서 제안한 정보보호 교육 표준 프레임워크에 반영할 필요가 있다. 이는 국내 정보보호 법률에 대한 이해와 국내 업무 환경에 대한 조직적 특징을 반영하여 정보보호 수강생이 교육을 통하여 본인 직무에 맞춤화된 교육 내용을 습득하여 이를 업무 환경에 바로 반영 가능하도록 하기 위함이다.

국내 정보보호 교육 운영의 정착과 활성화를 통하여 정보보호 전문 인력 양성과 더불어 국내 정보보안 경쟁력 확보가 가능할 것으로 예상된다.

References

[1] Ministry of Science and Technology Information and Communication and National Information Society Agency, “2020 yearbook of Information Society Statistics,” Mar. 2020

[2] Jung, Jinhyo, and Chang-Moo Lee. "An Analysis of Industrial Security Curriculums in Colleges," *Journal of Society for e-Business Studies* 24(2), pp. 29-53, May. 2020

[3] Kim, Min-Jeong, et al. "A Study on the Curriculum of Department of Information Security in Domestic Universities and Graduate Schools and Comparison with the Needs of Industry Knowledge." *Journal of The Korea Institute of Information Security & Cryptology,* 24(1), pp. 195-205, Feb. 2014

[4] Park, Wonhyung, and Seongjin Ahn. "Enhancing education curriculum of cyber security based on NICE," *KIPS Transactions on Computer and Communication Systems,* 6(7), pp. 321-328, June. 2017

[5] Ahn, Byunggoo, Harang Yu, and Hangbae Chang. "A Research on Activating Factor for Cultivating a Proactive Organizational Security Culture," *Convergence Security Journal* 20(2), pp. 3-13, June. 2020

[6] Yim, Myung-Seong. "Why Security Awareness Education is not Effective?," *Journal of digital convergence,* 12(2), pp. 27-37, Feb. 2014

[7] Kim, Choungbae. "An Analysis of Information Security Curriculum in Elementary School practical arts, Secondary School Informatics Teaching and Suggestions for Improvement," *Journal of the Korea Society of Computer and Information,* 25(10), pp. 69-75, Oct. 2020

[8] Jung-Yoon Yum and Se Hoon Jeong, "Effect of privacy protection intervention effect targeting early teenagers: Focusing on parent-mediated intervention," *Journal of Cybercommunication Academic So-*

ciety, 36(2), pp. 43-80, June. 2019

[9] Seo, Hyun-Jeong, and Seong-Sik Kim. "The Effect on Information Communication Ethics of Experience Type Smart Learning Contents Application for High School Information Security Education," *The Journal of Korean Association of Computer Education,* 19(6), pp. 81-89, Nov. 2016

[10] Lee, Chi-Seok, and Yanghoon Kim. "An analysis of relationship between industry security education and capability: Case centric on insider leakage," *Journal of Society for e-Business Studies* 20(2), pp. 27-36, May. 2015

[11] Kim, Bo-ra, Jong-Won Lee, and Beom-Soo Kim. "Effect of Information Security Training and Services on Employees' Compliance to Security Policies," *Informatization Policy,* 25(1), pp. 99-114, Dec. 2018

[12] Bahasoan, Awal Nopriyanto, et al. "Effectiveness of online learning in pandemic COVID-19," *International journal of science, technology & management,* vol. 1, no.2, pp. 100-106, July. 2020

[13] Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman. "Ten deadly cyber security threats amid COVID-19 pandemic," Dec. 2020

[14] Yang, Jeongmo. "A Study on Development of Standard Modeling Education Program in Information Security: Focusing on Domestic University Cases." *Convergence Security Journal, I*8(5_1), pp. 99-104, Dec. 2018

[15] Tae-Sung Kim, Min-Jeong Kim, and Jong-Ha Kim, "A study on fostering information security personnel through regular educational institution," *Journal of The Korea Institute of Information Security & Cryptology,* 14(4), pp. 78-91, Aug. 2004

[16] Best of Best (BoB), "BoB" https://www.kitribob.kr/learn/curriculum, Accessed: Aug. 2021. [Online].

[17] K-shield, "K-shield" http://kshieldjr.org/hr/home?custom=&year=2021&lastLoginTime=&isCmpt=false, Accessed: Aug. 2021. [Online].

[18] Ryu Haneul, et al. "Implementation of Flexible Test Bed for Cyber Attack Prediction and Countermeasure," *The Journal of Korean Institute of Communications and Information Sciences,* 44(9), pp. 1723-1729, Sep. 2019

[19] Kim, Dong-woo, 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, June. 2013

[20] Liu, Taikang, and Yongmei Li. "Standard Study of Electromagnetic Information Leakage and Countermeasures," *Electromagnetic Information Leakage and Countermeasure Technique. Springer,* Singapore, pp. 217-230, May. 2019

[21] Seongjin Ahn and KyungSun Oh, "Domestic and Foreign Comparative Analysis of The Information Security Curriculum," *In Proceedings of* Korean Association of Computer Education, 17(2), pp. 15-20, Aug. 2013

[22] Yang, J. M., et al. "A study on analysis and development of education program in information security major." *Journal of the Korea Institute of Information*

Security and Cryptology, 13(3), pp. 17-26, Feb. 2003

[23] Internet Trend Research, KISA Report, Feb. 2012

[24] Lim, Wongyu, and Seongjin Ahn. "A Study on Improvements of the Information Security Department via the Curriculum Analysis," *The Journal of Korean Association of Computer Education* 17(6), pp. 71-80, Nov. 2014

[25] Chul Kim, "Research on the development of information security curriculum in universities," *Review of KIISC*, 11(3), pp. 75-89, June. 2001

[26] Herath, Tejaswini, and H. Raghav Rao. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems,* vol. 47, no.2, pp. 154-165, May. 2009

[27] Safa, Nader Sohrabi, and Rossouw Von Solms. "An information security knowledge sharing model in organizations," *Computers in Human Behavior,* vol. 100, no.57, pp. 442-451, April, 2016

[28] Minjung Park and Sangmi Chai, "Comparing the effects of two methods of education (online versus offline) and gender on information security behaviors," *Asia Pacific Journal of Information Systems*, vol. 30, no.2, pp. 308-327, June. 2020

[29] Öğütçü, Gizem, Özlem Müge Testik, and Oumout Chouseinoglou. "Analysis of personal information security behavior and awareness," *Computers & Security,* vol. 56, pp. 83-93, Feb. 2016

[30] Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly,* vol. 34, no.3, pp, 523-548, Sep. 2010

[31] Hina, Sadaf, and P. Dhanapal Durai Dominic. "Information security policies' compliance: a perspective for higher education institutions," *Journal of Computer Information Systems.* vol. 60, no.3, pp. 1-18, Mar. 2018

[32] Minjung Park and Sangmi Chai, "Internalization of information security policy and information security practice: A comparison with compliance," *In Proceedings of the 51st Hawaii International Conference on System Sciences.* pp. 4723-4731, Jan. 2018

[33] Johnston, Allen C., and Merrill Warkentin. "Fear appeals and information security behaviors: An empirical study," *MIS quarterly,* vol. 34, no.3, pp. 549-566, Sep. 2010

[34] Jae-yong Park, "An analysis on training curriculum for educating information security experts," *Management & Information Systems Review* 31(1), pp 149-165, Mar. 2012

[35] Ki-Yoon Kim and Ken Surendran. "Information security management curriculum design: A joint industry and academic effort," *Journal of Information Systems Education,* vol. 13, no.3, pp. 227-237, Sep. 2002

[36] Eun-ju Lee et al. "Development of Information Security Education Framework for Information Security Employees: A Case of Educational Institutions," *The Journal of the Korea Contents Association* 14(1), pp. 386-399, Jan. 2014

〔37〕 Newhouse, William, et al. "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," *NIST special publication* 800, pp. 181, Aug. 2017
〔38〕 Nerantzi, Chrissi. "The use of peer instruction and flipped learning to support flexible blended learning during and after the COVID-19 Pandemic," *International Journal of Management and Applied Research* 7(2), pp. 184-195, vol. 7, no.2, July. 2020
〔39〕 Hwang, Gwo-Jen, Chiu-Lin Lai, and Siang-Yi Wang. "Seamless flipped learning: a mobile technology-enhanced flipped classroom with effective learning strategies," *Journal of computers in education,* vol. 2, no.4, pp. 449-473, Aug. 2015
〔40〕 Pemble, Matthew. "Balancing the security budget," *Computer fraud & security,* vol.10, pp. 8-11, Oct. 2003

〈저자소개〉

박 민 정 (Minjung Park) 정회원
2014년 8월: 성신여자대학교 법학과 졸업
2016년 8월: 이화여자대학교 빅데이터분석학 석사
2021년 2월: 이화여자대학교 경영학과 박사
〈관심분야〉 개인정보보호, 정보보안, 블록체인

이 기 혁 (GI Hyouk Lee) 종신회원
1988년 8월: 한양대학교 학사
1990년 2월: 한양대학교 공학 석사
2008년 2월: 건국대학교 공학 박사
2015년 8월~현재: 중앙대학교 융합보안학과 교수
〈관심분야〉 정보보호, 정보보호교육, 산업보안, 융합보안, 보안 거버넌스 등

채 상 미 (Sangmi Chai) 정회원
1999년 2월: 이화여자대학교 학사
2002년 8월: 서울대학교 경영학과 석사
2009년 6월: SUNY at Buffalo 경영학 박사
2012년 3월~현재: 이화여자대학교 경영학과 교수
〈관심분야〉 IT와 조직 및 전략, 정보보안과 조직 및 정책, 개인정보보호법 및 제도, 블록체인 등