박사학위논문

하이브리드 블렌디드 실천모형 기반의 초등 정보보안 핵심원리 교육 프로그램 개발과 실증

Development and Demonstration of Elementary School Information Security Core Principle Education Program based on Hybrid Blended Practice Model

제주대학교 대학원

융합정보보안학협동과정

정 유 진

2022년 2월

하이브리드 블렌디드 실천모형 기반의 초등 정보보안 핵심원리 교육 프로그램 개발과 실증

지도교수 변 영 철
지도교수 박 남 제

정 유 진

이 논문을 융합정보보안학협동과정 박사학위 논문으로 제출함.

2021년 12월

정유진의 융합정보보안학협동과정 박사학위 논문을 인준함.

심사위원장	이 은 주	㊞
위 원	주 연 수	㊞
위 원	김 인 중	㊞
위 원	변 영 철	㊞
위 원	박 남 제	㊞

제주대학교 대학원

2021년 12월

Development and Demonstration of Elementary School Information Security Core Principle Education Program based on a Hybrid Blended Practice Model

Yujin Jung
(Supervised by professor Yung-Cheol Byun)
(Supervised by professor Namje Park)

A thesis submitted in partial fulfillment of the requirement
for the degree of Doctor of Philosophy in Convergence
Information Security

2021. 12.

This thesis has been examined and approved.

Eunju, Lee

Thesis director, Yung-cheol Byun, Prof. of Computer Engineering
Thesis director, Namje Park, Prof. of Elementary Computer Education

Yeon-soo, Joo

InJung, Kim

Yung-Cheol, Byun

Namje, Park

2021. 12.

Department of Convergence Information Security
GRADUATE SCHOOL
JEJU NATIONAL UNIVERSITY

목 차

표 목 차

그 림 목 차

요 약

정보 시스템의 발전은 첨단 정보통신기술(ICT) 플렛폼과 맞물려 현대 사회를 디지털 전환의 시대로 이끌어나가고 있다. 이는 점차 현대사회가 고도화된 내용의 정보화 사회로 변환하고 있음을 의미한다. 정보의 가치가 높아지면서 이를 이용한 부당한 이익을 챙기려는 해커의 기법은 세분화되고 고도화되고 있지만 정보 사회의 구성원으로서 정보윤리와 정보보호의 필요성이 요구되는 만큼의 교육은 이루어지지 않고 있다. 사회의 변화 분위기 속에서 2015 교육과정에서는 정보교육을 필수 교과목으로 지정하여 일정 시간 이상을 필수로 이수하도록 개정되었고, 점차 발전해 나가는 미래 사회에 맞춘 인재를 양성하기 위해서는 정보교육 과정의 중요성이 점차 증대할 것으로 보인다. 하지만 현재 정보교육은 창의적 체험 활동 시간에 학교나 교사 재량에 의해 운영되고 있다. 정규 교과의 부재로 인해 교사 입장에서도 학생들의 정보보안 실천을 위해 무엇을 가르쳐야 하는 지에 대해 알기 어렵기 때문에 정보보호 교육은 네티켓(Netiquette) 중심의 정보 윤리 교육으로 한정되어 있기도 하다[1]. 특히 초등학생의 경우에 인터넷 이용률은 매우 높아지고 있으며, 초등학생에 대한 사이버 범죄가 급증함에 따라 초등학생에게도 정보보호 교육의 필요성이 높아지고 있다. 정보보호나 보안에 대한 인식이 취약한 초등생들의 경우에 쉽게 자신뿐만 아니라 주변인의 정보를 타인에게 알려주고, 아무런 죄의식도 없이 남의 정보를 가져다 악용하는 일이 발생하고 있다. 따라서 사이버 범죄로부터 초등학생을 보호하고 예방하기 위해서는 정보보안에 대한 교육이 절대적으로 필요하다는 것이 국가적인 관점에서의 공통적 의견이다[2].

이러한 실정 속에서 초등학생에게 정보보안 교육을 위해서 전문적 지식 등을 전달하는 전문 정보교육은 학습자의 학습 성취도를 낮추게 되는 원인이 될 수 있기 때문에 쉽게 접근할 수 있는 교육 프로그램을 구상하여 적용하였다. 본 논문에서는 총 세 개의 교육 프로그램을 개발하고 실증하였으며, 첫 번째는 초등학생들의 정보보안 교육의 이해 수준을 고려하여 게임을 하면서 자연스럽게 정보보안의 개념 등을 익힐 수 있는 게이미피케이션을 도입한 블록체인 기술의 핵심 원리를 파악할 수 있는 학습 교구를 개발하였다.

두 번째로 많은 청소년의 주요 관심사인 해킹 원리의 학습을 위해 학습자가 공격과 방어의 시나리오를 구상하고 보드 게임안에서 경험해 보아 자연스럽게 네트워크 해킹의 전문 용어 및 핵심 기술 등을 학습할 수 있도록 하였다. 또한 이는 학습자 스스로가 정보를 보호할 수 있는 능력 함양을 할 수 있도록 기술적인 부분을 보다 쉽게 접할 수 있는 시나리오 기반 교육 프로그램이다. 이 교육 프로그램은 네트워크 환경에서 적용되는 보안장비의 역할을 수행하는 패널들을 구성하여 공격을 수행하도록 함으로써 학습자에게 네트워크에서 적용될 수 있는 보안장비의 역할을 이해하도록 도움을 주어 학습자의 컴퓨팅 사고력을 강화하는 것을 목적으로 한다.

세 번째는 미래 신기술 중 하나이며 우리 사회에 매우 친숙하고 깊숙이 연관있는 지능형 CCTV의 안면인식 기술을 사이버보안 포렌식 기법과 접목하여 복잡한 상황의 숨겨진 이슈를 그림, 스케치, 상징이나 부호, 아이콘 등을 이용해서 이미지로 표현하고. 그래픽 퍼실리테이션(Graphic Facilitaion)을 이용해 찾아내는 리치픽처(Rich Picture) 기법을 활용하여 학생들로 하여금 어려운 원리에 쉽게 접근해 볼 수 있도록 구상하였다.

초등학생에게 안정적인 교육을 위해서는 앞서 언급한 것과 같이 교수자, 즉 현장 교사의 정보보안에 대한 올바른 개념과 어려운 원리에 쉽게 접근할 수 있는 교육이 수반되어야 할 것이고, 이를 위해서는 학교 관리자의 인식과 의지등에 따라 학교 조직의 전망과 목표가 달라지게 되고, 이는 학교 전체의 교육 문화에 영향을 미치게 되는 만큼 학교 관리자의 인식 변화 및 역량 함양이 우선 필요하다[3][4]. 학교 관리자의 역할은 교육 전체의 커리큘럼 구성뿐만 아니라 예산 및 행정 지원까지 포괄하는 학교 운영 전반의 광범위한 권한을 행사하며 학교 환경에서 교육 구현에 상당한 영향을 미치고 있다고 볼 수 있기 때문이다[5].

본 논문에서는 초등학생의 정보보안 교육의 중요성을 통감하여 학교에서의 정보보안 교육을 위해 교과서 수준에는 미치지 못하지만, 대체 교과 정도 수준에서라도 어려운 개념을 쉽게 파악하고 정확하게 인지하며, 스스로의 정보를 지킬 수 있으며 추후 나아가 정보보안 전문가 인재가 될 수 있는 방향성을 제시할 수 있도록 구상하였다. 앞서 언급한 바와 같이 본 프로그램은 초등학생 현장 교육뿐만 아니라 학교 교원연수와 관리자 연수를 통하여 일차적으로 교수자의 역량 강화

를 위한 프로그램으로 구상하였다. 해킹 원리 교육 프로그램의 효과성을 분석하기 위하여 학교 관리자를 대상으로 연수를 구상하고, 총 69명의 교장이 2회에 걸쳐 총 3차시 교육 연수에 참여하였다. 그 결과 4.87의 높은 만족도를 기록하였으며 FGD(Focus Group Discussion) 분석 결과는 해킹 원리 교육이 학교 현장에서 얼마나 필요한지를 보여주었다. 3차시로 구성된 안면인식 기술 원리 교육 프로그램은 현장 교원에게 다양한 교수학습자료를 제공하고 교수할 수 있는 연수를 운영하였으며 총 46명의 교원이 참가하였다. 총 2회에 걸친 연수를 통해 효과성 분석을 통하여 다양한 기술적 지식과 흥미로운 방식의 수업 설계로 향후 교육 프로그램을 고도화할 수 있는 유의미한 결과를 얻었다. 블록체인 핵심원리 교육은 온라인과 오프라인 수업 환경에서 모두 활용할 수 있도록 설계하였으며 전국의 초등학생 2학년부터 6학년 303명을 대상으로 교육을 시행하였다. 대응 표본 t-검정 결과 시행된 모든 항목에서 통계적으로 유의한 상승률을 보였다. 본 세 가지 교육 프로그램의 다양한 대상자를 통한 높은 만족도 등의 검증 결과는 본 연구가 초등학생을 대상으로 하는 사이버보안의 어려운 기술 원리 등을 여러 학습 도구를 통하여 쉽게 구상하여 학교 현장에 적용하는 것에 대한 향후 발전 가능성을 보여준다.

주요어 : 정보보안 기술 핵심 원리, 융합 교육, 해킹 원리학습, 블록체인 원리학습, 안면인식 기술, 사이버보안.

I. 서 론

1.1. 연구의 필요성 및 목적

최근 우리 사회는 코로나바이러스-19(Coronavirus: COVID-19)로 인한 언택트(Untact)기술의 수요 증가로 2010년대 초반 인공지능(Artifical Intelligence), 사물인터넷(Internet of Things), 클라우드(Clould) 컴퓨팅, 빅데이터(Big Data) 솔루션과 모바일(Mobile)의 통합된 형태로 나타난 블록체인 등 첨단 정보통신기술(ICT) 플랫폼의 발전과 맞물려 디지털 트렌스포메이션(Digital Transformation)으로의 변화를 앞당기고 있다[6]. 지속해서 언급되고 있는 4차 산업혁명에서 디지털 전환 시대는 다양한 분야에서의 ICT와 소프트웨어 기술이 접목되어 모든 것의 디지털화(化)를 의미한다. 우리나라는 COVID-19로 인한 경제 침체 극복 방안으로 2020년 5월 2차 비상경제 중앙대책본부 회의에서 한국판 뉴딜정책을 언급하였고, 7월 14일에 “한국판 뉴딜 국민보고대회”를 통해 3대 프로젝트를 포함 10대 중점 과제를 중심으로 추진 방향을 발표하였다.

한국판 뉴딜 추진 방향

3대 프로젝트		10대 중점 과제
디지털 인프라 구축	데이터 수집·활용 기반 구축	· 데이터 전 주기 인프라 강화 · 국민체감 핵심 6대 분야 데이터 수집·활용 확대
	5G 등 네트워크 고도화	· 5G 인프라 조기 구축 · 5G+ 융복합 사업 촉진
	AI 인프라 확충 및 융합 확산	· AI 데이터·인프라 확충 · 전 산업으로 AI 융합 확산
비대면 산업 육성		· 비대면 서비스 확산 기반 조성 · 클라우드 및 사이버 안전망 강화
SOC 디지털화		· 노후 국가기반시설 디지털화 · 디지털 물류 서비스 체계 구축

[그림 Ⅰ-1] 한국판 뉴딜 정책의 추진 방향[7]

정부는 디지털 뉴딜(Digital New Deal) 정책을 발표하며 교육 정책 분야 전반의 교육 인프라 디지털 전환을 위해서 모든 초·중등에 디지털 교육 인프라 조성 및 전국 대학·직업훈련기관의 온라인 교육 강화를 위한 움직임을 시작하고 있다.

D.N.A. 생태계 강화	교육인프라 디지털 전환	비대면 산업 육성	SOC 디지털화
① 데이터 구축·개방·활용 ② 전 산업 5G·AI 융합 확산 ③ 5G·AI 기반 지능형(AI) 정부 ④ K-사이버 방역 체계	⑤ 초중고 디지털 기반 교육 인프라 조성 ⑥ 전국 대학, 직업훈련기관 온라인 교육 강화	⑦ 스마트 의료·돌봄 인프라 ⑧ 중소기업 원격근무 확산 ⑨ 소상공인 온라인 비즈니스 지원	⑩ 4대 분야 핵심인프라 디지털 관리체계 구축 ⑪ 도시산단 공간 디지털 혁신 ⑫ 스마트 물류체계 구축

[그림 Ⅰ-2] 디지털 뉴딜 4대 분야 12개 추진과제[7]

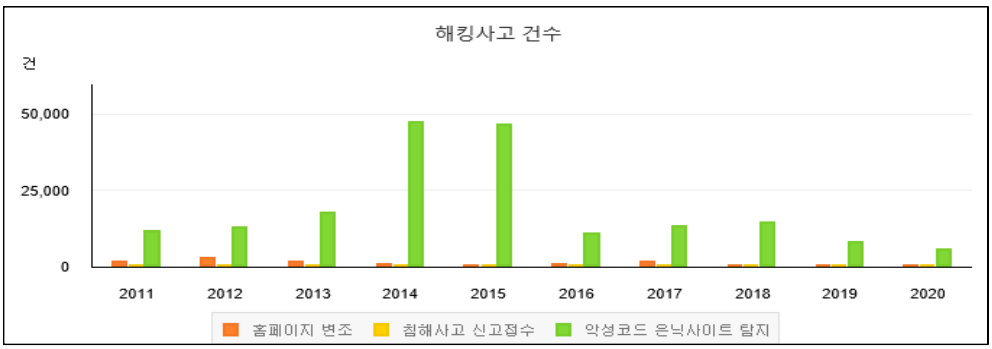
특히 디지털 뉴딜(Digital New Deal) 정책 중 교육 정책 분야는 교육 인프라의 디지털 전환을 위한 디지털 기반 교육 인프라 조성 및 온라인 교육 강화가 주 과제로 떠오르고 있다. COVID-19로 인한 비대면화 확산 및 디지털 전환 가속화 등 경제사회 구조의 대전환은 '디지털 역량'의 중요성을 재확인 시키는 계기가 되었고, 미래 교육 패러다임 변화에 대응한 원격 수업 가이드 라인을 마련하는 등의 정규수업으로 인정할 수 있는 법적 근거를 강화하였다[7].

OECD Education 2030 및 국내 미래 교육 관련 연구에서도 미래 교육은 현재 초·중등생이 성인이 되고 사회 구성원이 되었을 시점이다. 2030년에 학생들에게 필요한 능력이 무엇이며 학교 교육을 통해서 어떤 능력을 키워줄 것인지에 초점을 둔다. 이와 같은 사회의 변화는 지능정보사회의 도래로 인하여 산업구조와 일자리의 급격한 변화가 예측되고, 이는 구체적인 지식이나 기술을 직접 습득하는 구(舊)시대의 학습방식을 통해서는 미래 사회를 대비하기 어렵다는 것과 21세기 사회가 직면한 문제를 해결하기 위해서는 다양한 지식 영역을 넘나드는 융합적이고 창의적인 사고력과 실천력이 있어야 한다는 것에 기반한다.

이는 산업의 발전 속도가 점차 빠르게 진행되면서 단순한 기술 메커니즘에 다양한 알고리즘이 적용되고 있으며, 하나의 기기에 다수의 알고리즘이 적용됨에 따라 일반 사용자에게 편의성과 많은 이점을 제공하고 있다. 또한 이와 비례하여 기술의 복잡도 또한 나날이 변화하고 있는 사회 변화의 현상과 일맥상통하는 부분이며, 미래 서비스를 제공하기 위해서는 보다 다양한 지식을 실생활에 적용할 수 있는 방법이 요구된다는 것을 바로 보여주는 예이기도 하다.

결론적으로, 기술의 발전에 따라 학교의 교육제도 또한 변화하고 있고 특히 미래 사회에 발맞추어 학생들에게 더 다양한 관점에서 문제를 바라보는 시각을 제시하는 방향으로 발전하고 이는 현대 과학기술정보화 사회에서 제기되는 문제들은 융합적 지식과 사고, 다양한 관점이 상호 작용하는 구성원들의 협력에 의해 해결할 수 있으므로 융합 정보기술 원리교육을 접목한 교육 프로그램은 필연적으로 이어진다고 할 수 있다.

앞서 언급한 COVID-19는 정보화 사회에서 새로운 키워드를 양산하였는데 이는 2020년 초반 4차 산업혁명의 핵심 기술을 ABCD(AI, Blockchain, Cloud, Data)에서 CORONA(Cloud, On-demand, Remote, OTT, Network, AI)로 정리하는 데까지 이르렀다. 사회는 '전산화(Computerization)'와 '디지털화(Digitization)' 과정을 통해 새로운 생태계를 구축하기 시작하였고, 이에 따라 정보화 사회에서의 정보는 이전보다 훨씬 더 중요한 가치를 지니게 되었다. 정보를 사용하는 사용자나 정보를 제공하는 공급자의 처지에서도 컴퓨터를 사용하는 사람의 컴퓨터는 많은 개인정보를 저장하고 있고, 정보의 가치가 높아질수록 사회에서 컴퓨터를 활용한 생활이 다양화될수록 정보를 해킹하여 부당한 이익을 챙기려는 해커들은 더욱 기밀하게 움직이고 해킹 기법은 세분화·고도화되고 있다. 그러나 컴퓨터를 사용하는 연령대는 20대~40대에서 10대로 급속히 그 범위를 확장하고 있지만 모두 컴퓨터 전문가가 아닌 이상 해킹의 위협에서 벗어나긴 어렵다. 한국인터넷진흥원(KISA)에서는 해킹 공격 방법이 지능화·다양화됨에 따라 국내 침해사고 신고 접수 건수도 증가할 것으로 전망하였으며 2011년부터 2020년까지의 해킹사고 건수의 그래프를 [그림 Ⅰ-3]과 같이 발표하였다[8].



[그림 Ⅰ-3] 연도별 해킹사고 건수[8]

KISA의 지표 해석에 따르면 홈페이지 변조 사고의 경우에는 정치적·사회적 목적을 이루기 위해서 해킹을 하는 핵티비즘(hacktivism)의 공격으로 탐지 건수 증가하였으나 2018년에는 중소기업 웹 취약점 점검 및 보안 조치 강화 등으로 탐지 건수가 전년 대비 67.1% 감소하였고, 2020년에는 COVID-19로 인해 비대면 일상화에 따른 인터넷 이용 증가로 인해 약간의 증가가 보인다고 발표하였다[8].

침해사고 신고 접수 또한 해킹 공격 기법의 지능화·다양화로 인한 침해사고 발생 증가에 따라 지속해서 증가 추세이며 홈페이지 변조와 마찬가지로 COVID-19로 인한 인터넷 이용 증가로 침해사고도 증가하고 있다고 하였다. 가장 두드러지는 악성코드가 은닉되어있는 사이트 탐지 건수는 점검 대상 확대 및 유관기관 수집정보를 적용하는 등의 경우로로 인해 큰 폭으로 증가하였으나 2015년 이후 유포 방법이 달라지고 시스템의 고도화를 거치는 등의 노력으로 큰 폭으로 감소하였다. 2020년에 되어서는 홈페이지에 악성코드를 올려 이용자가 내려받길 기다리던 수동적 방식에서 적극적인 악성앱과 악성 이메일 등을 유포하는 등의 APT 공격으로 공격 방법을 다각화함에 따라 감소 양산을 띄고 있다고 분석하였다[8].

과거 지능정보 사회의 상호 연결성 등이 증가함에 따라 이전에는 보안 위협이 시스템에 피해를 끼쳐 사회 질서를 교란하는 정도였다면, 재택근무와 온라인 수업을 원활하게 가능하게 한 5G 네트워크 시대에는 그 영향의 범위가 실생활에 큰 영향을 줄 뿐만 아니라 인명피해까지 초래되는 등의 문제까지 매우 복잡하고 심각한 사회 문제로 대두되고 있다는 것이다.

앞서 원인으로 언급한 바와 같이 COVID-19 확산의 예방책으로 비접촉·비대면의 생활이 지속되면서 청소년의 인터넷 이용률은 일주일에 27.6시간을 사용하며 전년 대비 10시간이나 증가하였고 이는 사회적으로 인터넷 과다사용(중독), 인터넷 사용시간 통제 등에 의한 청소년 인권 침해 문제로 까지 점차 확대되고 있다[9].

청소년 통계 여성가족부 과학기술정보통신부·한국지능정보사회진흥원 인터넷 이용 실태조사(2021)에 따르면 청소년의 주 사용 목적이 비대면 수업으로 인한 교육과 학습이지만 인터넷 사용 시간이 증가가 청소년의 호기심과 맞닿아 청소년들의 혁신성은 보안 의식보다는 새로운 기술에 대한 호기심이나 열망, 체험에 더 집중되어 있음을 연구 결과를 알 수 있었다[10].

학교 성적 시스템을 해킹하거나 IoT 관련 장비 등을 해킹하여 피해를 입히는

등의 사이버 범죄를 저지르거나, 부모의 계정을 이용하여 불법사이트에 접속하고 정보를 노출해 보안의 위협을 받는 사례들이 뉴스를 통해 적지 않게 발표 되는 것만 보더라도, 청소년을 대상으로 한, 범위를 좀 더 좁히자면 초등학생을 대상으로 한 정보보안에 대한 교육이 반드시 필요하다고 볼 수 있다. 사회의 변화를 제일 먼저 감지하고 실생활에 자연스럽게 받아들이는 '디지털 네이티브(Digital native)' 세대인 초등학생의 경우에는 그 피해 규모가 파악되기도 전에 범죄와 범죄가 아닌 부분의 모호한 경계속에서 어떠한 가이드도 없이 그대로 노출되어있다.

무엇보다도 중요한 것은 청소년의 경우, 인터넷·모바일·지능정보기술 등을 일상적으로 접하는 환경에서 성장했고 디지털 공간이 사회화와 세계관 및 자아를 형성하는 데 있어 커다란 영향을 미치고 있기 때문에 기술에 대한 학습 없이는 그 피해는 늘어날 수밖에는 없다. 그럼에도 불구하고 정보보안 및 정보보안의 윤리 의식은 그에 맞추어 충분하게 형성되지 않은 상태이기 때문에 사이버 위험에 직접적으로 노출될 수밖에는 없는 것이다. 이러한 이유로 초등학생에게는 정보보안 교육이 특히 중요하지만 현재 한국의 정보보안 교육은 정보보호를 위한 사이버 공간에서 지켜야 할 에티켓, 윤리 의식교육을 중심으로 이루어지고 있으며, 기술 교육의 경우 전문 보안 인력 양성을 위한 고급 기술과 사이버 위협에 대응하기 위한 기술 중심으로만 대부분 이루어지고 있는 실정이다[11].

물론 초등학생에게 정보보안 교육의 당위성은 통감하고 있지만, 현실적으로 정보보안 교육을 할 수 있는 전문 인력과 전문 교육 커리큘럼, 프로그램들의 부재로 인하여 충분한 교육을 할 수 없는 학교 현장의 여건 또한 간과할 수 없는 중요한 사실이다. 많은 교과목을 교육해야 하는 학교 현장의 초등교사가 정규 교과목이 아닌 정보보안 교육을 위해서 연수를 받고 스스로 체득하여 정규 수업 시간에 적용한다는 것은 거의 불가능한 일처럼 보인다. 다시 말하면 초등교사에게 정보보안 교육을 할 수 있는 교재·교구 커리큘럼이 잘 구성된 프로그램을 제공한다면, 정보보안 교육이 가능할 수 있다는 것이다. 이는 정보보안 교육이 비교과 활동으로 이루어지고[1], 일관된 교육체계 없이 단발적으로 이루어지고 있는 등 효과적인 교육의 수행까지를 기대하기 어려울지라도, 정보보안 교육의 학교 현장 확산을 위한 발걸음으로 충분할 수 있을 것으로 기대한다.

따라서 본 논문에서는 초등학생 학습자에게 어려운 기술 용어가 잔뜩 끼어 들

어간 전문 서적이나 컴퓨터 공학 전공자 수준에서 쓰인 관련 교재들을 활용한 것이 아닌 디지털 네이티브 세대를 위한 흥미롭고 쉬운 정보보안 교육 프로그램을 구상하고 초등 교원이 학교 현장에서 쉽게 활용할 수 있도록 온/오프라인 블렌디드 학습지 형식으로 제공하는 교구를 제작하고 제공하여 학교 현장에서 정보보안 교육의 안정적인 착근을 도모하였다. 본 연구는 정보보안의 중요성에 대한 인식을 높여 향후 개정될 정보보안 교육의 교육과정 편성 등에 활용될 수 있는 학습 과정을 제안한다.

1.2. 연구의 범위

본 논문의 연구 범위는 사이버 환경 특히 모바일 디바이스에서 정보보안이 정보의 검색과 수집 및 가공, 송·수신 중에 정보의 훼손 및 변조되고 유출되는 등의 경우를 방지하기 위한 관리 및 기술적인 방법을 의미하는 것으로 의미를 정리하고, 정보보안 교육에 접근하였다. 이는 공급자 측면에서는 내·외부의 위협 요인으로부터 네트워크, 시스템 등의 하드웨어·데이터베이스 그리고 통신 및 전산시설 등의 정보 자산을 안전하게 보호 및 운영하기 위함으로 사용자의 측면에서는 개인 정보 유출 및 남용을 방지하기 위한 것으로 정리할 수 있다. 초등학생에게 정보보안 교육을 위해서 기존의 전문적 지식 등을 전달하는 전문인을 위한 정보교육이 아닌 정보보안의 위협이 될 수 있는 상황에서의 시나리오를 구상하고 이를 리치픽처, 게이미피케이션(Gamification)과 같이 새로운 교수·학습법 등과 접목한 교육 프로그램을 제안한다. 관련된 정보보안 기술은 현대 사회에 많이 언급되는 기술과 청소년의 흥미도를 고려하여 해킹이라는 대주제 안에서 네트워크 해킹의 용어의 자연스러운 습득을 위한 사이버 공격 및 방어 기술의 해킹 원리 모델 학습, 블록체인의 위변조 방지원리의 이해를 위한 학습모델 그리고 안면인식의 기본 원리 습득을 위한 학습모델을 구상하여 적용하였다.

본 연구의 최종 목적은 초등학생을 위한 사이버보안 정보 융합교육 프로그램의 개발과 학교 현장에 안정적인 착근에 있기 때문에, 적용 범위를 초·중등 교원과 학교 관리자에게까지 확대하여 현장 착근에 다소 많은 시간이 걸리더라도, 단발적인 프로그램 운영이 아닌 안정적인 대체 교과로서의 면모를 갖추기 위해 노력하였다. 학생에게 교수를 하기 위해서는 현장 교사의 요구를 잘 반영하는 것이 중요하다는 것을 연수를 통해 확인하였으며, 연구 결과에 따라 현장 교사의 요구를 적용하여 쉽게 활용할 수 있는 워크시트 형태로의 교구재 개발에 초점을 맞췄다. 이는 COVID-19 상황에서 온/오프라인의 하이브리드 수업이 지속될 수 있다는 가능성을 배제할 수 없는 현 학교 상황과 상대적으로 디지털화가 원활하게 이루어지지 못한 벽지학교, 도서 학교, 접적지역 학교, 섬 학교 등 도서・벽지의 지역에서도 고사양의 컴퓨터나 장비 없이도 수업이 가능 할 수 있도록, 종이를 출력해서 수업에서 활용 할 수 있도록 구상하였으며, 온라인 환경에서도 수업에 원활한 활용을 위해 라이브-워크시트(Live Worksheets) 프로그램을 활용한 워크시트도 제공하였다.

II. 이론적 배경

2.1. 미래 ICT / 보안 패러다임의 변화

2.1.1. 미래 ICT 패러다임의 변화

4차 산업혁명은 독일의 국가 주도산업 정책에서 언급한 용어인 공장의 완전한 자동화를 뜻하는 인더스트리4.0에 기원을 두고 있다고 할 수 있다. 이를 위해서는 가상 공간인 디지털 세상과 물리 환경인 현실을 연결하는 가상물리시스템(Cyber Physical System: CPS)이 강조되는데, 가상 환경인 디지털 공간이 물리 환경인 실제 공장을 제어하는 기초가 되기 때문이다. 가상물리시스템을 다르게 표현하면, 디지털 전환(Digital Transformation)이라고 할 수 있다. 디지털 전환은 현실의 가상으로의 전환, 가상과 현실과의 연결을 의미한다[12].

디지털 전환으로의 변화가 급속화 되면서 CORONA(Cloud, On-demand, Remote, OTT, Network, AI)가 COVID-19 시대의 키워드로 자리 잡고 있다. 재택근무·화상회의·온라인 수업 등의 비대면 산업이 급성장하여 수요가 폭발하였고, 접속 공간은 오프라인에서 온라인으로 이동되어 전시장과 콘서트가 AR과 VR로 재탄생 되었다. 이뿐만 아니라 원격업무와 교육·의료 등 신성장 동력이 비대면 플랫폼 전통산업으로 확장하고 있다. 온라인 스트리밍 서비스 또한 무선 데이터의 60%가 동영상에 집중된 콘텐츠 시장의 다크호스로 자리를 매기고 있으며 이 모든 것이 가능하게 된 것은 동영상 트래픽의 급증으로 화질의 저하 문제가 생기고, 이러한 기술적 문제를 보완하기 위한 전송속도와 많은 양의 트래픽을 한번에 처리할 수 있는 5G의 네트워크 발전이 가능했기 때문이다[13].

여기에 디지털 기술의 변화에 따라 사람들의 일상생활 패턴의 변화에 맞추어 끊임없이 변화하고 있는 다양한 영역의 '융·복합'을 모색하는 양상으로 변화해 나아가고 있다. 이는 인공지능(AI)로 서비스를 제공하는 플랫폼의 모습을 갖추게 되었다. 융·복합이라는 용어는 이미 지난 세월 동안 정보통신기술(Information and Communications Technology: ICT) 부문의 주요 화두가 되었다. ICT는 IT

의 확장형 동의어에서 더 나아가 통합 커뮤니케이션의 역할과 원거리 통신, 컴퓨터와 컴퓨터 정보에 접근하여 저장하고 전송 및 조작할 수 있도록 하는 소프트웨어, 미들웨어, 스토리지, 오디오비주얼 시스템을 강조하는 용어이다. 다수의 ICT 분야 전문가들이 별개의 흐름으로 진화하고 있는 통신, 방송, 미디어, 컴퓨팅 등의 부분이 디지털 정보의 생성, 처리, 저장 분배라는 틀을 통하여 서로 간의 경계가 모호해질 것으로 예측하였다[14].

그러나 IPTV 케이블의 초고속인터넷 접속 서비스의 제공 등 융·복합의 초기 단계에서는 기존 개발자의 위상 변화나 서비스 혁신은 두드러지게 나타나지 않았지만, 컴퓨팅 부문의 발전과 인터넷의 진화, 이를 적극적으로 활용하는 새로운 개발자와 사업자들의 도전으로 부문 간 융합의 변화가 나타나기 시작했다.

ICT 패러다임의 변화는 각종 매체가 엔드유저(End user)에게 제공하는 정보인 콘텐츠(Content), 온라인에서 생산 · 소비 · 유통이 이루어지는 장소를 의미하는 플랫폼(Platform), 컴퓨터 간의 통신 기술인 네트워크(Network)와 전자기기를 통칭하는 디바이스(Device)의 각 부분 간 상호의존의 심화라고 할 수 있다[15].

먼저 콘텐츠를 살펴보면 인터넷상에서는 더 이상 사진, 서적, 음악, 동영상 등의 구분이 무의미하다는 것은 전제하고 모든 콘텐츠가 디지털화되면서 플랫폼 제공자에 의해서 이용자에게 제공된다.

플랫폼은 소프트웨어 기술을 보유한 ICT 기업이 주도권을 잡게 됨을 의미하는데 특히 소프트웨어기술력과 클라우드 인프라를 보유한 클라우드 서비스 제공자가 대표적인 플랫폼 제공자이다.

디지털 융합 시대의 네트워크는 인터넷망이다. 서킷(Circuit) 방식의 전화망과 같은 전통적인 네트워크는 네트워크 보유자가 자체적으로 이용자 식별 등의 지능적 서비스를 제공하지만, 인터넷의 경우에서는 아카마이(Akamai Technologies)와 같은 다양한 서비스 제공기업들이 서버 클러스터(Cluster)를 통하여 효율적인 트래픽 전송 및 보안 등의 네트워크의 다양한 기능을 경쟁 시장에서 제공한다. 이러한 지능형 네트워크 서비스 제공자도 일종의 플랫폼 제공자가 되기 때문에 사실상 분리는 어렵다. 디바이스 부문은 인터넷과 연결되고 iOS와 같은 범용 운영 체제를 갖춘 디바이스 내부의 소프트웨어 프로그램이 플랫폼과 연결되어 서비스를 완결한다. 애플(Apple)은 플랫폼 제공자이면서 디바이스 제공자인 대표적인 예이다[16].

2.1.2. 보안 패러다임의 변화와 중요성

C(Contents)-P(Platform)-N(Network)-D(Dvice)의 경계가 모호해지고 통합되는 양상을 띌수록 이러한 기술을 악용하여 기존 공격 수법을 더욱 정교하게 만들거나 과거에는 존재하지 않은 완전히 새로운 방식의 사이버 공격이 발생할 가능성이 커졌다.

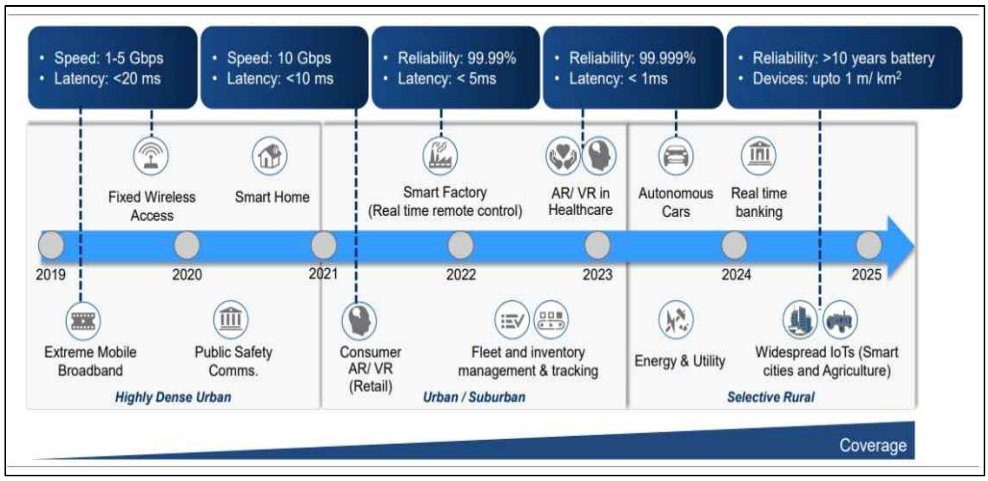
경제협력개발기구(OECD)에서도 디지털 시대의 신뢰를 위해서는 디지털 정보보안이 필수적이며 이를 위한 권장 사항을 제공하고 있다. OECD는 보안에 대해 혁신 및 성장을 지원하는 ICT의 잠재력을 저해하지 않으면서 신뢰를 강화하는 정책을 개발하고 촉진하는 것을 목표로 하여 사이버 정보보안 대신 디지털 정보보안이라는 용어의 사용을 권장하고 있다[17]. "디지털"이라는 용어는 디지털 경제, 디지털 변환 및 디지털 기술과 같은 표현과 일치하며. 이는 ICT로부터 신뢰를 증진하고 기회를 극대화하고자 하는 이해 관계자 간의 건설적인 국제 대화의 기반을 형성한다고 볼 수 있다고 설명하며 이는 디지털 정보보안이 순전히 기술적인 측면과 형법 집행 또는 국가 및 국제 정보보안과 관련된 것과는 대조적으로 사이버 정보보안의 경제적 및 사회적 측면을 나타내는 것을 의미한다고 설명하고 있다[17].

디지털 정보보안은 에너지 및 물 분배, 금융 서비스, 건강 관리와 같은 중요한 경제 및 사회 활동이 점점 더 디지털에 의존하고 있고 디지털 보안 위험이 증가하고 있음을 우려하고 있다. 디지털 정보보안의 사회적 관점은 사이버 리스크가 세계 경제에 영향을 미치고 있으므로 가장 중요한 시스템 문제 중 하나로 떠올랐다. 세계경제포럼(World Economic Forum: WEF)은 디지털 정보보안에 대한 글로벌 지출은 연간 107억 달러에 달하고, 2035년에는 1조 달러를 넘을 것으로 예상된다고 발표했다. 이러한 상황에서 세계경제포럼은 2019년 세계경제포럼 사이버안보 연차총회에서 제기된 보안 문제를 연구하기 위해 '미래 시리즈: 사이버 2025'를 발족하였고 이 시리즈의 하나로 세계경제포럼에서는 옥스퍼드대학의 글로벌 사이버보안역량센터(Global Cyber Security Capacity Centre: GCSCC)와 공동으로 주요 신흥기술의 미래를 전망하고 문제점을 진단하기 위한 연구 중 하나

로 '사이버보안, 신흥기술 미 시스템적 위험' 보고서를 발표하였다. 이 보고서에서는 사이버 공간의 변화를 촉진하는 대표적인 4개의 변혁적(變革的, Transformational)인 기술로 유비쿼터스 연결성(Ubiquitous connectivity), 인공지능(AI), 양자컴퓨팅(Quantum computing), 디지털 신원(Digital Identity)에 대한 미래 위험을 예측하고 해결 과제들을 제시하였다[18].

인터넷에 연결된 사물인터넷(IoT) 등을 통해 디지털화가 가속되면서 언제 어디서나 인터넷을 이용할 수 있는 유비쿼터스 연결의 시대가 가까워지며 고속의 안정적인 이동통신을 가능하게 하는 5G가 본격적으로 구축되었다. 이에 따라 네트워크 가상화, 에지 컴퓨팅(Edge computing) 등이 진화하고, 개인 맞춤형 네트워크를 향해 발전해 나아가고 있다[19].

새로운 네트워크와 데이터 분석 기술을 이용하여 기존의 물리적 세계에서 연결되지 않았던 기반 시설에 대해 보다 효율적이고 안정적인 통제가 가능해지고, 자율주행차나 드론 등의 상용화가 가까워지고 있음을 의미한다. 사회 전반에 모바일의 연결성이 확대되면서 다양한 개인, 기업과 사회의 활용이 증가하고, 새로운 무선 기술을 이용한 가치를 창출하여 공급망 관계가 변화하는 가운데 신기술의 출현과 도입의 가속화로 기기, 네트워크, 서비스가 초연결되며 상호 의존적이고 정교한 공유인프라가 실현된다면 경제사회 전반의 유비쿼터스 연결 시대를 맞이할 수 있다는 것을 의미한다고 볼 수 있다.



[그림 Ⅱ-1] 유비쿼터스 연결성과 활용 분야[20]

그러나 유비쿼터스 연결의 진화는 새로운 사업 모델을 만들어내면서 조직적인 정보보안 위험을 야기할 수 있고, 기술의 발전으로 초연결사회에 진입하면서 위험은 범위 등의 측면에서 심각성이 증폭될 수 있다. 대규모의 연결된 세계는 지능형 운송이나 의료수술 등에서 중요한 기능의 안전이 통신 시스템의 무결성과 가용성에 점점 더 의존하면서 통신 시스템에 대한 침해로 인해 인간의 안전을 위협하고 치명적인 사고를 초래할 수도 있다는 점도 매우 중요하다[21][22].

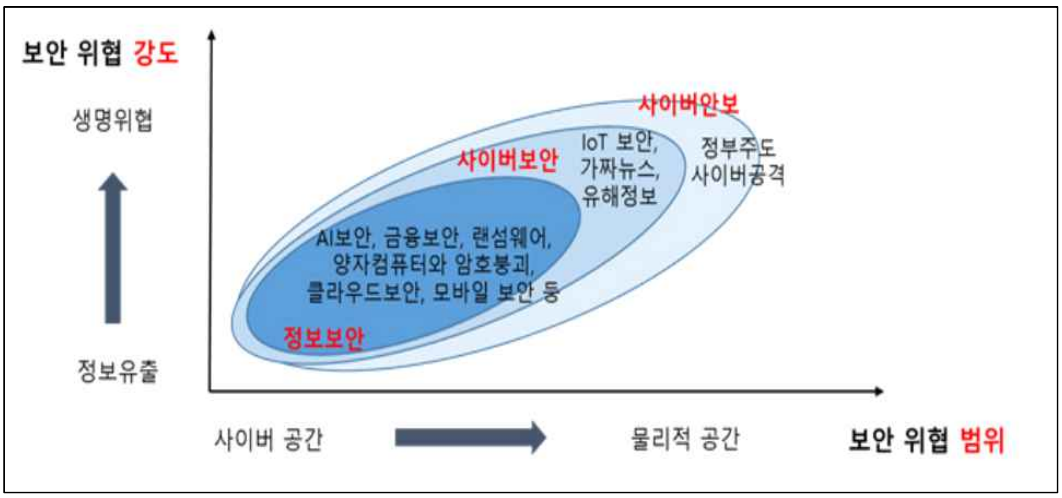
국제사회에서 공식적으로 보안취약점 관리정책의 필요성을 언급하고 설계 방향을 제시하기 시작했다. 2021년 2월 3일 OECD 디지털경제정책위원회(Committee on Digital Economy Policy)의 산하 보안작업반(Working Party on Security in the Digital Economy)이 취약점 공개정책(Vulnerability Disclosure Policies, VDP)의 상세한 요소와 절차를 담은 보고서를 발표하였다. 이미 2019년 OECD가 전 세계적으로 추진되고 있는 디지털 트랜스포메이션(Transformation)의 보안취약점이 위협될 것이라고 지적한 것과 일맥상통한다. OECD는 보안취약점에 대한 사회적 인식을 바꿔야 하며 각 정부 정책 관계자들이 보안취약점을 고려해야 한다고 강조했다[17].

한국인터넷진흥원(Korea Internet & Security Agency: KISA)의 요약본에 따르면 OECD는 “코드는 취약점을 포함하기 마련이고, 모든 스마트 제품은 코드를 보유하기 때문에 어느 정도 취약할 수밖에 없다”라며 “스마트 제품 취약점을 이용한 공격은 막대한 경제·사회적 비용을 초래할 수 있다”라고 지적한 것을 볼 수 있다. 사회는 ‘전산화(computerization)’, ‘디지털화(digitization)’의 과정을 통해 새로운 생태계를 구축하기 시작하였고, 이러한 경향은 최근 COVID-19사태로 인한 언택트(Untact) 기술의 수요 증가와 맞물려 점점 더 가속화하고 있다고 분석하였다[18].

디지털 전환은 다양한 분야에서의 ICT와 소프트웨어 기술이 접목된 모든 것을 일컫게 되면서 시대의 키워드가 산업화에 집중되었다면 현재에는 디지털화 즉 정보화에 보다 집중되고 있다는 것을 보여준다[13]. 정보화가 가속화되면서 정보화 사회에서의 정보는 이전보다 훨씬 더 중요한 가치를 지니게 되었다. 정보는 부와 권력을 얻을 수 있는 중요한 자산이기 때문이다. 이로 인하여 정보보안에 대한 중요성도 함께 주목받게 되었으며 최근에는 내부정보 유출 방지, 개인정보 보호, 개발 보안, 통합 보안관리 분야가 정보보안의 핵심 이슈로 떠오르고 있다.

정보보안은 미래에 대한 구상의 시작을 알리는 디지털로의 변화의 속에서 정보의 수집 및 가공, 송·수신 중에 정보의 훼손 및 변조되고 유출되는 등의 경우를 방지하기 위한 관리 및 기술적인 방법을 의미한다.

정보보안은 정보를 제공하는 공급자의 측면과 사용하는 사용자 측면에서 살펴볼 수 있다. 공급자 측면에서의 정보보안은 내·외부의 위협 요인들로부터 하드웨어 데이터베이스나 통신 및 전산 시설 등의 정보 자산을 안전하게 보호하는 것이고, 사용자 측면에서는 자신의 개인정보가 유출되거나 남용되지 않도록 정보를 보호하는 것을 의미한다. 다음 그림은 보안 패러다임의 변화에 대해 그 그림으로 나타낸 것이다.



[그림 Ⅱ-2] 보안 패러다임의 변화[23]

양·질적으로 변화하는 보안 위협에 대한 대응은 기존과 다른 방식으로 전개되어야 한다. 정보보안은 각종 위협으로부터 정보를 보호하는 것을 의미하고 과거의 정보 유출·훼손, 변조에 국한되었던 사이버 공격이 양자컴퓨팅의 등장과 랜섬웨어 보편화와 익명화, 블록체인의 취약점에 사이버 공격 그리고 인공지능 기술을 악용하는 사례까지 고도화되고 있다[23].

특히 블록체인(Blockchain) 기술이 전 세계 금융기관에서 사용하고 있는 SWIFT (Society for Worldwide Interbank Financial Telecommunication)을 표적으로 삼은 공격에 대비하기 위한 기술로 기대를 모으고 있으나, 최근 EU 산하의 정보보호기구 ENISA(European Union Agency for Cybersecurity)는 블록체

인이 기존 금융시스템에 적용된다고 하더라도 블록체인의 익명성을 이용하여 사기 거래, 자금세탁 이중 지급 등의 비정상 거래가 발생할 수 있기 때문에, 금융기관을 대상으로 하는 사이버 공격은 여전히 위협적일 것으로 전망하였고, 이는 블록체인 네트워크에 연결된 모든 컴퓨터가 공격 대상이 될 수 있어 대단위의 손해를 입을 수 있다고 하였다[24]. 이는 블록체인뿐만 아니라 기본적인 네트워크 보안이 중요하다는 것을 보여주는 예가 되기도 한다. 인공지능이 지능을 더 갖춰가면서 인공지능 기술이 피해자의 취약점을 찾아내고 정밀한 공격이 가능하도록 사이버 무기를 스스로 제작하는 등의 잠재력을 가지고 있기 때문에 이에 대한 대응책을 마련할 필요가 있다.

2.2. 디지털 네이티브 세대와 보안 트렌드

2.2.1. 모바일 디바이스의 발전과 디지털 네이티브 세대

사회가 발전함에 따라 전반적인 시민의식이 성장하고 있으며, 이 과정에서 개인정보에 대한 인식 수준이 높아지고 있다. 이로 인하여 일반인들 사이에서도 자신의 개인정보에 대한 경각심을 가지고 외부 유출에 민감해지고 있으며, 개인정보의 보호를 위한 보안의 중요성 또한 두드러지고 있다. 하지만 보안 인식에 대해 아직 미성숙한 청소년층에서는 보안의 필요성에 대해 이해하기 어렵다. 하지만 인터넷과 같은 스마트 미디어에 대한 접근성이 좋아지는 현재, 청소년층의 낮은 보안 인식은 청소년층의 개인정보 위협과도 직결된다[10].

하지만 단순히 보안의 인식 제고를 목적으로 청소년층에게 어색한 콘텐츠를 기반으로 교육을 진행하는 경우, 그 효과성이 절감될 수 있다는 문제가 있다. 따라서 디지털 네이티브 세대와 연관성이 높은 콘텐츠임과 동시에 보안 인식을 끌어올릴 수 있는 콘텐츠여야만 한다. 이러한 점에서 모바일 디바이스는 매력적인 콘텐츠이다. 모바일 디바이스에 대한 사용 연령층은 낮아지고 있으며, 가장 쉽게 접근할 수 있는 매체이기 때문이다.

정보통신정책연구원(2020)의 자료에 따르면 청소년층의 스마트폰 보유율이 초등 저학년을 제외하고 평균적으로 90%에 육박하는 것으로 확인되었다. 자료에 따르면, 초등 저학년 37.8%, 초등 고학년 81.2%, 중학생 95.9%, 고등학생 95.2%로 집계되었다. 그뿐만 아니라 만 6세 미만의 아동을 대상으로 스마트 미디어를 처음 접한 시기를 조사한 결과 약 45.1%의 아동이 만 1세 이상에서 처음 스마트 미디어를 접한 것으로 나타나 점차 사용 나이가 낮아지는 추세를 보인다. 이처럼 어린 시절부터 인터넷 환경에서 자라 디지털 기기의 활용이 자유로운 디지털 네이티브 세대는 개인용 PC, 스마트폰과 같은 스마트 미디어에 대한 노출이 일반적으로 이뤄질 수밖에 없다[25].

이와 같은 스마트 미디어는 사용자의 개인정보를 유출할 수 있다는 문제를 항상 동반하고 있으나 저연령층의 학생들은 이에 대한 인식이 어려워 문제가 발생

할 수 있다. 현대(Hyundai motor company)의 한 발표 자료에서는 청소년을 대상으로 개인정보 제공 시 사용하는 동의서의 내용에 대한 미확인 사유를 설문한 결과 70%에 육박하는 학생들이 내용의 확인이 귀찮거나 어려워서 확인을 하지 않은 것으로 나타나며 이 결과를 통하여 보안 인식 수준을 확인할 수 있었다[26]. 따라서 스마트 미디어에 대한 노출이 높아진 저연령층에 대한 보안 인식 제고를 위해 정보보안을 이해하고, 실천할 수 있는 교육이 요구된다.

2.2.2. 선제적 지능형 영상감시 기술

폐쇄 회로 텔레비전(Closed Circuit Television: CCTV)이라고도하는 비디오 감시 시스템은 공공장소, 공공 기반 시설, 상업용 건물 등을 포함한 다양한 설정에 광범위하게 배포되어있다. 대부분은 물리적 자산 및 공간의 실시간 모니터링과 수집된 비디오 정보를 검토하여 보안 지표 식별 및 보안 조치 계획이라는 두 가지 목적으로 사용되고 있다.

비디오 감시 시스템은 수십 년 동안 공공 및 보안 분야에 없어서는 안 될 부분이 되었고 공공 및 보안 분야 외에도 비디오 감시 시장의 지속적인 성장을 주도하고 있는 부분은 전 세계적으로 증가하는 범죄율과 보안 위협으로 인한 것으로 해석된다.

Mordor Intelligence의 최근 보고서에 따르면 비디오 감시 시장은 2016년에 299억 8,000만 달러였으며 2022년에는 721억 9,000만 달러에 이를 것으로 예상된다. 이 시장 잠재력은 또한 최근 IT 기술의 발전으로 추진되고 있는데 비디오 감시 시스템의 발전은 다음과 같은 기술 동향에 의해 주도된다[27].

우선은 지능형 및 상황 인식 비디오 데이터 수집이다. 최근 신호 처리의 발전은 지능형 비디오 감시 시스템, 특히 비디오 데이터 수집 속도를 유연하게 조정할 수 있는 시스템의 개발을 가능하게 하였고, 특히 보안사고의 지표가 감지될 때마다 데이터 수집 비율을 높여 보다 정확하고 신뢰성 있는 분석을 위한 충분한 정보를 제공한다.

두 번째로 빅데이터 인프라 구축이다. 최첨단 빅데이터 인프라는 빅데이터의 4V인 거대한 크기(Volume), 빠른속도(Velocity), 다양한 형태(Variety) 및 정확성

(Veracity)을 특징으로 하는 비디오 데이터 저장 및 액세스의 새로운 지평을 열었고, 수집률이 높은 스트리밍 데이터를 포함하여 여러 대의 카메라에서 방대한 양의 데이터를 수집하는 것이 과거보다 훨씬 쉬워졌다. 빅데이터 시스템은 원활하고 비용 효율적인 방식으로 확장되는 비디오 감시 아키텍처를 만들고 구현하기 위한 수단을 제공할 수 있기 때문이다[28].

세 번째로 데이터 스트리밍의 발전을 들 수 있다. 지난 몇 년 동안 많은 스트리밍 시스템이 등장했으며 이전에 논의된 빅데이터 시스템의 중요한 부분인 동시에 스팀 관리 및 스트리밍 분석을 위한 기능을 제공한다.

네 번째로 예측 분석 및 인공지능의 발전이다. 2016년과 2017년은 Google의 Alpha AI 엔진에서 사용된 것과 같은 딥러닝 접근 방식의 출현으로 인해 인공지능의 역사에서 중요한 해로 여겨진다. 심층 신경망의 진화는 비디오 감시 시스템에 직접 활용되어 뛰어난 지능을 부여하고 보다 효과적인 감시 프로세스를 가능하게 하였다. 예를 들어 AI는 예측 분석을 가능하게 하여 보안 운영자가 보안사고를 예측하고 사전에 대비할 수 있도록 할 수 있다.

다섯 번째 드론과 사물인터넷(IoT)의 혼합 IoT 디바이스 및 비디오 감시 시스템과 스마트 오브젝트는 보안 및 감시 기능의 차세대를 제공하는 실마리가 되었다. 이러한 방향으로 최근에는 기존의 고정 카메라로는 불가능했던 영상감시의 다양한 활용과 기능을 제공하기 위해 무인 항공기(Unmanned Aerial Vehicle: UAV)인 드론이 배치되고 있다.

산업 자산 및 프로세스의 지속적인 디지털 혁신은 점차 물리적 및 사이버보안 조치의 수렴으로 이어지고 있다. 비디오 감시 시스템은 물리적 영역을 모니터링하는데 사용할 수 있는 IT 인프라를 나타내기 때문에 이러한 통합에서 핵심적인 역할을 하게 된다. 따라서 보안 및 감시에 대한 총체적이고 통합된 접근 방식을 위해 다른 보안 시스템과 유연하게 통합될 수 있는 특징이 있다.

앞에서 나열된 기술은 지능형 비디오 감시 시스템의 개발, 배포 및 운영에 새로운 지평을 열어 주었다. 이를 위해서는 비디오 감시 인프라에 적합한 아키텍처를 고안하고 구현하는 것이 중요하다.

최신 비디오 감시 시스템 아키텍처는 에지(Edge)/포그(Fog) 컴퓨팅을 따르고. 이는 영상정보를 현장에 더 가깝게 처리하는 패러다임이다. 이를 통해 대역폭을

절약하고 실시간 보안 모니터링을 수행할 수 있으며, 카메라는 비디오 프레임을 캡처하고 처리할 수 있는 에지 노드(node)의 일부로 네트워크 에지에 배치된다.

에지 노드는 식별된 보안 컨텍스트를 기반으로 프레임 속도를 조정하여 데이터 수집 인텔리전스를 구현할 수도 있다. 또한 클라우드 인프라에 연결되어 여러 카메라의 정보가 더 거친 시간 규모로 연결, 검토 및 분석한다.

에지/포그 컴퓨팅 아키텍처는 비디오 감시와 제시된 기술의 결합을 지원하기 위한 이상적인 선택으로 여겨지기도 한다. IoT 드론은 모바일 에지 컴퓨팅 아키텍처의 일부로 적절한 에지 노드와 통합되어야 하고 실시간 스트리밍 분석은 비디오 감시 배포의 클라우드가 아니라 에지에서 수행되어야 하기 때문이다[29].

딥러닝 기능은 에지와 클라우드 계층 모두에 배포하고 에지의 심층 신경망은 실시간으로 복잡한 보안 패턴의 추출을 지원할 수 있다. 이는 도시 전체 배포와 같이 동시에 많은 에지 노드가 포함하는 넓은 영역의 보안 패턴 및 지식의 추출은 클라우드에서의 딥러닝 배포를 통해서만 가능하기 때문이다. 일반적으로, 일부 기능을 클라우드에 배치할지 에지에 배치할지 결정하는 것은 상당히 어렵다. 예를 들어 처리 속도 대 일부 감시 기능에 대한 처리 정확도에 대한 관련 결정은 일반적으로 절충안의 해결과 관련이 있다. 비디오 감시 시스템은 여러 하드웨어 공급업체의 개방형 아키텍처를 활용하고 이는 감시 솔루션이 다양한 비디오 캡처 장치와 방식인 고화질 카메라, 유무선 카메라, 드론과 UAV의 카메라 등으로 구성될 수 있기 때문이다.

개방형 아키텍처는 유연성, 배포 용이성 및 기술 수명을 제공할 수 있기 때문에 최근에는 포그 컴퓨팅의 주요 용도 중 하나로 비디오 감시를 제공하기 위해 에지/포그 컴퓨팅을 위한 개방형 표준 기반 아키텍처를 도입하려는 노력이 있어왔다. 이와 같은 기술 발전 속에서 당면한 과제는 적절한 에지 컴퓨팅 아키텍처의 사양 외에도 비디오 감시 시스템 배포자는 다른 문제도 해결해야 한다는 것이다.

이러한 과제 중 하나는 개인 정보 보호 및 데이터 보호 규정 준수와 밀접한 관련이 있다. 실제로 감시 센서의 배치는 개인 정보 보호 및 데이터 보호에 관한 법률 및 지침의 적용을 받으며, 이것은 배치의 성격과 규모에 제한을 준다. 마찬가지로 드론의 사용도 관련 규정을 준수해야 한다.

또 다른 문제는 솔루션의 자동화 수준과 관련이 있다. 자동화는 일반적으로 추

가 인적 자원 없이 더 넓은 영역을 다루고 모니터링하는 것이 바람직하지만 인적 검토와 개입은 여전히 전체 솔루션의 신뢰성 핵심이다.

또한, 비디오 감시 시스템의 사이버 물리적 특성에서 비롯될 수 있는 새로운 위협과 관련된 또 다른 문제가 있는데, 물리적 보안 사고를 감지하는 비디오 감시 인프라의 능력을 훼손하는 수단으로 물리적 공격은 비디오 감시 인프라에 대한 사이버 공격을 동반할 수 있다는 점이다.

또 다른 과제는 데이터 기반 인텔리전스로 예측 분석 및 AI의 일부인 구현과 관련이 있다. 이 기술에는 거의 사용할 수 없는 보안사고와 함께 대량의 데이터가 필요하다. 에지에서의 AI는 가볍고 효율적인 심층 신경망으로 발전을 해야 하지만 에지 AI 제품 및 서비스를 제공하는 혁신적인 신생 기업의 등장에도 불구하고 아직 초기 단계에 있다. 이러한 문제에 대처하기 위해 비디오 감시 솔루션의 개발자와 배포자는 표준 및 규정을 더 잘 준수하는 동시에 점진적/단계적 배포 접근 방식을 채택해야 한다. 즉 작업자 중재 시스템에서 AI 기반의 완전 자동화된 시각적 감시로 원활하게 전환할 수 있어야 한다.

간단한 규칙에서 시작하여 더 복잡하고 비대칭적인 공격 패턴을 탐지할 수 있는 보다 정교한 기계 학습 기술로 옮겨가는 데이터 기반 인텔리전스의 점진적 배포도 필요하다. 그리고 비용 대비 최고의 가치로 고급 기능을 활용하는 수단으로 미래 및 기존 감시 센서를 모두 수용할 수 있는 개방형 아키텍처를 배포하는 해야 하겠지만 전반적으로 인공지능 기반의 지능형 영상감시 기술은 선제적인 위험에서 매우 혁신적 미래형 첨단 사회 안전 시스템으로 발전할 수 있다[30].

[그림 Ⅱ-3] 지능형 영상감시 기술의 활용 예시[31]

2.2.3. 사이버보안 위협 및 공격 기법과 사이버 포렌식

지난해 국내·외에서 발생한 보안 이슈와 현장의 여러 사례를 분석하여 2021년 사이버보안 7대 트렌드가 선정되었다[32].

첫 번째로는 COVID-19 상황에서 원격근무가 확대되며 보안이 취약한 가정용 네트워크와 단말기를 통한 정보 해킹 시도가 증가하고 있다. 재택근무로 인한 기업 임직원의 스마트폰과 개인 컴퓨터에 대한 공격과 메신저와 영상회의 등의 업무지원 시스템을 통한 정보 유출 등이 큰 사회적 이슈로 대두대고 있다.

두 번째로는 글로벌 해킹 트렌드를 주도하는 랜섬웨어(Ransomware) 바이러스이다. 랜섬웨어는 컴퓨터 시스템을 감염시켜 접근을 제한하고 데이터 데이터 유출 협박, 협박을 통해 몸값(랜섬)을 요구하는 악성 소프트웨어로, 기존의 불특정 다수에 대한 공격에서 점차 특정 목표를 겨냥한 표적형으로 고도화되고 있다. 최근에는 다양한 변종이 출현하고 있고, 랜섬웨어를 서비스형으로 판매하는 사례가 발생하는 등으로 위협의 강도가 커지고 있다.

세 번째로는 AI 기술의 발전이 보안의 새로운 창과 방패로 떠 오르고 있다. AI 기술 발전은 보안 영역도 크게 변화시키고 있다. AI 학습을 통해 대량의 해킹 공격의 성공률을 높이고, AI를 활용한 영상과 음성 합성 기술을 이용한 딥페이크(Deep-Fake)의 정보 왜곡 및 조작 위험성이 더욱 높아졌다. 이를 방어하기 위해 AI 기반 멀티미디어 위·변조 검출 및 자동탐지 및 분석 기술이 발전하면서 AI를 기반한 공격과 방어에 대한 연구가 확대되고 있다.

네 번째로는 지능형 시스템을 갖춘 스마트팩토리가 확산하고 IoT와 5G의 도입으로 네트워크 연결성이 높아지면서 생산설비 및 제조공정의 보안 위협도 커지고 있다는 것이다. 지난해 해외에서 발생한 자동차, 석유 기업 대상 사이버 공격은 정보시스템(Information Technology: IT)을 넘어서 운영기술(Operational Technology: OT)과 산업제어시스템(Industrial Control System: ICS)의 보안 중요성을 각인시킨 대표적인 사례로 볼 수 있다.

다섯 번째로 데이터의 보호가 데이터 산업 활성화를 위한 필수 조건이 되었다는 것이다. 국내에서도 데이터 3법 개정과 마이데이터(My-data) 사업 활성화에

따라 데이터 보호를 위한 다양한 기술과 솔루션이 등장하고 있다. 특히 데이터 산업의 성공을 위해서는 기존의 정보 암호화뿐 아니라 개인정보의 안전한 유통 및 활용을 위한 비식별화 및 프라이버시 보호 기술이 필수적으로 거론되고 있다.

여섯 번째로는 클라우드(Cloud)의 보안 위협 부분이다. 클라우드 시스템의 단순 사고가 대규모 접속 장애 및 정보 유출로 이어지고, 클라우드 시스템만 전문적으로 공격하는 사례도 늘고 있다. 특히 대규모 시스템을 보유한 금융 ·공공 기관이 퍼블릭 클라우드를 이용할 경우에 보안 설정 및 접속 관리는 물론 인프라, 플랫폼, 소프트웨어 등 서비스별 철저한 보안 체계를 정립하는 것이 무엇보다 중요할 것이다.

마지막으로 의료 분야가 해커의 집중 공격 대상이 되고 있다. COVID-19 상황에서 의료기관, 제약회사를 대상으로 의료시스템, 의료정보, 백신 자료 등을 노리는 해킹과 랜섬웨어 공격이 집중되고 있다. 현재 운영 중인 시스템과 인프라부터, 솔루션, 정책까지 모든 보안 체계를 꼼꼼하게 점검하고, 체계적인 컨설팅을 통한 취약점 점검 및 대응체계의 수립이 반드시 필요한 이유이다.

보안 방법에 대해 언급하기 전에 우선 구체적인 해킹의 사례를 좀더 구체적으로 살펴보면 서드 파티 소프트웨어(Third Party SW)를 통한 공급망 공격이 증가한 것이 눈에 띈다. 올 상반기에는 기업에서 많이 쓰이는 중앙관리형 소프트웨어, IT 시스템, 단말기 등의 취약점을 악용한 '공급망 공격(Supply Chain Attack)'이 두드러지게 나타났다. 미국 주요 안보 기관과 보안 기업 등 1만 8,000여 곳을 공격한 네트워크 관리 솔루션 솔라윈즈 오리온(SolarWinds Orion)과 115개 이상의 국가에서 5,000개 이상의 피해를 유발한 마이크로소프트 익스체인지 서버(Microsoft Exchange Server) 프록시로그온(ProxyLogon) 취약점은 공급망 공격의 심각성을 드러낸 대표적인 예다[33].

또한, COVID-19 예방을 위한 재택근무 확산에 따라 가상사설망(VPN) 사용이 증가하면서 시트릭스 넷스케일러(CVE-2019-19781)나 펄스 시큐어(CVE-2019-11510) 등 VPN을 활용한 공격도 늘어났다. 국내에서도 VPN 솔루션의 관리자 페이지 접근 및 계정 변경 취약점으로 인한 정보 유출 사고 등에 대응할 수 있도록 보안 업데이트를 권고하고 있다. 이는 원격 액세스 인터페이스(RDP, SSH, VPN) 등을 교두보로 삼는 공급망 공격이 증가한 만큼, 전산 자원의 보안등급 재

산정을 통한 보안 거버넌스 수립이 요구된다[34]. 협력업체 및 상용 소프트웨어에 대한 검수와 관리 감독 체계를 통해 사이버보안의 복원력(resilience)을 강화하고 모니터링 및 사고 대응 체계를 구축하는 데 힘을 기울여야 한다는 것을 의미한다.

2021년 상반기에는 디지털 전환 가속화, APT 공격 그룹 간의 불법 정보 공유, 가상화폐 가치 상승의 영향으로 랜섬웨어 공격이 두드러졌다. 미국 바이든 대통령이 사이버보안 강화 행정명령(Improving the Nation's Cybersecurity)을 발표하게 할 정도로 전례 없는 대형 보안사고가 연속적으로 발생했다. 대형 송유관 업체 콜로니얼 파이프라인(Colonial Pipeline)을 공격한 다크사이드(DarkSide), 축산가공업체 JBS 푸즈(JBS Foods)를 공격한 레빌(REvil) 랜섬웨어 감염사고가 대표적이다[33].

대규모 랜섬웨어 감염을 주도하고 있는 공격 그룹들은 서비스형 랜섬웨어(RaaS)를 통해 월간 구독형, 범죄수익률 분배형, 일회성 랜섬웨어 라이센스 수수료 지불형 등으로 서비스를 다양화하면서 사이버 생태계의 무법자로 자리 잡고 있다. 공격 효과를 극대화해 범죄수익을 높이기 위해, 파일 암호화에서 나아가 주요 파일을 유출하고 정보 주체에게 정보공개를 빌미로 협상을 직접 시도하며, 분산서비스거부(Distributed DoS attack: DDoS) 공격을 시도하는 등의 다중 협박 전략을 취하고 있다[33]. 이와 같은 랜섬웨어로 인한 피해를 최소화하기 위해서는 랜섬웨어 위협에 유연히 대응하기 위한 보안 전략 수립이 요구되고, 해결책으로는 지속적인 데이터 백업 및 이중화, 접근제어 보안 강화(RDP, VPN 등) 전략을 토대로 랜섬웨어 감염을 예방하기 위한 사용자 행동 지침이 공유되고 주기적인 모의 훈련이 실행되어야 한다는 점이 언급되고 있다.

최근에는 특정 국가의 지원을 바탕으로 대규모 사이버 공격을 주도하는 사례들이 빈번히 발생하고 있다. 정치적·금전적 목적으로 의료, 언론, 국방, 외교, 안보, 보안 등 다양한 산업 분야를 대상으로 공격을 계속하고 있다. COVID-19 등 사회적 이슈를 이용한 사이버 공격 시도도 꾸준히 증가하는 추세다. 특히 올해 상반기에 발생한 국가 보안시설 해킹사고나 공급망 공격 등의 대규모 보안사고의 주체로 러시아, 북한 등이 지목되고 있다[35]. 이에 따라 미국 정부는 행정명령 발표를 통해 사이버보안 문제가 보안 영역을 넘어 국가 간의 외교 분쟁으로 이어질 수 있다는 점을 시사했으며 사이버 전쟁(Cyber War)에 유연히 맞서기 위

해서는 최신 사이버 위협 인텔리전스(Cyber Threat Intelligence; CTI)를 제때에 확인할 수 있는 위협 정보의 공유 체계와 사이버보안의 복원력(resilience)을 강화하기 위한 능동적인 대응체계가 마련되어야 한다.

COVID-19 대유행이 장기화하면서, 의료와 제약 분야를 대상으로 하는 사이버 공격도 꾸준히 발생하고 있다. 올 상반기에도 COVID-19 백신 제약 회사를 사칭하거나 COVID-19 연구 결과와 중앙재난안전대책본부, COVID-19 백신 업체 등 COVID-19와 관련된 키워드를 사이버 공격에 활용한 사례들이 연이어 포착됐다. Covidvirus, COVID-19, Pandemic 등 COVID-19 관련 키워드를 이용한 신규 도메인이 급증하고 악성 도메인 활용 비율이 급격히 증가했다.

국가기관 및 조직에서 획득한 중요 정보 및 개인정보를 빌미로 대가를 요구하고 협상에 응하지 않을 때는 다크웹을 통해 적극적으로 정보를 판매하는 행위가 증가했다. 국내에서도 다크웹을 통해 정보가 유출되고 이 정보를 악용한 크리덴셜 스터핑(Credential Stuffing) 및 스피어 피싱(Spear Phishing) 등의 추가 공격이 발생하는 사건이 일어나면서, 다크웹에 대한 경각심이 높아졌다. 실제로 다크웹을 통해 389억 건의 공공기관 도메인 메일 서비스 주소를 포함한 계정정보가 유출되고, E그룹의 카드 정보 200만 건을 탈취한 클롭(Clop) 랜섬웨어 공격 조직이 다크웹을 통해 일부 정보를 공개하며 협상을 유도하는 사건들이 일어났다[34].

또한, 민감정보와 개인정보와 함께 원격 제어 프로그램 접속 계정도 다크웹을 통해 활발히 판매되고 있어 문제가 되고 있다. SW 업데이트 서버 및 개발서버 등을 통해 악성코드를 유포하는 형태의 공급망 공격에 악용될 여지가 있으므로 예상 피해 범위를 추산하기 어려운 상황이다. 유출된 정보를 토대로 시도되는 사이버 공격에 맞서기 위해서는 조직 내 중요 유출 정보를 모니터링할 수 있는 위협 인텔리전스(Threat Intelligence) 확보, 주기적인 계정정보 변경 관리, 공격 표면(Attack Surface) 식별을 통한 보안 대응 체계 수립이 필요하다[34].

해커의 공격 위험에 대비하기 위한 보안취약점(Security vulnerabilities) 분석의 기술도 발전되어 왔다. 어느 분야에서든 약점에 대한 위험(risk)을 평가하는 것은 취약점을 찾는 것만큼이나 중요하다. 위험은 일반적으로 위협 모델링 (Theat modeling)이나 코드리뷰(Code review), 침투 시험(Penetration testing) 등의 방법을 통해 식별하는 것이 가능하고, 위험을 평가하기 위해 CVSS(Common

Vulerability Scoring System), CWSS(Common Weakness Scoring System)와 CWE/SANS Top 25 Most Dangerous Software Errors, The OWASP Risk Rating Methodology, DREAD model 등 다양한 보안취약점 평가 방법이 존재한다. 이를 위해 소프트웨어의 보안취약점은 미국 국립 표준기술연구소(NIST)를 비롯하여 소프트웨어 보안취약점을 다루는 각 벤더별로 그 취약점을 평가하기 위한 체계를 갖추고 있다. 이중 NIST의 지원을 받는 MITRE에서 관리하는 CVSS가 보안취약점 평가를 위한 표준으로 사용되고 있다[36][37].

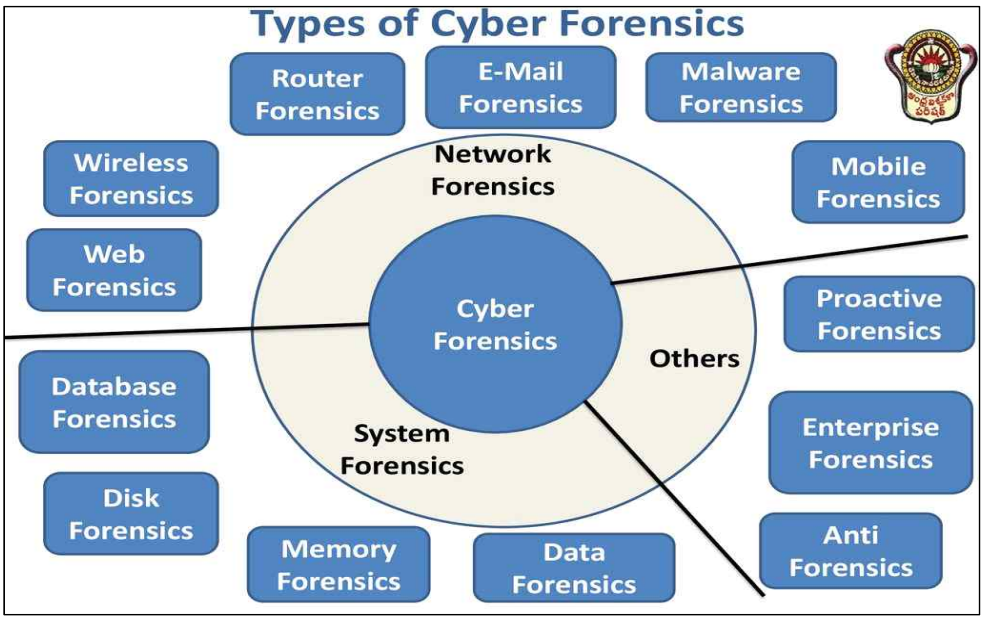
해킹 공격이 범죄에 일정 부분을 차지하고 있으며 이러한 해킹 공격을 수사하는 사이버 포렌식 기술도 점차 발전하고 있다. '사이버 포렌식(Cyber forensics)'이란 디바이스에 남아있거나 삭제된 데이터를 분석해 범죄의 단서를 찾아내는 수사 기법을 통칭하는 말이다. 범죄 현장에서 확보한 개인 컴퓨터, 서버 등의 시스템이나 전자 장비에서 수집할 수 있는 디지털 증거물을 수집, 확인, 식별, 분석, 기록, 재현 등의 과학적으로 도출하고 증명 가능한 방법으로 수행한다. 일례로, 태블릿PC나 노트북, USB 등에 있는 파일을 디지털 포렌식으로 복구하면서 스마트 기기가 범인의 것이라는 분석을 도출한 바 있다. 이처럼 디지털 포렌식 기술은 각종 사건·사고 수사에 사용되고 있다[38].

최근에는 모바일뿐만 아니라 스마트밴드, 스마트워치, 드론 등 디지털 포렌식 대상 기기가 늘어나고 있다. 우선 스마트밴드를 통해 사망 시각과 장소를 추정할 수 있다. 스마트밴드는 심박수, 건강정보, 위치 및 활동 정보를 수집하기 때문에 사건·사고의 객관적 증거가 될 수 있다. 드론을 통해서 시간대별 위치정보와 고도 정보를 이용해 출발지, 도착지, 사고지점 등을 유추할 수 있다. 위치정보를 기반으로 비행경로를 분석하고 촬영된 사진과 동영상을 확보하는 방식이다.

또 모터의 추력과 드론 자체의 무게를 알면 짐의 여부와 무게를 알 수 있다. 더 나아가서 전문가들은 디지털 포렌식 기술 대상이 사물인터넷(IoT), AI 스피커, 자율주행차량으로 확대될 것으로 전망한다. 자율주행차량의 경우 이동 경로, 스마트폰 연동 정보 등 더 많은 정보를 저장하기 때문이다. 따라서 앞으로 자동차 포렌식 기술이 급부상할 전망이지만, 이처럼 다양한 기기의 디지털 포렌식을 위해서는 클라우드 기술이 뒷받침되어야 한다는 것도 간과해서는 안 되는 사실이다[39].

기본적으로 디바이스는 클라우드와 연결되어 있기 때문. 특히 IoT 장치의 경우

클라우드에 더 많은 데이터가 저장된다. 또 클라우드에는 IoT, 스마트폰과 관련된 데이터뿐만 아니라 사용자의 다양한 데이터베이스(DB)가 저장된다. 클라우드 분석을 위해서는 빅데이터 처리 기술, 관계 분석 기술, 데이터 시각화 기술 등이 필요하다. 디지털 포렌식 전문가들은 향후 몇 년간의 디지털 포렌식의 트렌드는 IoT, AI 스피커, 드론, 자동차 등으로 클라우드를 통해 더 많은 데이터를 가져올 수 있을 것으로 전망하고 있다.



[그림 Ⅱ-4] 사이버 포렌식의 종류[40]

2.3. 국내·외 정보보안 교육 현황

2.3.1 국내 정보보안 교육 현황

최근의 혁신적 기술 진보를 배경으로 지능 정보사회의 핵심 기술인 기계 학습, 딥러닝을 비롯한 AI(인공지능) 기술이 비약적으로 발전하면서, 국내 교육부에서도 정보보안 교육의 중요성이 대두되고 있다. 국내의 종합 계획을 살펴보면, 4차 산업혁명으로 인간 교육의 영역으로 인식되었던 인간의 지적 능력까지 컴퓨터로 구현되어, 인공지능이 우리 삶의 모든 영역에 걸쳐서 패러다임 전환이 예상된다. 인공지능의 기술 발달에 따른 국내·외 고용의 변화로 인해 2030년까지 전 세계 일자리의 20%가 자동화가 될 것이며 우리나라의 기존 일자리는 700만 개가 감소하고 신규 최대 730만 개의 새로운 일자리가 창출될 수 있을 것으로 보고 있다. 전 세계적으로도 7천 500만 개의 일자리가 대체 되고 1억 3천 300만 개의 새로운 일자리가 창출될 것으로 예측하였다. 이와 같은 전망을 종합해 보면 인공지능 기술이 기존 단순 반복 업무의 일자리를 대체하지만, 새로운 유형의 일자리 창출이 대폭 증가할 것이고 인공지능 기술에 기반한 지능정보사회에서는 산업시대의 읽고, 쓰고, 셈하기에 더하여 컴퓨팅 능력을 기본 역량으로 요구하게 될 것이다. 인간의 힘으로 혼자서 해결하기 어려운 복잡한 문제를 해결하기 위해 컴퓨팅 사고력과 협업 능력이 새로운 핵심역량으로 부상되는 이유이다[41].

우리나라는 국제 컴퓨터·정보 소양 연구(ICILS-International Computer and Information Literacy Study, 2018)에서 컴퓨팅 사고력 즉 컴퓨터를 이용하여 해결할 수 있는 문제를 인식하고, 알고리즘 적 해결책을 개발·평가하여 컴퓨터로 수행할 수 있는 개인의 능력, 정보 생성 및 의사소통에 컴퓨터를 사용할 수 있는 개인의 능력인 컴퓨터·정보 소양은 덴마크에 이어 2위를 차지할 만큼 뛰어나다.

그러나 2015 개정 교육과정에서 초·중등학교 정보교육을 필수화하고 2018년부터 단계적으로 적용, 인정 교과서와 검정교과서 등을 보급하는 동시에 중학교 학교급의 학교·학생 맞춤형 교육을 위해 학교장 선택과목의 신설을 지원하고 고등학교의 학교장 선택과목도 신설하여 학생의 진로와 희망에 따른 과목 선택권 등

을 확대하는 등의 노력을 하고 있으나, 수업 시수 부족으로 양질의 교육을 제공하기에는 한계가 있고 COVID-19에 따른 원격교육의 확대로 초등학교 저학년부터 정보 통신 기기에 대한 기본적인 ICT 활용 능력의 필요성이 증대되고 있기 때문에, 모든 학교급에 정보교육 과정을 편성하고, 초등학교부터 고등학교까지 체계적이고 연속적인 정보 기초 교육을 시행하는 등 양질의 교육 기반 마련이 필수적이다.

이러한 교육의 기반을 마련하기 위해는 현장 교사의 정보보안 교육을 통한 역량 강화가 필요하다. 교원의 역량 강화를 위해서는 초임에서 퇴임까지 교직 경력별 체계적, 지속적인 정보 역량 강과 연수 프로그램을 마련하고 지식 습득 중심의 연수를 넘어 정보보안 교육내용에 대한 실질적 교수 역량을 신장 시킬 수 있도록 체계적인 연수, 학교급별, 고교 유형별 맞춤형 연수와 인공지능, 데이터 과학 담당 교사의 역량 강화를 위해 대학, 연구소. 민간기업, 유관기관 등에 일정 기간 동안 파견하여 빠르게 변화하는 정보기술 분야의 교육 역량을 제고해야 한다는 목소리가 높다. 정보보안 교육의 높은 요구에도 불구하고 국내의 교육 동향을 살펴보면 인공지능 활용 교육이 주를 이룬다[42].

국내의 각 시도교육청과 학교 내의 실정과 관심 속에서 2015 교육과정에는 정보 교과 교육과정이 포함되어 있다. 이미 과거 6차 교육과정에서 초등학교부터 고등학교까지 컴퓨터 관련 내용과 과목을 정착하였고 7차 교육과정에서는 인문계 고등학교의 일반 선택과목으로 '정보사회와 컴퓨터' 과목이 신설되었으나 소프트웨어 활용 교육에 치중되면서 내용도 중복되었다[43]. 2015 개정 교육과정이 되어서야 초등학교 고학년 실과와 중·고등학교의 정보 교과를 소프트웨어 중심으로 개설하였고 이전 교육과정에서 정보 과목으로 불리던 중학교 정보와 고등학교 정보를 '정보 교과'로 통합하여 컴퓨터 과학의 원리, 문제 해결 능력, 정보기술의 올바른 사용 등에 관한 내용으로 구성하였다. 여기서 주목할 점은 정보 과목의 목표인데 주로 핵심은 정보 윤리 의식을 바탕으로 정보보호 능력을 함양하고 실생활의 문제를 해결할 수 있는 정보기술 활용 능력과 컴퓨팅 사고력, 다양한 학문 분야의 복잡한 문제 해결을 위한 협력적 문제해결력을 기르는 데 중점을 두고 있다. 이에 해당하는 교육 커리큘럼 중 초등학교의 교육 커리큘럼을 살펴보면 실과과목에 적용된 기술 시스템 영역 소프트웨어의 이해 / 절차적 문

제 해결 / 프로그래밍 요소와 구조와 기술 활용 영역에는 개인정보와 지식 재산 보호 / 로봇의 기능과 구조가 있다. 본 내용에는 주로 인공지능의 소개 및 알고리즘과 관련된 놀이 활동 등이 주를 이루고 있는데, 중·고등 교육을 살펴보더라도 ICT 활용 교육에만 초점이 맞춰있다는 것을 알 수 있다. 다음은 학교급별 정보교육 교과 내용 요소를 표로 나타낸 것이다[44].

[표 Ⅱ-1] 학교급별 정보 교육 교과 내용 요소[44]

학교급	영역	핵심 개념	내용 요소
초등학교 (실과)	기술 시스템	창조	생명 기술 시스템/식물가꾸기/동물돌보기
		효율	수송기술과 생활 /수송 수단의 안전 관리
		소통	소프트웨어의 이해/절차적 문제 해결 /프로그래밍 요소와 구조
	기술활동	적응	일과 직업의 세계/ 자기 이해와 직업 탐색
		혁신	발명과 문제 해결/개인정보와 지식 재산 보호/로봇의 기능과 구조
		지속가능	친환경 미래 농업 / 생활 속의 농업 체험
중학교 (정보 교과)	정보문화	정보사회	정보사회의 특성과 진로
		정보윤리	개인정보와 저작권 보호/사이버 윤리
	자료와 정보	자료와 정보의 표현	자료의 유형과 디지털 표현
		자료와 정보의 분석	자료의 수집/정보의 구조화
	문제 해결과 프로그래밍	추상화	문제 이해/핵심요소 추출
		알고리즘	알고리즘 이해/알고리즘 표현

		프로그래밍	입력과 출력/연산/제어 구조 /프로그래밍 응용
	컴퓨팅 시스템	컴퓨팅시스템의 동작 원리	컴퓨팅 기기의구성과 동작 원리
		피지컬 컴퓨팅	센서 기반 프로그램 구현
고등학교 (정보교과)	정보문화	정보사회	정보 과학과 진로
		정보윤리	정보보호와 보안/저작권 활용/사이버윤리
	자료와 정보	자료와 정보의 표현	효율적인 디지털 표현
		자료와 정보의 분석	자료의 분석/정보의 관리
	문제 해결과 프로그래밍	추상화	문제 분석/문제 분해와 모델링
		알고리즘	알고리즘 설계/알고리즘 분석
		프로그래밍	프로그램 개발 환경/변수와 자료형/연산자, 배열, 함수/표준 입출력과 파일 입출력/중첩제어구조 /프로그래밍응용
	컴퓨팅 시스템	컴퓨팅시스템의 작동원리	운영 체제 역할/네트워크 환경 설정
		피지컬 컴퓨팅	피지컬 컴퓨팅 구현

이 밖에 2015 개정 교육과정에 따른 검인정 교과서 중 초등 실과 2종(천제교과서, 교학사), 중학교 정보 4종(천재교과서, 미래엔, 성안당, 한빛아카데미), 고등학교 정보 4종(교문사, 금성출판사, 씨매스, 천재교과서)의 교과서 내용을 살펴보면, 단원 구성은 교육부 내용 체계를 기반으로 되어있으며, 내용의 구성은 [표 Ⅱ-2]와 같이 초등 실과의 경우 1%대, 중등 정보 교과의 경우 3~6% 대로 정보보안의 비율이 높지 않다[1].

[표 Ⅱ-2] 학교급 별 정보 교과서 내 정보보안 교육 비율[1]

학교급	출판사명	전체 페이지 수 (페이지)	정보보안 페이지 수 (페이지)	정보보안 관련 교육 비율 (%)
초등 실과교과	천재교과서	132	2	1.51
	교학사	128	2	1.56
중등 정보 교과	천재교과서	188	9	4.78
	미래앤	170	11	6.47
	성안당	184	8	4.34
	한빛아카데미	170	8	4.70
고등 정보 교과	천재교과서	244	14	5.73
	교문사	211	13	6.16
	금성출판사	232	8	3.44
	씨매스	252	16	6.34

[표 Ⅱ-2]에서 정리한 검인정 교과서의 정보보안에 관한 내용을 살펴보면 초등 실과과목과 중학교 정보 교과의 경우 개인정보보호와 관련된 내용만 다루고 있으며, 고등학교 정보 교과의 경우 정보보안과 관련된 법규를 다루는 것을 알 수 있다.

초등 실과 교과서의 개인정보보호는 개인정보의 정의, 개인정보 유출 방지 방법으로 온라인 계정의 비밀번호 복잡도 설정과 주기적인 변경 및 공공장소에서 컴퓨터 사용 후 로그아웃하기, 출처가 불분명한 온라인 자료 다운로드 금지 등의 내용을 다루고 있다.

중등 정보 교과서의 개인정보보호는 개인정보보호법 내 개인정보의 정의를 인용하였고, 스팸, 스미싱, 피싱 등 개인정보 침해위협 방식에 관해 설명하고, 개인정보보호방안, 개인정보 침해사고 발생 시 신고 방안 등에 대하여 수록되어 있다.

고등정보 교과서의 정보보안은 정보보안의 3대 요소인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 토대로 정보보안의 개념과 중요성, 바이

러스, 악성코드, 랜섬웨어 등의 보안 위협의 종류와 방화벽, 암호화, 바이러스 백신 등 정보보안 위협의 대응 방안에 대하여 다루고 있다. 또한 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 통신비밀보호법 등 정보보안 관련 법규에 관하여 설명하고 있다.

이 외에 국내 공공기관의 정보 분야의 교육과정은 교육부 정보보호센터 주관의 교원들을 위한 보안 교육 프로그램이 있다. 본 정보보호센터의 교육은 교육기관의 정보보호 인식 제고와 역량 강화를 위해 설립되었고 주로 개인정보보호 교육을 위한 교육과정 및 교재를 개발하여 연수를 운영하고 있다. 그리고 한국인터넷진흥원(KISA)의 사이버보안인재센터의 교육 프로그램과 케이-쉴드 주니어(K-Shield Jr.) 교육 프로그램이 운영되고 있는데 사이버보안인재센터의 교육은 국가 공무원과 공공기관에 종사하는 관련 직종의 직무교육을 하고 있으며, 케이-쉴드 주니어 교육 프로그램 역시 주로 직장인들이나 취업준비생을 위한 교육으로 실무 능력을 함양 시킬 수 있는 교육이 운영된다.

케이-쉴드 주니어는 교육과정은 정보보호 관리진단, 보안사고 분석 대응 두 가지로 분리하여 교육생을 선발한다. 정보보호 관리진단 과정은 정보보안 컨설턴트, 기업 보안 담당자, 모의해킹 분야로의 인력 양성을 위한 교육과정으로 구성되어 있다. 보안사고 분석 대응 과정에는 실제 보안사고에 대한 대응 이해 능력을 향상시키기 위한 악성코드 분석, 침해사고 분석, 보안솔루션 개발, 보안 관제(Computer Emergency Responce Team: CENT) 등의 분야를 교육한다. 이와 같은 프로그램은 정보보호에 대한 수강생들의 관련 지식 습득 기회를 제공하고 국내 정보보호 시장의 원활한 인력 수급을 위한 관련 분야의 전문 인력 양성 과정이기 때문에 선발 과정을 거친 후 선발된 수강생을 대상으로 프로그램을 이수할 수 있다.

국내 전문대학, 4년제 대학교, 대학원에서 이루어지는 정보보안 교육 또한 취업을 목적으로 공학 기초전공 학습 등을 공동된 커리큘럼으로 전공생의 위주로만 교육이 진행되고 있다. 이러한 점은 교육 프로그램의 접근성을 낮춰 초등학생 개인의 정보보호 지식 향상과 일반인에 미치는 파급효과가 적을 수 밖에 없다.

범국민 보안 교육과정이나 초·중등 정보보안 교육은 거의 이루어지고 있지 않다고 봐도 큰 무리가 아니다[42].

2.3.2. 해외의 정보보안 교육 현황

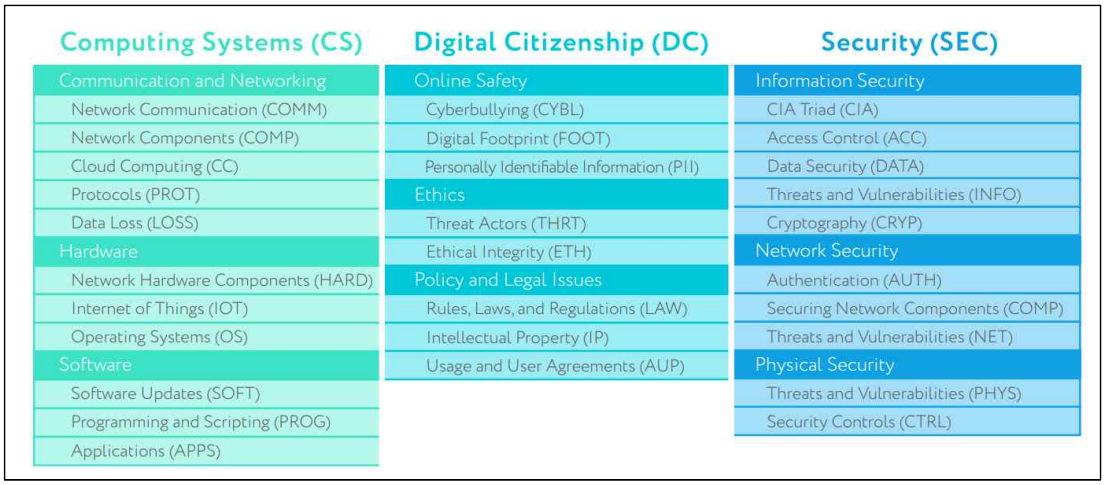
해외의 정보보안 교육의 경우 초등학교 1학년부터 체계적으로 교육프로그램을 구상하고 단순한 지식의 습득 능력보다 컴퓨팅 사고력 기반의 창의적 문제 발견 및 해결 능력을 강조하고 있다. 미국의 경우 백악관의 '국가 AI 연구 개발 전략 계획 보고서'에 초·중·고 AI 교육의 중요성에 대해 강조하고 초·중등 교육에서의 인공지능 교육과정 가이드라인을 개발하고 교사를 위한 교수·학습 자료 및 도구의 개발과 온라인 개발을 제공하고, 국내·외 협업 커뮤니티 활성화 등을 추진하고 있다.

영국의 경우 2018년 상원 AI 특별위원회의 '영국의 AI 보고서(AI in the UK : Ready, Willing, and able'에서 초등 단계에서부터 AI 교육이 필요하며, 교사 양성과 컴퓨팅 교육과정 개발 및 핵심 교과에 필수적으로 정보교육이 포함될 것을 권장하고 있다. 앞서 언급한 미국과 영국이 교육 정책을 변경하는 것으로의 접근이었다면 프랑스와 에스토니아는 교육시스템 및 플랫폼 구축에 조금 더 초점을 맞추었다[45].

CT(Computational Thinking)에 대한 미국의 컴퓨터 과학을 가르치는 교사 모임(Computer Science Teachers Association: CSTA)을 중심으로 CT에 대한 구체적인 교육의 사례를 알아보았다.

미국은 K-12 프로그램에서 정보보안 교육을 컴퓨터 과학 교과목 전반에서 다루고 있다. K-12 프로그램은 CSTA라는 미국의 컴퓨터 과학 교사 모임으로 컴퓨터 과학 교육에 대한 다양한 자료를 공유하기 위해 만들어진 단체가 2003년 K-12(초·중등) 학습자에게 체계적으로 컴퓨터 과학을 교육할 수 있는 교육과정 기준안과 다양한 수업 형태 제안하였다. 본 프로그램에는 저학년에는 전반적으로 사이버보안의 기초 이론과 관련 법과 제도 및 규범 등의 이해를 중심으로 학년이 올라갈수록 시스템 및 네트워크상의 위협 등 전문적이고 기술적인 내용을 주로 학습한다[45]. 본 프로그램은 홈페이지를 통해 K-12 사이버보안 학습 표준 프로그램을 제공하여 가이드를 제시하고 있으며 커리큘럼은 [그림 Ⅱ-5]와 같다.

본 프로그램의 표준안은 교사가 학생들에게 사이버보안의 기본 개념에 관해



[그림 Ⅱ-5] K-12 사이버보안 학습 표준 커리큘럼[46]

설명하고 기술적인 내용을 제공한다. 각 학년 수준에서 학생들이 알아야 하고 할 수 있는 것에 대한 학습 목표를 설정하여 더 많은 수의 사이버보안 경력을 추구하는 데 필요한 기술과 지식. 표준을 제시하고 있다. 본 프로그램에서 파란색 부분의 보안(SEC) 학년별 교육 프로그램에서 다루고 있는 내용을 살펴보면, 정보보안, 네트워크 보안, 물리적 보안 총 세 개의 커리큘럼 안에서도 K-1~12를 총 4단계로 나누어 단계적인 프로그램을 운영하는 것을 알 수 있다. 교육은 저학년일수록 만화 등을 활용한 상황별로 시나리오를 작성하여 쉽게 접근할 수 있도록 구성한 부분이 중요한 특징으로 보인다[46].

프랑스의 경우 무료 온라인 컴퓨팅 교육플랫폼의 개발뿐만 아니라 미국의 미네르바스쿨과 비슷한 학비 없는 IT 교육기관인 에꼴42(Ecole 42)를 설립하였다. 에꼴42는 강사도 교과서도 학비도 없이 주체적이고 협업 능력이 뛰어난 IT 인재 양성을 목적으로 한다[47].

에스토니아의 경우에는 창의적인 소프트웨어 개발의 가치를 발견하고, 세계 최초로 컴퓨터 프로그래밍을 7세부터 19세까지 교육하고 있다. 2012년부터는 초·중등 학습자들을 대상으로 SW 교육 프로그램인 'Proge Tiger'를 운영하고 있으며 민관이 협력하여 특별 교육 프로그램을 지원, 핀란드의 IT 기업이 자문역을 수행하고 있다. 이러한 전폭적인 국가의 지원으로 2011년 영국 벤처 창업 경진대회에서는 예선 20개 팀 중에 4개의 팀이 출전하는 등의 성과를 보였다. 이는 또한 스타트업을 통한 기술 및 자본 창출 증가와 세계 최초의 전자투표 방식의 소프트

웨어를 개발하는 등 지속적이고 체계적인 교육이 국가발전에 이바지하는 대표적인 사례로 언급된다. 에스토니아는 디지털 학습 상황을 마치 거울을 보듯 스스로 평가할 수 있도록 지원해주는 온라인 도구인 디지털 미러를 개발하여 학교 스스로 정보교육 전반의 자가 평가 시스템을 도입하여 학교와 학생의 목표 도달을 위한 피드백을 제공하는 것이 특징이다[48].

교원 전문성 강화에 목표를 둔 해외 사례로 보면 호주는 교사 전문성 개발 기준을 정립하고 초임 교사, 숙련 교사, 높은 성취 교사, 리더 교사 총 4단계로 교사의 급을 구분하여 국가 차원에서의 체계적인 연수 체제를 운영하고 있다. 호주 정부는 주 전체의 교사 인증기관과 협의하여 모든 교사의 전문성을 인증하는 과정에 책임을 진다. 싱가포르는 21세기 교사 교육모형과 교사 경력별 전문성 개발 모형을 기반으로 지원하고 국립교육원과 싱가포르 교사 아카데미를 중심으로 학교 기반의 전문적 학습 공동체를 통한 전문성 개발을 위하여 노력하고 있다. 정보보안 교육 내에서 원격으로 진행하며 안정한 온라인 행동 및 사이버 불링(사이버 폭력) 등에 대응 및 신고 방법 학습을 통해 자신의 권리를 보호할 수 있는 방법과 윤리 의식 제고를 주요 목표로 하는 사이버 안전 및 윤리 교육을 하고 있다[49].

영국은 2014년 ICT 활용 교과를 컴퓨터 과학으로 개편하고 초·중고 필수 교과과정으로 시행하고 있다. 이 밖에도 방과 후 소프트웨어 교육 프로그램인 '코드 클럽'을 정규교과 과정으로 채택하고 초등학교에서 컴퓨팅을 주당 50분 이상 교육하고 있다. 11세 이상 학생들에게는 실제 프로그래밍 언어를 교육하여 컴퓨터 과학, IT 기술, 디지털 스킬의 세 가지 부분을 포함 최소 2개의 프로그래밍 언어를 습득하는 것을 목표로 하고 있다[50].

일본의 경우 우리나라와 비슷한 수준의 정보보안 교육을 진행하고 있는데 정보윤리 교육을 하며 일상생활에 필요한 정보보안 관련 지식의 이해 및 습득을 통해 자신을 보호할 수 있는 수장 학습을 목표로 한다. 세부적으로는 윤리, 법률, 안전 지식, 정보보안 개념의 학습 등이 있다[49].

인도에서도 초등학교 고학년과 중학교에서 프로그래밍을 교육하여 컴퓨터 원리에 대한 이해를 증진하고, 논리적 사고력과 창의력, 문제해결력을 향상시키는 데 중점을 두고 교육과정을 운영하고 있다. 정보 교과는 이미 초·중등학교의 필

수 및 선택 필수 교과로 지정하였으며 IIT(India Institute of Technology) Bombay는 2010년 SW 스타트업과 함께 저학년용 컴퓨터 과학 교육과정인 'CM(Computer Masti)' 커리큘럼을 완성하여 미래 국가 정보보안 분야 발전을 위한 인재 양성에 노력하고 있다[49].

이스라엘의 사이버 교육은 군 사이버 부대 군인들에 의해 고안되었으며 이스라엘의 사이버 스쿨(Cyber School)은 초·중등 교육 및 성인 사이버 부트 캠프까지 고급 컴퓨팅을 교육하고 연구하는 기관으로 사이버 인식, 의미뿐만 아니라, 실용적인 첨단 보안 툴 학습 및 공격 툴 학습을 제공한다. 이 기관의 사이버보안 프로그램은 초등학생부터 고등학생, 성인에 이르기까지 컴퓨터 프로그래밍 기술과 다양한 유형의 사이버 공격에 대처하는 방법을 교육한다. 초등 1~2학년생 대상으로 한 사이버 키즈 프로그램의 커리큘럼은 컴퓨터 구조 및 사용, 인터넷, 올바르게 사용하기, 디지털 공간에서 주의할 점, 애니메이션 만들기, 오피스 응용 프로그램, 바이러스 및 컴퓨터 보호 등으로 컴퓨터에 자연스럽게 친화되면서도 사용할 때 주의할 점을 동시에 배운다. 같은 구성으로 내용은 더욱 심화된 3학년 이상의 고학년용 프로그램이 있으며, 본격적인 보안 내용과 해킹에 대해서는 중학교(7학년)부터 배우게 되는데 코스별 내용은 는 다음 [표 Ⅱ-3]과 같다[49].

[표 Ⅱ-3] 이스라엘 사이버 스쿨 교육과정의 코스별 내용[49]

분류	초등학생을 위한 사이버 교육		
대상	사전 관련 지식 없는 학생		
코스	사이버 코스 (1학년)	사이버 코스 (3학년)	사이버 테크 코스 (5~6학년)
커리큘럼	•컴퓨터 구조 및 사용 •인터넷-알아가고 올바르게 사용하기 •디지털 공간에서의 주의 •애니메이션 만들기 •사무실 응용 프로그램	•고급컴퓨터 사용 •인터넷을 알아가고 올바르게 사용하기 •디지털 공간에서의 주의 •프로그래밍 중-재생 중 •사무실 응용 프로그램 •바이러스 및 컴퓨터 보호	•컴퓨터 구조 및 사용 •자바 스크립트 언어의 초기 코드 •컴퓨터 및 홈 네트워크의 보안 •코드 게임 구축 •인터넷의 올바른 사용과 안전한 브라우징 •웹 및 인식 검색, HTML •바이러스 및 PC 보호

분류	청소년 사이버 교육 (7~9학년)		
대상	컴퓨터, 기본 영어의 기본 지식, 프로그래밍 언어와 시스템을 이해할 수 있는 사람		
코스	파이썬 코스	사이버 해킹	사이버 트렌드
커리큘럼	•파이썬 소개 •변수 •루프 •리스트 •사전 •기능 •고급 라이브러리 •객체 지향 프로그래밍	•컴퓨터 및 네트워크 아키텍처 •컴퓨터 및 네트워크 보안 해킹 •프로그래밍 기본 사항 •시작 운영 체제 및 응용 프로그램 •정보 전달 방법 및 정보보안 방법 •외부 소스로의 정보 유출 방지 •바이러스 유형, 대처 및 자체 바이러스 구축 •디지털 공간의 허점/고급 해킹 방법	•개발(파이썬 기초, 파이썬 페루, 파이썬 보안) •인프라(통신 및 정보보안, Microsoft 운영 체제 보안, 리눅스 운영 체제 보안) •사이버(사이버의 기초, 사이버 프로, 공격적인 사이버)

마지막으로 중국의 사례를 살펴보면 2001년부터 '종합 실천 활동' 내 정보기술 교육을 필수과목으로 지정하였고 초·중등학교까지 정보기술을 포함한 탐구학습, 봉사활동, 체험학습 등을 '종합 실천 활동'의 교육과정으로 편성하고 구체적인 내용은 지역과 학교에서 자율적으로 개발할 수 있게 하였다. 저학년은 응용 소프트웨어 활용부터 시작하고 고학년에서는 논리력 향상을 위한 프로그래밍 기술을 익히도록 교육내용을 구성하였다. 베이징의 경우 초등학교 3학년부터 중학교까지 정보기술 영역 104시간 학습, 고등학교에서는 독립교과로서 정보기술을 일주일에 필수 2시간과 선택 2시간으로 교육하고 있다[51].

또한 중국의 교육부는 시진핑 총서기의 총체적인 국가 안보 사상을 실현하기 위해 배포한 '대/중/소학 국가 안전 교육 지도 요강'에서 국가 안보 교육의 주요 내용을 정치, 국토, 군사, 경제, 문화, 사회, 과학기술, 네트워크, 생태, 자원, 원자력, 해외이익 등 12개 분야로 분류하면서 정보보안에 중요성에 대해서도 교육을 시행하고 있다. 특히 인터넷 보안 중에서도 정보보안에 대해서 정보사회의 건전한 발전을 보장하고 추진하는 기반이라고 설명하였다. 이는 중국이 동남아시아권 타 국가보다도 인공지능 기술 분야 등에서 앞서 나갈 수 있는 원동력이 될 수 있다.

Ⅲ. 하이브리드 블렌디드 실천모형 디자인

3.1. 교수·학습 모형 선행연구 분석

3.1.1. 맞춤형 교수·학습 모형 연구·분석

비대면 수업이 장기화하고 앞으로 미래 교실의 방향성이 언급될수록 교육 대상자의 특정 성취기준이나 학습 목표를 개인에게 맞추고 영역별로 도전적 목표에 다다를 수 있도록 설계할 수 있는 수준별 맞춤형 교수(differentiated instruction)의 수업 설계가 매우 중요하다. 맞춤형 수업 설계 연구가 최근에는 교과의 변인을 고려하는 연구로 시작되고는 있지만, 아직 학생 관련 일반적이고 장기적인 변인에 집중하는 경향이 강하여 학습 목표를 중심으로 전개되는 교과 수업에 적용하기에 한계가 있다[54]. 이대식(2016)은 특정 학습 목표를 학습자에 맞추어야 하는 교사의 관점에서 학습자의 일반 변인들을 학습에서 맞추라는 식의 일반적인 지침 정도로는 실제적인 도움을 얻기 어렵다고 비판했다. 교과 교육에서 맞춤형 수업이 이루어지기 위해서 교과의 특정한 학습 목표와 관련하여 학생의 다양한 요구등을 고려하는 수업의 타당성을 주장하고 있으며, 이러한 현장의 요구와 목소리에 따라 학습 목표와 연계한 맞춤형 수업 설계가 중요함을 알 수 있다.

맞춤형 수업의 대표적 전문가인 톰린슨(Tomlinson, 1999)은 수업에 대한 철학으로 맞춤형 수업을 제안했다. 수업 철학으로 맞춤형 수업이란 교사가 학생의 차이(differences)를 고려하여 수업을 구성할 때 학생이 가장 잘 배우며, 동시에 맞춤형 수업은 학생의 서로 다른 필요에 '반응(response)'하는 수업 전략이나 방법들을 포괄적으로 의미한다. 즉, 맞춤형 수업의 핵심은 반응적 수업(responsive teaching)으로, 교사가 수업에 참여하는 학생들의 서로 다른 필요에 주목하고 이를 분석하여 수업 설계 및 학생과의 상호작용에 반영하는 것이 강조된다. 학생의 차이를 수업 설계에 반영하기 위해서는 학습의 내용, 과정, 결과 측면에서 다각적인 검토가 요구된다. 먼저, 교과 수업에서 맞춤형 수업 설계가 이루어지기 위

해서는 상세화한 학습 목표를 실제 수업 설계와 어떻게 연계할 수 있을지 구체적 방안 탐색이 필요하다. 맞춤형 수업 설계를 구체적으로 확대해갈 때 연구자 및 교육 실행가들에게 맞춤형 수업의 실행 가능성을 확장할 수 있기 때문이다[54]. 맞춤형 수업 연구에서 가장 강조하는 부분은 어떻게 학생의 차이를 고려하여 학습의 과정을 구성할 것인 대한 문제이다. 기존 맞춤형 수업 연구에서 전형적인 방법은 학습자를 변인에 따라 분류하고, 분류된 학습자 변인에 따라 수업 내 활동을 다르게 제시하는 것이었다. 하지만 선행연구에서 특정한 학습 목표를 직접 고려하는 맞춤형 수업의 설계 방안에 관한 연구는 찾아보기 어렵다.

이에 따라 학습 목표를 충분히 반영한 맞춤형 수업 설계 방안이 마련될 필요가 있다. 또한 맞춤형 수업에서 학습의 결과를 학생의 차이에 맞춘다는 것은 Tomlinson과 McTighe의 200년 연구에 따르면 학습한 결과를 학생이 선호하는 방식으로 표현하도록 허용하는 것을 말한다. 예를 들어, 글이나 그림, 동영상 등 다른 양식(mode)을 사용한 학습 결과 보고서를 허용하는 것이다. 따라서, 기본적으로 학생의 서로 다른 학습 목표 수준을 고려한 평가 기준 차별화 방안의 고려가 필요하는 것에 중점을 두어 분석하였다.

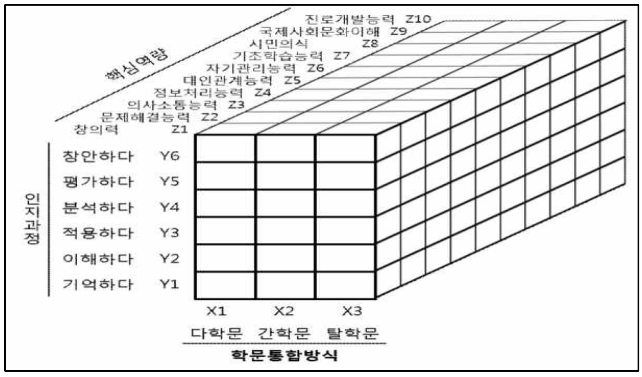
3.1.2. 다학문적 맞춤형 교육과정 모형 연구·분석

21세기를 준비하는 학습은 ICT를 활용한 교육과정의 혁신에 중점을 두고 발표되었다. 이것은 ICT를 하나의 독자적 교육 부분으로 간주하지 않고, 교육 패러다임 변화를 주도하는 도구로 활용할 것을 주장하고 있다. 21세기 학습 능력은 가장 핵심이 되는 영역으로 21세기의 인간에게 필요한 학습 능력을 체계화, 조직화를 하여 표준안을 마련하였다. 학습 능력은 크게 세 개의 범주로 나누었고 총 10개의 학습 능력을 제안하였다[52].

다학문적 접근방법은 일차적으로 학문 분야에 초점을 둔다. 교사들은 하나의 주제를 중심으로 여러 학문 분야의 내용을 선정하고 조직한다. 한 교과 영역 내의 하위 학문 분야를 통합하는 것을 학문 내 접근방법이라고 한다. 언어라는 과목 안에 읽기와 쓰기, 그리고 말하기가 통합되는 일이 가장 흔한 예이다. 학문

내 접근의 사회과 프로그램에서 역사, 지리, 경제, 정치 분야가 통합된다. 또 통합과학이라는 과목에 생물학, 화학, 물리학, 지구과학과 같은 하위 학문 분야의 관점들이 통합된다. 이러한 통합을 통하여 학생들이 여러 하위 학문 분야들 사이의 관련성을 이해하고, 하위 학문 분야와 현실 세계와의 관계를 파악할 수 있을 것이다. 다학문적 접근방법을 활용하되, 기능과 지식, 태도 등을 융합하여 정규학교 교육과정으로 개발할 수 있다. 특정 주제를 가지고 학생들이 여러 교과 영역에 걸쳐 학습할 수 있고, 컴퓨터 기능을 각 교과 내용에 통합시킴으로써 공학을 교육과정 전반에 융합할 수 있다.

초·중등학교의 맞춤형 다학문적 교육을 위한 교육과정을 개발하기 위해서는, 우선 다문학 교육의 이론 정립과 이론적 모형이 있어야 하고, 수업 모형 개발 및 교육과정이 개발돼야 할 것이다. 앞에서 소개한 21세기에 필요한 통합 학습 요소, 통합교육과정 이론과 교육과정 설계 모형인 큐빅 교육과정 모형, STEAM 교육 모형[53], 배선아의 통합교육과정의 통합유형 분석 모형, 블룸(Benjamin S. Bloom)의 신교육목표분류(Taxonomy)에 관한 문헌 연구를 바탕으로 다학문 맞춤형 학문 통합 모형을 제안하였고 [그림 Ⅲ-1]에서 다학문적 맞춤형 학문 통합 모형의 실제를 확인할 수 있다. [55].



[그림 Ⅲ-1] 다학문적 맞춤형 학문 통합모형[52]

다학문 맞춤형 학문 통합 모형에 사용할 X축의 요소는 큐빅 모형의 학문 간 통합 정도에 따라 다학문적 통합, 간학문적 통합, 탈학문적 통합으로 분류하고, Y축의 요소는 Bloom의 '신교육 목표 분류학의 인지적 영역'을 사용하여 낮은 사고력을 요

구하는 인지과정부터 높은 사고력을 요구하는 인지과정의 순서대로 분류하였고 선택할 수 있도록 하였다. 마지막으로, Z축의 요소는 미래 한국인이 갖추어야 할 10가지 핵심역량으로 통합 교육을 위한 수업 진행 시 내용과 절차에 적합한 핵심역량을 요소를 선택할 수 있도록 하였다.

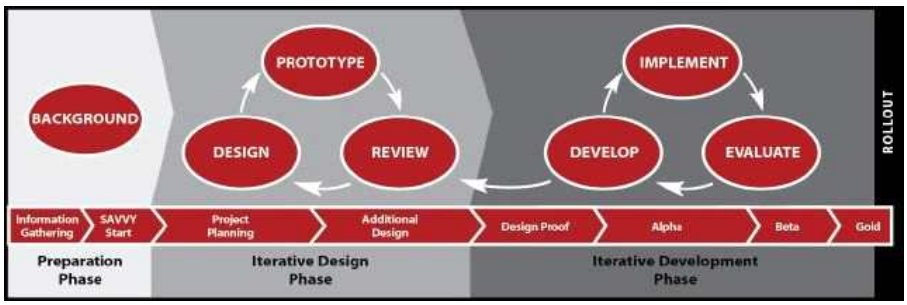
본 모형은 현장에서 교사들이 통합수업에 적용하기 쉽고 모든 학교급에서 다양한 학생들의 수준에 맞게 교육과정을 적용할 수 있도록 설계하였다. 아울러 유치부부터 고등학교 및 특수학교에서도 이 모형을 적용하여 수업 및 평가에 적용할 수 있도록 구성하고 있다. 전문가와 현장 교사들을 대상으로 모형의 타당도를 검증하고, 다학문 맞춤형 학문 통합 모형으로 교육과정을 개발하여 실제 현장 학생들에게 적용할 수 있다.

3.1.3. SAM 모델 교수·학습 모형의 연구·분석

Successive Approximation Model의 약자인 SAM은 사용 가능한 교육 자료의 즉각적인 요구를 충족하기 위한 반복적인 설계 및 제공 모델의 역할을 한다. 인지주의에 뿌리를 둔 ISD (Instructional Systems Design)의 개념은 1950년대부터 시작되었으며 교육 자료를 체계적으로 구성하는 방법으로 처음 개발되었다. 행동주의의 핵심은 성과의 산출물에 더 관심이 있고 새로운 정보의 학습과 보유를 향상시키는 인지과정에는 관심이 덜하다. 행동주의의 단점으로 인해 인지 심리학자인 Robert Gagne는 체계적으로 구조화되는 학습의 가장 초기 화신인 시스템 개념을 도입했다. 시스템 개념은 학습이 순차적이고 긍정적인 결과를 보장하기 위해 교육 자료의 설계에 더 많은 시간을 투자해야 한다고 제안하였고, ADDIE 모델은 플로리다 주립 대학의 심리학자 팀이 교육 양식을 구성하고 설계하기 위한 실무자 가이드로 개발되었다[56].

본 모델은 5개의 분석, 설계, 개발, 구현 및 평가 내에 여러 단계를 포함했으며 ADDIE 모델의 아이디어는 후속 단계로 이동하기 전에 각 단계를 완료하는 것이다. 이 모델은 Instructional Design 프로젝트의 토대 역할을 했지만, 본질적으로 경직되고 너무 선형적이라고 비판받아왔다. ADDIE 모델에서 자주 제기되는 문

제는 교육 효과를 평가하는 과정이 느리고 프로젝트가 실행 특성으로 인해 의도한 대상에 도달하는 데 과도한 시간이 걸릴 수 있다는 것이다. ADDIE 모델은 1990년대 초부터 민첩성을 높이기 위해 진화했으나 단계의 순차적인 특성은 여전히 한계가 있다. 그럼에도 불구하고 신속한 프로토 타이핑은 ADDIE 모델의 제한 요인에 대한 대응으로 SAM 모델은 ADDIE 모델 프로세스의 박스형 특성에 대한 대안으로 개발되었으며. SAM 모델은 단축된 단계를 사용하여 전체적이고 유연한 프로젝트를 생성하는 신속한 설계 및 개발 모델 역할을 한다. 다음 [그림 Ⅲ-2]는 SAM 모델을 도식화한 것이다[57].



[그림 Ⅲ-2] Successive Approximation Model[57]

분석 단계로 시작하는 ADDIE 모델과 유사하게 SAM 모델은 준비 단계에서 시작한다. 이 단계는 학습자에 대한 배경 정보를 수집하는 데 사용된다. 이것은 일반적으로 학습자의 강점과 약점을 조사하고, 고유한 사전 지식에 대해 배우고, 프로젝트의 전반적인 목표를 설정하는 것으로 구성된 빠른 단계이다. 준비 단계는 SAVVY 시작이라고 하는 것으로 끝난다. SAVVY 시작은 모든 이해 관계자가 교육 설계 및 잠재적인 교육 방식에 대해 브레인스토밍을 시작하고 모을 수 있는 기회이다. SAVVY 시작은 팀이 디자인 아이디어를 빠르게 교체하는 세션이다. 프로토타입은 일반적으로 SAVVY 시작이 끝난 후 추가 디자인 세션의 중추 역할을 하는 스케치 및 대략적인 스토리보드이다. 회의는 브레인스토밍, 신속한 프로토 타이핑, 반복으로 구성된다. SAVVY 시작이 끝날 때 팀은 각 콘텐츠 영역에 대한 잠재적인 설계를 제시해야 한다[56][57].

프로젝트가 반복적인 디자인 단계로 이동함에 따라 팀은 일반적으로 규모가 작아지고 주제 전문가 및 프로젝트 디자이너와 개발자로 좁혀진다. 이 단계는 프로

젝트 계획과 추가 설계로 구성된다. 프로젝트 계획 단계는 항상 SAVVY 시작 후에 이루어져야 하며 프로젝트 일정, 예산 (시간 및 비용) 설정 및 완료해야 하는 작업 할당으로 구성된다. 예를 들어, 특정 교수자는 스크립트 작성, 교육 계획 설계를 담당하고 다른 교수자는 교육 자료의 실제 개발을 담당할 수 있다[58].

프로젝트 계획이 완료되면 팀은 이제 추가 설계를 진행할 수 있다. 이것은 프로젝트 설계 결정이 내려지고 교육 구성 요소가 더 세련되고 가시적으로 될 때이다. 추가 설계 단계에서는 SAVVY 시작에서 내린 초기 설계 결정을 사용하고 합의된 설계 증명을 얻을 때까지 추가로 반복한다. 하나의 콘텐츠 영역에 대해 디자인 팀(team)은 세 가지 잠재적인 디자인을 만들기 위해 노력해야 한다. 그 이유는 팀이 필요한 교육 구성 요소가 하나의 설계에만 집착하지 않기 때문이다. 기본적으로 팀을 창의적이고 명백한 디자인 솔루션 이상으로 생각하도록 확장한다. 처음에는 어려울 수 있지만 결국 전체 교육과정 설계를 향상시키는데 도움이 될 것이다[58].

팀이 합의된 설계를 가지면 프로젝트는 개발, 구현 및 평가의 지속적인 루프로 이동한다. 이 단계에서는 최종 사용자가 피드백을 제공할 수 있는 유용한 정보를 항상 확보할 수 있도록 완료된 프로젝트의 작은 청크를 개발하는 것이 중요하다. 이것은 SAM의 가장 큰 차별화 요소 중 하나이다. 피드백을 받기 위해 프로젝트가 끝날 때까지 기다리는 ADDIE와 달리 SAM은 학습자가 모든 단계에서 사용하고 상호 작용할 수 있는 유용한 기능을 항상 가지고 있다[57].

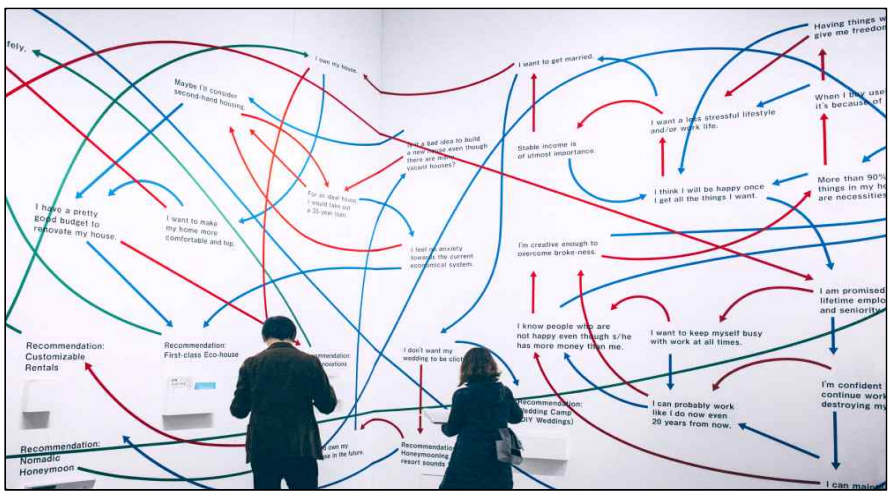
알파 단계는 완전히 완료된 프로젝트의 첫 번째 버전 역할을 한다. 이 단계에서는 코스의 모든 구성 요소를 처음부터 끝까지 사용할 수 있다. 여기에는 미디어 및 형성 피드백 루프 형태의 학습자 상호작용이 포함된다. 이 단계에서 주요 과정 결함을 발견해서는 안 되지만 사소한 편집 기회가 나타나는 것은 여전히 흔하다.

베타 및 골드 릴리스 단계는 SAM 내의 최종 구성 요소이다. 베타는 피드백과 최종 검토를 기반으로 한 수정된 알파 버전이며 베타는 알파 단계의 피드백을 기반으로 프로젝트를 검토하고 수정할 수 있는 마지막 기회이다. 최종 수정이 이루어지면 프로젝트는 골드 릴리스로 이동하고 전체 배포 준비가 된다[58].

결론적으로 SAM을 사용하면 교육 설계자가 코스를 조기에 많은 테스트 하고 사용자 피드백을 기반으로 수정에 기민하게 대응할 수 있다. 이는 학습 목표에 유연하게 대처할 수 있으며 프로젝트의 완결성을 보장할 수 있다.

3.1.4. 시나리오 기반 교수·학습 모델 연구·분석

시나리오 기반 학습(Scenario-Based Learning: SBL)은 시나리오를 사용하여 문제 기반 또는 사례 기반 학습과 같은 능동적 학습 전략을 지원하는 것이다. 일반적으로 학생들이 해결해야 하는 비구조적이거나 복잡한 문제를 기반으로 한 스토리라인을 따라 작업하는 과정을 포함한다. 교육 시나리오는 과정의 교육과정을 설명하고 이 과정에서 교사를 안내하는 것을 목표로 하는 구조화된 계획을 구성하기 때문에 기본적으로 교육 경험의 형식과 내용, 즉 학습 결과, 교육 이론, 오리엔테이션 등을 정의한다고 볼 수 있다. 시나리오 기반 학습은 발생하는 모든 것이 학습자의 선택을 반영하기 때문에 학습자가 현실적인 작업 과제를 해결하고 진행하면서 현실적인 피드백을 받는 몰입형 교육 환경에 용이하다. 학습자가 텍스트를 읽고 시험을 치르며 수동적으로 정보를 습득하는 기존의 교육 학습 방법과 달리 시나리오 기반 교육에서는 수업의 처음부터 끝까지 과정에 적극적으로 참여할 수 있도록 흥미를 유도한다. 시나리오와 역할에 몰입한다는 점은 롤 플레이(Role-playing Game: RPG) 방식의 게임이 갖는 장점과 같은 맥락이라고 할 수 있다[59][60]. 이는 동시에 대화만으로도 몰입감 있는 경험을 만들어 학습에 적용할 수 있는 영감을 주는 사례이기도 하다[60][61].



[그림 Ⅲ-3] 시나리오 기법 학습 예시[60]

시나리오 기반 학습을 통해 얻을 수 있는 시나리오 구성 방식은 특정 시점에 내려진 결정이 이후의 상황에 영향을 미치는 경우와 학습의 방법이 분석과 문제 해결 기술을 요구하는 경우, 그 문제에 대한 한 가지 명확한 해결책이 없는 경우와 마지막으로 실습을 하기 어려운 경우에 유용하게 활용 할 수 있다. 따라서 시나리오 기반 학습법은 군대에서, 경찰 및 조종사, 수술을 해야 하는 외과 의사와 같은 직업군에서 시뮬레이션 기법으로 앞에서 언급된 직업 외에도 실수의 대가는 매우 클 수 있는 현장에서 유용하게 활용되어 왔다.

시나리오 기반 과정은 실제 경험을 대체할 수 없지만, 학습자는 최소한 신체적 상해나 기타 심각한 결과의 위험 없이 모의 환경에서 실수를 용인하고 실수로부터 배울 수 있는 학습을 할 수 있다. 시나리오 기반 학습은 실제 작업 상황에 몰입하여 학습자에게 현실감을 주기 때문에 재미있고 흥미롭다. 동시에 실수는 훈련 과정의 일부로서 학습자들이 실수에 낙담하지 않도록 안전한 환경을 제공하기 때문에 학습자가 수동적으로 정보를 흡수하는 것이 아니라 모든 감각을 동원하고 생각하고 결정하도록 장려할 수 있다[62].

이러한 기능은 의무 준수 교육 유형과 같은 흥미가 떨어지는 상황에서 특히 중요하다. 모든 시나리오 기반 학습이 '폭탄 불능화를 위한 레드 와이어 절단'과 같은 극한 상황에서 효과를 드러내는 것만은 아니다. 즉시 효과가 나타나지 않을 수도 있는 상황에서도 시나리오 기반 교육을 통해 시간을 단축하고, 실제로 가까운 미래에 나타날 조치도 결과에 맞게 조정할 수 있다. 자동차 진단 과정을 수강하는 학습자들은 자신의 판단이 옳았는지 알기 위해 엔진 부품이 배송되고 교체될 때까지 기다릴 필요가 없다. 설득력 있는 시각효과만으로는 약한 시나리오를 소화해낼 수 없으므로 좋은 대본을 만드는 것이 전체 과정에서 가장 어려운 부분이다. 시나리오 기반 학습 훈련을 할 때 주의해야 할 5가지 사항은 다음과 같다[63].

첫째, 그 분야 전문가의 기본적인 가이드가 필요하다. 학습자는 매일 처리해야 할 세부 사항을 모르는 강사나 공장처럼 기계적으로 콘텐츠를 제작하는 아웃소싱 업체가 만드는 과정을 바로 발견할 수 있다. 여기서 문제는 시나리오를 적절하게 만들고 가상 캐릭터가 동료, 고객, 환자 등 실제 사람처럼 보이게 하는 것이다. 주제 전문가가 중추적인 역할을 하는 곳이다. 전문가는 학습자에게 문맥을 알려주고, 가장 흔한 실수를 공유하며, 학습자의 표현이 정확하고, 치명적인 실수를 저지르지

않도록 할 수 있다.

둘째, 시나리오 캐릭터를 실제 사람으로 생각하는 것이 전체 훈련을 더 효과적으로 만들 수 있다. 학습자가 캐릭터에 현실적인 이름을 붙이는 대신 역할에 대한 이름 즉 '클라이언트'이나 '관리자' 등으로 대한다면, 과도한 몰입이 줄 수 있는 불편한 상황에서 분리된 판지 모양의 인물일 뿐이라는 것을 인지할 수 있다.

셋째, 기분이 아닌 행동으로 설명한다. 상황을 드러내는 가장 분명한 방법은 그 상황이 어떻게 보이는지 묘사하는 것이다. 감정적인 부분이 드러나게 되면 이는 자칫 부자연스럽고 너무 말이 많거나 어설프게 들릴 수 있기 때문에, 학습자가 직접 말하는 것으로 상황을 드러낸다면 시나리오를 좀 더 현실감 있게 만들 수 있다. 이는 피드백을 주거나 받게 되는 상황에서도 질문이 훌륭하더라도 "맞아!" 또는 "잘못했어, 다시 해봐"라는 기계적인 피드백보다는 성과를 보여주게 된다.

넷째, 시나리오 기반 학습의 전체 아이디어는 상황을 분석하고 결정을 내리기 위해 자기 능력을 최대한 활용해야 하는 학습자를 중심으로 하기 때문에, 충분한 단서 즉 도움이 되는 동시에 산만하게 할 수도 있는 것을 만들어 실제로 분석해야 할 내용을 가지고 있어서 알아챌 수 있는 신호를 남기는 것이 중요하다. 시나리오가 학습자가 해야 할 일에 집중되어 있을 때, 다른 방법으로 작성할 수 있는 옵션의 범위를 의도적으로 좁히는 대신, 학습자들이 해야 할 일을 하지 않는 이유에 집중하도록 노력하게 되면 문맥을 느낄 수 있고 질문과 옵션 모두에 흥미로운 세부 사항을 제공할 수 있다. 만약에 문맥을 잘 모를 때는 질문이 너무 일반적이고 지루하게 들린 수 있어서 상황에 더 가까이 관심을 기울이는 것은 대개 흥미로운 선택지를 만들어내는 데 도움이 된다.

마지막으로 학습자가 실패하게 해야 한다. 실수를 저지르고 다양한 관점을 안전하게 경험할 수 있다는 것이 시나리오 기반 교육을 매우 중요하고 흥미롭게 만들기 때문에 어느 정도 믿을 수 있는 어려운 상황을 만들고 학습자가 어떤 일이 일어날지 보기 위해 오답을 선택하게 하는 것이 교육을 구상하는 사람으로서의 역할이 된다. 그렇기 때문에 학습자가 현실에서 실수하지 않도록 하기 위해 항상 '공통적인 실수' 옵션을 모색하고 추가할 가치가 있는 것이다.

[표 Ⅲ-1] 시나리오 플랜의 절차

단계	결정요소	기법
핵심이슈 선정	중요도, 시급성, 사회이슈	브레인스토밍
의사결정요소 도출	시장크기, 성장률, 물가전망	통계기법
변화동인 규명	의사결정요소의 상세동인	PEST, 5Force
시나리오 도출	변화동인기반 시나리오도출	불확실성 메트릭스
시나리오 쓰기	시나리오를 기술하고 대응책 기술	시나리오 기술서
대응전략 수립	각 시나리오별 의사결정트리 형식의 대응책 마련	Logic tree, MECE, 의사결정트리
모니터링	시나리오 예의주시	조기경보

3.1.5. 블렌디드 러닝 교수·학습 모델 연구·분석

블렌디드 러닝(Blended Learning)은 이러닝(e-learning)의 확대로 그 한계성이 인식되면서 이를 극복하기 위해 고안된 방식이다. 이러닝은 1990년대 이후 기술의 발달과 컴퓨터의 보급이 일반화되면서 본격적으로 시작되었다. 이는 교육의 효율성을 높이고 시간과 장소의 구애 없이 다양한 학습자들이 참여할 수 있는 교육 형태로 각광을 받았으나, 교수자 중심의 내용 전달 위주로 진행되어 학습자들의 학습 성취도에 크게 영향을 주지 못했다는 비판을 받기도 했다. 이에 온라인과 오프라인 학습의 블렌딩을 통해 다양한 교육 경험을 제공하고 지식 접근에 대한 용이성을 높이는 블렌디드 러닝의 중요성이 높아졌다[64].

특히, 2019년 발발한 COVID-19의 영향으로 학생들의 등교 일정이 변화하고, 원격 학습이 일반화되면서 확장된 교실 환경에 맞춰 교육의 효과성을 높일 수 있는 수업 체계 도입이 필요하게 되었다. 본 논문의 비대면 블렌디드 러닝은 본래의 블렌디드 러닝에서 '비대면'에 초점을 맞춘 교수 설계 방식으로 정의한다. 성공적인 비대면 블렌디드 러닝이 이루어지기 위해서는 블렌디드 러닝의 수업 설계 영역과 그 요소를 정확히 파악하고 이를 고려하여 수업을 설계함이 필요하

다. 김주영(2005)은 블렌디드 러닝의 영역과 그 요소를 10가지로 분류하였다. 분류된 연구 결과를 살펴보면, 블렌디드 러닝의 수업 설계 영역은 교실 현장과 온라인 학습의 영역이 포함되어 있으며, 활용되는 교수·학습 전략도 일반적인 강의식 수업에 더하여 토론식, PBL 등의 활발한 의사소통이 가능한 전략이 수반된다. 또한, 디지털 기반의 다양한 학습 매체를 활용한 수업이 가능하며, 평가 방법 영역에서도 전통적인 자필 평가 방식과 더불어 자기 성찰 평가와 과정 중심의 수행 평가를 그 요소로 포함하고 있다. 본 논문에서는 김주영(2005)이 제안한 블렌디드 러닝 수업 설계 영역과 요소에서 '비대면'을 부분을 강조하여 수정하였다. 자세한 비대면 블렌디드 러닝의 수업 설계 영역과 요소는 다음 표와 같다[65].

[표 Ⅲ-2] 블렌디드 러닝 수업 설계 영역과 요소

영역	요소	영역	요소
학습 환경	• 온라인 사이버 학습 • 오프라인 교실 학습	학습 형태	• 개별 학습 • 협동 학습 • 일체 학습
학습 목표	• 인지적 목표 • 정의적 목표 • 심체적 목표	학습 매체	• 텍스트 자료 • 오디오 기반 매체 • 비디오 기반 매체 • 멀티미디어 기반 매체 • 컴퓨터·인터넷 기반 매체 • 실감미디어 기반 매체
학습 내용	• 구조화된 학습 내용 • 비구조화된 학습 내용	상호작용 유형	• 학습자 – 학습 내용 • 학습자 – 교수자 • 학습자 – 학습자 • 학습자 – 커뮤니티
학습 시간	• 실시간 • 비실시간 • 실시간과 비실시간 병행	평가 방법	• 자필 평가 • 자기 성찰 평가 • 수행 평가
학습 장소	• 교실 수업 • 교실 밖 체험 현장 수업 • 온라인 수업을 할 수 있는 PC나 태블릿이 있는 장소	교수·학습 전략	• 강의식 • 토론식 • PBL • 플립러닝 등

비대면 블렌디드 러닝의 수업 실천을 위해서는 먼저, 학교 안팎의 교육자원을 파악하고 개별 학생의 역량과 요구를 진단하는 것으로 시작한다. 본 단계에서는 단위 학교와 가정에서의 온라인 학습을 위한 환경 준비 상태와 활용 역량을 파악하고 학습자의 특성을 고려하여 적합한 교육플랫폼을 선정한다. 이후, 비대면 블렌디드 러닝의 관점으로 교육과정의 전체적인 흐름 속에서 교과별 온·오프라인 시수를 분배하고 학습량 적정화를 고려하여 성취기준을 살펴본다. 이러한 단계를 거쳐 온라인과 오프라인이 병행되는 학습 상황 속 학생들에게 맥락 화 된 학습 경험의 제공을 위해 교수·학습 및 평가 계획을 설계한다. 맥락 화 된 학습 설계를 바탕으로 학습 과정과 결과에 대한 학습자 맞춤형 피드백을 고려하여 설계한다. 본 과정에서 피드백은 성취 목표, 학습자의 학습 수준, 학습 전략을 종합하여 제공하는 것이 필요하다. 마지막으로 교육과정-수업-평가가 연계된 비대면 블렌디드 러닝 운영 결과에 대해 학습자와 교수자가 함께 소통하는 과정으로 마무리된다.

3.2. 제안하는 하이브리드 블렌디드 실천모형 디자인

하이브리드 블렌디드 실천모형은 3.1. 에서 언급된 여러 가지 모형의 단점을 극복하여 개발되었고 시나리오 학습기법과 SAM 모형의 수업 설계 절차를 주축으로 비대면 블렌디드 러닝, 맞춤형 교수·학습법을 혼합하고, 지능정보사회에 대응하기 위해 첨단기술 콘텐츠를 교수 내용으로 적용한 수업 설계를 바탕으로 정보보안 교육을 진행하는 실천적 모형이다.

본 모형은 지능정보사회 대비 학습자의 역량을 강화하기 위하여 변화하는 교실 환경에서 역동적으로 적용할 수 있으며, 혁신적 교수학습법에 대한 이해를 기반으로 DNA(Data, Network, AI)와 같은 첨단기술을 활용하여 초개인화 학습, 협동 학습 등의 연계가 가능하다. 이는 정보보안 교육의 안정적인 현장 착근과 새로운 교육 프로그램의 구상으로 을 목적으로 한다.

하이브리드 블렌디드 실천모형의 수업 설계는 SAM 모형의 계획-개발-평가의 수업 설계 절차와 비대면 블렌디드 교수학습법의 학교 안팎의 교육자원 파악-개별

학생의 역량과 요구진단-블렌디드 러닝 관점의 성취기준 정립-온·오프라인 병행의 맥락 화 된 학습 설계(수업 재구성)-학생 맞춤형 피드백 블렌디드 러닝 환류, 맞춤형 학습지원-협동 학습 지원-교수학습 평가-교수학습 개선을 혼합하여 준비(Ready)-설계(Set)-실행(Go)-평가(Review)의 단계로 구성하였다.

이에, 준비(Ready) 단계에서는 본격적인 수업 설계를 위해 학교 안팎의 교육자원을 파악하고 인공지능 도구를 활용하여 개별 학생의 역량과 요구진단, 학생별 특성 분석, 학생별 학업 분석을 시행한다. 또한, 가입(Enroll)과 경험(Experience) 요소를 유념하여 학생들의 주의를 끌고 학습의 결과가 실생활에 전이될 수 있도록 수업을 준비한다.

설계(Set) 단계에서는 온·오프라인 수업이 가능할 수 있도록 성취기준을 정립하고 맥락 화 된 학습 설계를 위해 구체적으로 성취 가능한 학습 목표를 설정하고 목표 달성 지원 계획을 수립한다.

실행(Go) 단계에서는 학습자의 학습 요구와 교과 특성을 고려하여 교수학습을 설계하고, 교수학습 방법과 맞춤형 학습지원 도구와 방안을 추천한다. 본 단계에서 팀별 학습을 할 경우도 고려하여 협력학습을 위한 지원 도구와 피드백을 제공할 수도 있다. 또한, 수업 개발에서 학습자의 다중지능과 감각을 깨우는 정보(Label)의 전달과 실습(Demonstrate)의 요소를 포함하는 것이 중요하다.

마지막 평가(Review) 단계에서는 인공지능을 활용하여 교수학습 수준을 평가하고, 학생 맞춤형 피드백을 설계하여 제공한다. 이 과정에서 개발된 수업을 향후 개선할 수 있는 방향을 설정하고 결과를 환류하게 된다. 학습자에게는 수업을 마무리하며 복습(Review)으로 학습의 결과를 장기 기억할 수 있게 하고, 배운 과정과 결과를 축하(Celebrate)하여 학습을 긍정적인 기억으로 연계하여 교육의 효과를 높일 수 있도록 한다. 또한 모든 평가 단계에서는 한국형 인터내셔널 바칼로레아(International Baccalaureate: IB) 평가를 적용하여 국제적 수준의 과정 중심 평가 시스템을 도입한다. 이러한 수업 설계 절차는 교사의 편의에 따라 유연하고 빠르게 적용할 것을 권한다. 특히, 준비와 계획 단계에서는 애자일(Agile) 방법론을 적용하여 프로토타입(Prototype)을 개발해보고 반복적으로 시정하면서 점차 완성된 수업으로 발전할 수 있다. [표 Ⅲ-3]은 상기 기술한 하이브리드 블렌디드 모형의 수업 설계 단계를 도식화한 것이다.

[표 Ⅲ-3] 하이브리드 블렌디드 모형의 수업 설계 단계

SAM MODEL	비대면 블렌디드	다학문적 맞춤형	시나리오
계획	학교 안팎의 교육자원 파악	가입(Enroll)	학생별 학습 유형 분석
	개별 학생의 역량과 요구진단	경험(Experience)	학습 전략 추천
개발	블렌디드 러닝 관점의 성취기준 정립	정보(Label)	학습 목표 설정
			목표 달성 지원
	온·오프라인 병행의 맥락 화 된 학습 설계 (수업 재구성)	실습 (Demonstrate)	교수학습 설계
			교수학습 지원
			맞춤형 학습지원
평가	학생 맞춤형 피드백 설계	복습(Review)	협력학습 지원
	블렌디드 러닝 환류	축하(Celebrate)	교수학습 평가
			교수학습 개선

하이브리드 블렌디드 모형 수업 단계
<Ready> 학교 안팎의 교육자원 파악, 개별 학생의 역량과 요구진단, 가입(Enroll), 경험(Experience), 학생별 학습 유형 분석
<Set> 계획, 블렌디드 러닝 관점의 성취기준 정립, 온·오프라인 병행의 맥락 화 된 학습 설계(수업 재구성), 학습 목표 설정, 목표 달성 지원
<Go> 개발, 정보(Label), 실습(Demonstrate), 교수학습 설계, 교수학습 방법 추천, 교수학습 지원, 맞춤형 학습지원, 협력학습 지원
<Review> 학생 맞춤형 피드백 설계, 블렌디드 러닝 환류, 복습(Review), 축하(Celebrate), 교수학습 평가, 교수학습 개선, 한국형 IB 평가

Ⅳ. 초등 정보보안 교육 프로그램 개발과 실증

4.1. 하이브리드 블렌디드 실천모형 기반 초등 정보보안 프로그램 구성

하이브리드 블렌디드 실천모형은 교육의 콘텐츠로 다양한 미래 첨단기술 중 정보보안 기술을 그 주제로 삼고 있다. COVID-19의 창궐로 뉴노멀 시대로의 전환이 급격하게 이루어지고 있는 시대 상황에서 미래 예측에 대한 중요성이 증가하고 있다. 이에, 미래 사회에 일어날 수 있는 여러 이슈를 조망하고 이에 대응할 수 있는 유망기술 분야를 이해하고 관련 인재를 육성하는 것이 어느 때보다 중요한 시점이다.

한국과학기술기획평가원(2021)에서는 기업 간담회 및 특허 분석 등을 통해 10대 미래 유망기술을 선정하였는데, 이를 정리해보면, 첨단 의료기술, 인공지능 관련 기술, 정보보안, 메타버스 초실감 미디어 기술 등으로 나누어 볼 수 있다[66]. (① 비침습 생체정보 기반의 심혈관 질환 관리 기술, ② 교통약자를 위한 Level 4 자율주행 자동차, ③ LXP 기반의 개인 맞춤형 큐레이션 기술, ④ 자율주행 기반의 라스트마일 딜리버리서비스, ⑤ 지능형 엣지 컴퓨팅, ⑥ VR/홀로그램 기반 실시간 협업 플랫폼, ⑦ 인터페이스의 벽을 허무는 Beyond Screen 기술, ⑧ 초연결 시대의 사이버 지킴이, 인공지능 보안기술, ⑨ 비대면 초실감 미디어 제작 및 중계 기술, ⑩ 온라인 쇼핑 쓰레기를 줄이는 녹색포장 기술)

앞서 2장에서 언급한 디지털 네이티브 세대인 초등학생이 미래 사회에 걸맞은 인재로 성장하기 위해서는 앞에서 언급된 미래 유망기술에 대한 기술 지식을 체계적으로 교육해야 한다는 것은 많은 해외 사례를 보아도 알 수 있다. 미래 사회 인재로 성장하기 위해서는 기술 지식의 습득이 우선시 되겠지만, 초등학생에게 전문적인 기술 지식을 교육하기 여간 까다로운 것이 아니다. 하이브리드 블렌디드 실천모형을 기반으로 하여 본 논문에서 제안하는 교육 프로그램들은 초등학생이 흥미를 잃지 않고 기술의 습득을 할 수 있는 방법을 모색하기 위해 현재 가장 많이 접하는 스마트 미디어가 가진 기술에 대해 주목했다.

첫 번째로, 모바일 디바이스가 가지고 있는 생체 인증 방식이다. 생체 인증 방

식은 편의성을 위해 적용을 확대하고 있는 추세로, 청소년층의 스마트 디바이스 사용층에서도 기기의 신원 확인 인증을 위해 본인의 생체정보를 활용할 수 있으며, 특히 얼굴 영역에 기반한 안면인식 기술의 사용이 보편적으로 사용된다.

모바일 디바이스 생체정보 기반 인증 방식은 2013년부터 시작되어 지문, 홍채, 안면인식과 같은 다양한 기술들이 접목되어 사용되고 있다. 모바일 디바이스 시장 중에서 가장 큰 소비자 그룹을 가지고 있는 애플사(社)의 경우 2013년도 출시한 아이폰 5S에서부터 지문인식 기술이 적용되었으며, 삼성사(社)에서는 2014년 출시한 갤럭시S5에서부터 지문인식 기능을 추가하였다. 이처럼 초기에는 지문인식에 기반한 생체 인증 시스템으로 휴대폰의 인증을 사용하였으나, 현재에는 안면인식 기반의 인증 시스템이 대중화되어있다[67].

[그림 Ⅳ-1] 모바일 디바이스 생체 인증 역사[67]

[그림 Ⅳ-1]은 모바일 디바이스 중에서도 상위 2개 기업의 생체 인증 시스템 도입 역사를 보이는 것이다. 모바일 디바이스의 생체정보는 단순히 기기에 대한 사용자 인증 수단만이 아닌 모바일 디바이스를 이용하여 사용하는 서비스에 대한 인증 수단으로도 적용되고 있다.

모바일 디바이스 사용자의 연령층이 낮아짐은 저연령층의 컴퓨팅 능력을 향상시킬 수 있으며, 검색 엔진을 사용한 지식의 습득이 수월하다는 순기능을 가지고 있으나, 모바일 디바이스의 역기능에 대해서는 취약한 모습을 보인다. 특히, 데이터 수집을 위해 파일을 다운로드하는 과정에서 명확한 출처가 밝혀지지 않은 애플리케이션이나 파일을 다운로드함에 따라 악성코드 또한 동시에 받아질 수 있다. 이처럼 사용자의 디바이스에 다운로드된 악성코드는 사용자 데이터 탈취부터 위변조까지 모바일 디바이스의 보안성에 큰 악영향을 끼칠 수 있으며, 이

과정에서 사용자의 생체정보가 유출되는 경우에는 오염된 생체정보를 향후 재사용이 어렵다는 문제를 동반한다. 이와 같은 생체정보를 활용하기 위해서는 [표 Ⅳ-1]과 같은 7가지의 특성을 충족하여야만 한다.

[표 Ⅳ-1] 생체인식기술에 활용되기 위한 7가지 고유한 특성[68]

특성		설명
일반적으로 갖추어야 할 특성	보편성(Universality)	모든 사람이 가지고 있는 생체특성이어야 함
	유일성(uniqueness)	같은 특성을 가진 사람이 없어야 함
	영구성(permanence)	절대 변화하거나 변경되지 않아야 함
	획득성(Collectability)	센서로부터 생체특성 정보 추출 및 정량화가 용이함
신뢰성을 높이기 위한 추가적인 특성	정확성(Performance)	시스템에 정확도, 처리 속도, 내구성 등
	접근성(Acceptability)	시스템에 대한 거부감을 느끼지 않는 정도여야 함
	기만성(Circumvention)	정상적으로 시스템을 속이기가 용이한 정도

[표 Ⅳ-1]은 정보통신정책연구원에서 생체인식 기술 활용을 위한 7가지 고유특성을 보이는 것으로, 일반적인 생체정보는 개인을 식별할 수 있는 신체정보이기에 단시간 내에 큰 변화를 가질 수 없으며, 세월의 흐름에 따라 장기간에 걸쳐 변화를 나타낸다[68]. 하지만, 이와 같은 특성은 생체정보의 유출이 발생하는 경우 큰 문제가 될 수 있다. 생체정보는 그 특성상 단기간에 변경할 수 없으며, 한번의 유출로 치명적인 피해를 일으킬 수 있다는 단점을 가진다. 따라서, 안면 정보와 같은 생체정보를 사용하는 사용자는 정보 활용에 신중해야 한다.

또한 이에 대한 인식은 성인층에서도 크게 인지하지 못하고 있으며, 저연령층의 모바일 디바이스 사용자는 생체정보 유출의 피해를 이해하기 어렵다. 이와 같은 문제를 해소하기 위해서는 저연령층의 모바일 디바이스 사용자를 대상으로 모바일 디바이스 사용의 위험성을 눈높이에 맞춰 교육할 수 있어야 한다. 따라서 본 논문에서는 안면인식 기술 원리를 체험해보는 활동을 통해 안면인식 기술의 핵심원리를 학생들이 쉽게 이해할 수 있도록 교육 프로그램을 설계했다.

두 번째로는 이와 같은 모바일 디바이스는 사용자의 신원을 증명하기 위한 안전한 인증 수단을 요구하고 있으므로 블록체인의 분산 신원 증명(Decentralized Identity, DID) 기술에 주목하였다. COVID-19 사태에 의해 기존의 오프라인 중점의 사회가 점차 온라인 중점의 사회로 변화하고 있으며, 이 과정에서 사용자의 신원을 증명을 요구하는 과정이 온라인에서 증가함에 따라 기존의 물리적인 실물 신분증의 한계가 뚜렷해지고 있다. 온라인 환경에서의 개인정보 및 데이터의 주권이 주요한 화제로 떠오름에 따라 최근에는 분산 신원 증명이 큰 화두가 되고 있다[69]. 분산 신원 증명은 직접 사용자의 신원을 확인하는 오프라인 증명과 달리 인증을 진행하는 대상자를 직접 확인하는 것이 어렵다. 분산 신원 증명은 블록체인을 활용하여 사용자를 인증하는 기술을 의미한다. 블록체인은 데이터를 분산된 환경에 기록하여 데이터의 무결성을 강화하는 기술로 사용자 각각이 독립된 하나의 디바이스를 사용하기 때문에 분산 환경에 참여하는 모바일 디바이스 환경에 적합하여, 향후 보안성 강화를 위한 요소로써 주목된다. 특히 블록체인은 외부자에 의한 무분별한 데이터 위변조를 방지한다는 측면에서 인증 시스템에 적용하기 위한 연구 및 상용화 시도가 증가하고 있다.

따라서 본 논문에서는 현재 모바일 디바이스의 인증 시스템의 한계를 해결하기 위한 기술로 DID 기술을 선정하고, 이를 피 학습자를 대상으로 교육하여 피교육자에게 친숙한 모바일 디바이스의 문제를 확인하고, 이를 해결하는 과정을 교육함으로써 학습자 스스로 문제를 해결할 수 있는 컴퓨팅 능력을 향상시킬 수 있는 교육과정의 요소 기술로 블록체인 기술을 선정하였다[70].

마지막으로 해킹 원리교육을 모바일 디바이스를 주로 사용하는 미숙한 사용자에게 필요한 정보보안 교육 프로그램으로 선정했다. 2020년 3월 세계경제포럼(World Economic Forum)에서 폴 미(Paul Mee) 사이버보안 대표위원은 “만 3세에서 4세 사이 어린이의 절반이 가정에서 인터넷을 사용하며 이들이 성장해서 4명 중 1명은 18세가 되기 전에 신원 도용이나 사기, 사이버 폭력을 경험하게 된다는 2019년 미국 국립교육통계센터(National Center of Education Statistics)의 통계를 인용하면서 초등 사이버보안 교육의 중요성에 대해 피력하였다[71].

모든 정보가 디지털화되는 시기에서 정보는 곧 엄청난 가치를 가지게 되고, 정보의 가치가 높아질수록 해킹의 위험에서 벗어나기 어렵지만, 국내의 경우 어느

장소를 방문하더라도 쉽게 와이파이 환경에서 무료 데이터를 사용하게 되고, 이는 정보보안에 매우 허술한 통로가 된다. 따라서 네트워크 해킹을 알고 여러 종류의 네트워크 해킹의 위험에 대비하는 것이 중요하다.

본 논문에서는 초등학생 학습자를 대상으로 모바일 디바이스의 이해를 돕고, 모바일 디바이스 정보 유출의 위험성을 이해할 수 있도록 유도하며, 향후 모바일 디바이스의 보안성을 강화하는 방안을 소개함으로써 초등교육과정의 학습자에게 교수할 수 있는 학교 선생님과 학교 관리자를 대상으로 폭넓은 교육 방법을 제시하였다. 이는 디지털 네이티브 세대가 본 세 가지의 교육과정에 대해 이해하고 학습하여 위험을 인지할 수 있고, 이를 해결하는 방안으로 2015 개정 교육과정 중 정보 과목에 대체 단원으로 활용할 수 있도록 기대한다.

이처럼 본 논문에서는 초등 정보보안 교육 프로그램은 하이브리드 블렌디드 실천모형을 기반한 안면인식 핵심원리, 블록체인 핵심원리, 해킹 핵심원리 교육 프로그램으로 총 세 가지의 개별적인 정보보안 교육 프로그램을 제안하였다. 제안된 교육 프로그램의 특징으로는 선정된 교육의 콘텐츠가 정보보안 분야에서 자주 활용되고 미래 유망한 기술이며, 학생들이 이해하기 쉽도록 정보보안 기술의 핵심원리를 다양한 교수학습자료와 학습 게임 등으로 설계한 것이 특징이다.

이에 따라, 4.2. 절에서는 안면인식 핵심원리 교육 프로그램 개발과 적용 결과를 다루고 있다. 해당 교육 프로그램은 순서도, 리치픽처 등 다양한 창의적 교수학습활동을 통하여 흥미로운 방식으로 인공지능 기술을 활용한 안면인식 기술을 이해할 수 있도록 설계되었다. 총 3차시에 걸쳐, 안면인식 기술의 원리 및 개념을 이해하고 인공지능의 판단 과정을 인식하며 안면인식 기술을 체험하는 활동을 통해 구성주의 학습을 실현할 수 있다. 본 논문에서 설계한 교육 프로그램은 현장 교원을 대상으로 시범 적용되었으며, 교육 프로그램 인식조사를 수행하여 교육 효과를 파악하였다.

4.3. 절에서는 블록체인 핵심원리 교육 프로그램을 개발하고 시범적으로 적용한 결과를 보여준다. 본 논문의 교육 프로그램은 마인드맵과 같은 창의적 교수법을 적용하였으며, PBL(Problem-Based Learning)을 적용한 프로그램으로 구성하였다. 교육 프로그램의 내용 체계는 1차시에서는 블록체인 핵심원리 개념에 대하여 교수하며, 2차시에는 블록체인 학습 게임을 실시한다. 3차시에서는 교수자가

가상으로 설정한 블록체인 위조 및 변조 문제 상황을 극복할 수 있는 창의적인 문제 해결 방안을 제시하는 것으로 설계하였다. 이러한 교육 프로그램은 전국의 초등학생을 대상으로 적용되었으며, 창의적 문제해결력을 조사하여 정보보안 창의 융복합 인재 양성 목표에 대한 본 교육 프로그램의 효과성을 분석하였다.

4.4. 절에서는 정보보안 기술 중 해킹 원리 핵심 기술 교육 프로그램을 개발하고 적용한 결과를 나타내고 있다. 교육 프로그램은 학습 게임을 구상하여 게임에 초점을 맞춰 설계하였으며, 해킹 원리 이해, 해킹 원리학습 게임 수행, 해킹과 정보보안 교육의 중요성이 포함된 3차시의 과정으로 구성하였다. 설계한 교육 프로그램은 초등학교 관리자를 대상으로 적용되었으며, 만족도 조사를 시행하여 적용 결과를 분석하였다.

4.2. 안면인식 핵심원리 교육 프로그램

안면인식은 기술을 통해 사람의 얼굴을 인식하는 방식이다. 안면인식 시스템은 생체인식을 사용하여 사진이나 비디오에서 얼굴 특징을 맵핑하며, 일치하는 안면의 특징을 찾기 위해 알려진 얼굴의 데이터베이스와 정보를 비교한다. 안면인식 기술 시장은 2017년 40억 달러에서 2022년 77억 달러로 성장할 것으로 예상된다. 안면인식은 많은 상용 응용 프로그램이 있기 때문이다[72]. 범죄자 감시에서 마케팅에 이르기까지 모든 분야에서 사용할 수 있기 때문이다.

안면인식 기술은 1960년대부터 본격적으로 시작되었다. 수학자이자 컴퓨터 과학자인 Woodrow Wilson Bledsoe는 얼굴 사진을 다양한 분류로 분류하는 데 사용할 수 있는 측정 시스템을 처음 개발했다[73]. 법 집행 기관은 곧 Bledsoe이 개발한 시스템에 관심을 갖게 되었고, 1970년대부터 1990년대까지 기관들은 자체적인 안면인식 시스템을 개발했다. 이것은 오늘날의 기술에 비하면 조잡했지만 이러한 시스템에 대한 작업은 현대적인 안면인식 프로그램으로 이어졌다. 2010년대가 되어서야 컴퓨터가 안면인식을 보다 표준적인 기능으로 만들 만큼 강력해졌다. 실제로 2011년에는 안면인식 소프트웨어가 테러리스트 오사마 빈 라덴의 신원을 확인했으며, 2015년, 볼티모어 경찰서는 프레디 그레이가 경찰 밴으로 이

송되는 동안 입은 척추 부상으로 사망한 후 시위에 참여한 사람들을 안면인식 기술을 사용하여 식별했다. 더불어, 날로 고도화되는 범죄 기술에 대응하기 위한 포렌식 사이언스(Forensics Science) 분야에서도 안면인식 기술이 광범위하게 활용되고 있다. 소비자는 이제 스마트폰 및 기타 개인 장치에서 안면인식을 사용한다.

2015년 Windows Hello와 Android의 Trusted Face를 통해 사람들은 얼굴을 조준하기만 하면 장치에 로그인할 수 있고, 애플사(社)의 iPhone X는 2017년 Face ID 얼굴 인식 기술을 공개하기도 했다. 이처럼 우리 실생활에 안면인식 기술은 다양하게 사용되고 있으며, 앞으로 CCTV 기술과 선제적 감시 시스템 등 더욱 발전할 것으로 예상된다. 그러나, 안면인식은 개인의 신원을 확인하는 데 도움이 될 수 있지만, 개인 정보보호의 취약성에 대한 문제도 꾸준히 제기되고 있다.

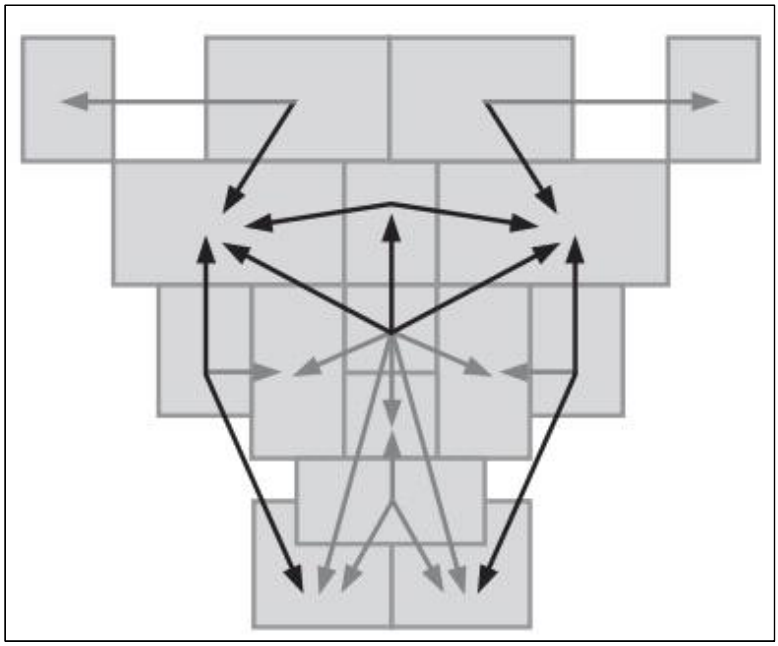
이에, 본 논문에서는 초등 정보보안 교육 프로그램 중 첫 번째로 인공지능을 적용한 지능형 CCTV와 모바일 기기에서 활용되는 안면인식 기술을 학습할 수 있는 교육 프로그램을 제안하는 바이다.

4.2.1. 교육 프로그램에 적용한 안면인식 핵심 기술

본 교육 프로그램에 적용한 핵심원리 기술은 얼굴 영역을 검출하는 알고리즘이다. 얼굴 영역의 검출에는 얼굴의 특정 영역에 대한 특징값에 기반한 검출을 수행한다. 이를 위한 알고리즘은 다양하게 연구되고 있으며, Knowledge-based method, Feature invariant approach, Template matching method와 같은 다양한 방안이 존재한다[74]. 이 중에서 본 교육 프로그램에서는 특정점을 기반으로 얼굴 영역을 검출하는 방식인 Template matching method를 기반으로 학습 과정을 설계하였다.

Template Matching method는 일반적인 표준 얼굴 패턴 정보를 사전에 추출한 데이터베이스를 구성하고, 이후 대상에 대한 입력 영상이 들어오는 경우, 사전에 추출한 영상정보의 템플릿과 상관관계를 분석하여 대상의 안면을 인식하는 기술을 의미한다[75]. 이때 사용되는 얼굴 패턴에는 얼굴의 형태, 눈, 코, 입과 같이 일반적인 요소들을 독립적으로 등록하여 사용하며, 각각의 독립 요소를 입력

영상과 비교한다. [그림 Ⅳ-2]는 Template matching method 기반의 얼굴 영역 검출에 대한 간단한 개념을 설명하는 것이다[72].



[그림Ⅳ-2] Template maching method 예시[72]

Template matching method는 구현이 용이하지만, 대상의 크기 변화나 회전에 의한 변화, 형태의 변화에 민감하게 반응하기에 실제 환경에서 대상자를 검출하기에는 문제가 있으나, 이를 보완하기 위해 다양한 연구가 진행되고 있다.

본 교육 프로그램에서 해당 기법을 사용한 이유는 궁극적인 교육의 대상자가 초등학교 고학년 수준의 저연령층이며, 고차원의 메커니즘에 대한 이해보다는 해당 기술의 개념에 대한 이해 수준을 요구하기 때문이다. 특히, 메커니즘의 수행 과정을 학습자가 직접 실행할 수 있기 때문에 본 교육과정에 적합하다고 판단하였다[76].

4.2.2. 안면인식 핵심원리 교육 프로그램 개발

(1) 개발 배경

현대 사회 모바일 기기의 보안기술에서 핵심적으로 쓰이는 원리로 지문, 홍채 인식과 더불어 안면인식 기술이 꼽히고 있다. 이는 사람의 얼굴 윤곽과 이목구비의 위치, 간격 등을 점으로 표시한 후 이를 연결하였을 때 생성되는 다각형을 기존에 기기에 등록된 다각형과 대조하여 유사도(일치율)가 일정 수준 이상이 되면 동일 인물로 인식하는 원리이다[4].

포렌식 사이언스(Forensic Science)란 '범죄조사에 적용하는 과학적 방법과 기술'을 의미한다. 첨단기술을 활용한 지문, DNA 분석, 혈흔 분석 등을 통한 범죄 현장의 증거물을 분석하는 것이 대표적인 포렌식 사이언스라고 할 수 있다. 포렌식 사이언스 분야 역시 꾸준히 발전하고 있으며 드라마, 영화 등을 통해 대중에도 점차 알려지고 있는 추세이다[77].

이에 따라 본 교육 프로그램에서는 포렌식 사이언스와 모바일 기기 보안기술에서 주로 사용되는 안면인식 기술 원리를 초등학교 수준으로 소개하고 실생활에서 활용되는 예를 제시하였다. 이를 통해, 안면인식 기술의 중요성을 알리며, 안면 정보 유출의 심각성에 대해 학생들이 인지하여 정보보안 역량을 함양할 수 있도록 개발되었다.

(2) 개발 절차

교육 프로그램 개발을 위해 하이브리드 블렌디드 실천모형의 수업 설계 절차에 따라 교육 대상을 먼저 선정하였으며, 현장에 맞춘 프로그램으로 개발할 수 있도록 2015 개정 교육과정에서 본 교육 프로그램과 연계할 수 있는 교과와 성취기준을 탐색하였다. 더불어, 학생들의 융합적 사고력 증진을 위하여 교육 프로그램에 접목할 수 있는 창의적 교수학습법을 모색하고 선정하였다.

교육 프로그램 설계에 필요한 선행연구 후, 교육 프로그램의 대상자는 초등학생으로 선정하였으며, 2015 개정 교육과정 중 초등학교 실과, 미술, 사회 등의 수업에서 연계할 수 있는 교육 프로그램으로 설계하였다. [표 Ⅳ-2]는 안면인식 기술 원리교육 프로그램과 연계된 2015 개정 교육과정 교과목과 성취기준이다[44].

[표 Ⅳ-2] 안면인식 핵심원리 교육 프로그램과 연계된 2015 개정 교육과정[44]

학교급	학년(군)	과목	영역(단원)	성취기준
초등학교	5-6학년 군	실과	기술 활용	**[6실 05-06]** 생활 속에서 로봇 활용 사례를 통해 작동 원리와 활용 분야를 이해한다.
초등학교	5-6학년 군	미술	체험	**[6미 01-04]** 이미지를 활용하여 자신의 느낌과 생각을 전달할 수 있다.
초등학교	3-4학년 군	사회	다양한 삶의 모습과 변화	**[4사 04-03]** 자원의 희소성으로 경제활동에서 선택의 문제가 발생함을 파악하고, 시장을 중심으로 이루어지는 생산, 소비 등 경제활동을 설명한다.

더불어, 창의적 교수학습법 중 말풍선과 그림 등 다양한 도구를 활용하여 주제를 자유롭게 표현하는 리치픽처 기법을 활용하여 학생들의 참여를 유도할 수 있도록 구성하였다. 리치픽처 기법은 상황을 탐색, 인정 및 정의하고 다이어그램을 통해 표현하여 예비 멘탈 모델을 만드는 방법이다. 또한, KEEP-STOP-BEGIN 표현법을 적용하여 토론을 시작하고 상황에 대해 폭넓고 공유된 이해에 도달하는 데 도움이 되며, 특히 복잡한 상황에 대한 인지와 표현을 할 수 있어 말로써 표현하기 어려운 본인의 의견을 풍부하게 표현할 수 있어 학습자 주도적 학습이 가능하도록 돕는다.

또한, 세부적인 학습 목표는 효율적으로 정보를 처리할 수 있는 정보처리 활용 능력 향상과 인공지능 활용 CCTV 알고리즘 이해, 안면인식 기술 원리 인식 제고로 정립하였다. 학습 목표에 따라 교육 프로그램은 3차시로 구성하였으며, 수업 차시에 따른 지도상의 유의 사항과 다양한 교육 자료를 제시하여 교육 프로그램 전개에 있어 교수자의 편의를 도모하였다. [표 Ⅳ-3]은 안면인식 핵심원리 교육 프로그램의 개발 절차를 나타낸다. 하이브리드 블렌디드 수업 설계 절차에

따라 수업 준비(Ready)에서는 교육 대상자를 선정하였으며, 수업 설계(Set)에서는 2015 개정 교육과정의 교과와의 연계성을 모색했다. 수업 실행(Go) 단계에서는 창의적 교수학습법을 모색하고, 학습 목표를 정립하였으며, 교육 프로그램을 실행하며, 수업에 필요한 교수학습자료를 제공한다. 마지막으로, 수업 평가(Review) 단계에서는 학생들의 성취도를 평가하고 학생 맞춤형 피드백을 제공한다.

[표 IV-3] 안면인식 핵심원리 교육 프로그램 개발 절차

하이브리드 블렌디드 수업 준비(Ready)	⇔	교육 대상자 선정 초등학생 3학년~6학년 대상 교육
하이브리드 블렌디드 수업 설계(Set)	⇔	2015 개정 교육과정 교과 및 성취기준 탐색 초등학교 5-6학년 군 미술**[6미01-04]** 이미지를 활용하여 자신의 느낌과 생각을 전달할 수 있다. 초등학교 5-6학년 군실과 **[6실 05-06]** 생활 속에서 로봇 활용 사례를 통해 작동 원리와 활용 분야를 이해한다. 초등학교 5-6학년 군 사회 **[4사04-03]** 자원의 희소성으로 경제활동에서 선택의 문제가 발생함을 파악하고, 시장을 중심으로 이루어지는 생산, 소비 등 경제활동을 설명한다. ↓ 창의적 교수학습법 모색 리치픽처, KEEP-STOP-BEGIN 기법 선정 ↓ 학습 목표 정립 · 정보처리 활용 능력 향상 · 인공지능 활용 CCTV 알고리즘 이해 · 안면인식 기술 원리 인식 제고
하이브리드 블렌디드 수업 실행(Go)	⇔	교육 프로그램 실행 · 1차시: 안면인식 기술 원리 및 개념 이해 · 2차시: 인공지능의 판단 과정 인식 · 3차시: 안면인식 기술 체험 ↓ 학습자료 제공 교수학습자료, 지도상의 유의점
하이브리드 블렌디드 수업 평가(Review)	⇔	수업 평가 교수학습 평가 및 피드백 제공

(3) 지도상 유의 사항

본 안면인식 핵심원리 교육 프로그램을 학생들에게 적용할 때 고려할 다음과 같은 세 가지의 유의 사항을 제시한다.

첫째, 지능형 CCTV나 모바일 보안의 전문적 원리와 안면인식 기술, 인공지능 기술을 초등학생 학습자가 모두 이해하는 것은 현실적으로 어렵다. 본 교육에서는 학생들이 전문적 기술 시스템을 이해하는 것이 아닌 기술적 원리를 단순화한 활동을 통하여 학습자에게 인공지능 활용, 안면인식 기술, 정보보안의 핵심원리를 이해하고 흥미를 유발하는 것을 중점으로 한다.

둘째, 본 교육 프로그램은 안면인식의 원리 이해를 바탕으로 정보보안에 다양한 위협이 될 수 있는 요소를 파악하여 학습자가 주도적으로 학습 내용을 이해하고 나아가 실생활에 적용할 수 있도록 한다. 안면인식 기술의 발전은 인간의 한계가 보완되고 안전하고 편리한 생활을 실현시켜줄 것이라 기대되고 있지만, 이에 따른 다양한 문제 또한 존재한다[73]. 학생들의 논의를 돕고 창의적 문제 해결 방안 도출을 위해서 실생활에서 정보보안을 실천할 수 있는 방안에 대해 토론의 주제를 유지, 삭제 또는 새롭게 시작하는 세 가지 측면으로 문제를 바라보는 KEEP-STOP-BEGIN을 적용한다[78].

또한, 전체 상황의 복잡성을 이해하여 개선을 만들고 개입을 시도할 때 고려해야 하는 주요 요소와 관계를 그림으로 설명할 수 있는 리치픽처 기법을 도입하여 안면인식 기술의 장단점, 개선 사항, 정보보안 시스템 관련 위협 요소를 토론하고 이러한 첨단기술의 바람직한 발전 방향을 식별하고 고안하는 데 도움을 줄 수 있도록 한다. 리치픽처 기법 도입을 위해서는 큰 플립 차트나 보드지를 준비해야 하며, 3~4명 이상의 팀으로 자리를 구성해야 한다. 또한, 모둠원 각자가 그림을 쉽게 그릴 수 있도록 모든 사람이 닿을 수 있는 거리에 종이를 놓아야 한다. 교수자는 팀 모두가 리치픽처 완성에 이바지할 수 있도록 격려하고 드로잉 기술이 중요하지 않다는 점을 주지시킨다. 가능하면 다양한 색상의 마커나 드로잉 도구를 준비해주는 것이 좋다.

안면인식 기술 시스템은 현재 빠른 속도로 발전하고 있는 유망기술이다. 그러

나 학습자의 입장에서는 다소 낯선 개념일 수 있고, 학습자 본인과 크게 연관 없는 기술로 인식하여 학습의 필요성을 이해하지 못할 수 있다. 이를 극복하기 위해 주변에서 쉽게 볼 수 있는 기술의 사례를 제시하면 주제의 중요성을 제고할 수 있다.

(4) 교육 프로그램 구성 방안

제안된 교육 프로그램은 '안면인식 기술 원리 및 개념 이해', '인공지능의 판단 과정 인식', '안면인식 기술 체험'의 총 3차시로 구성하였다.

먼저, 1차시에서는 '안면인식 기술 원리 및 개념 이해' 단계로 안면인식이 작동하는 원리, 안면인식 활용 사례, 포렌식 사이언스에서 활용되는 안면인식 기술 등에 대해 교수한다. 안면인식의 작동 원리는 4단계로 나누어지며, 1단계에서는 사진이나 동영상에서 얼굴을 캡처하며, 2단계에서는 안면인식 소프트웨어가 얼굴의 기하학을 읽는다. 안면인식 소프트웨어가 인식하기 위해서는 중요한 얼굴의 주요 랜드마크를 식별하는데, 이에 포함되는 요소로는 눈과 눈 사이의 거리, 이마에서 턱까지의 거리 등이 있다. 3단계는 인식을 할 특정 사람의 얼굴 서명(Facial Signature)을 소프트웨어에 입력된 안면 데이터베이스와 비교하는 것이다. 4단계에서는 마침내 안면 프린트(Faceprint)와 프린트가 일치하는 데이터베이스를 찾아 결정을 내리는 것으로 마무리하는 것이다. 이러한 작동 원리는 3차시 '안면인식 기술 체험'에서 단순화한 활동을 통해 직접 체험함으로써 학습 주제의 인식 제고에 도움을 줄 수 있다. 이에 더하여, 안면인식 기술 활용 사례로는 공항의 CCTV 모니터링, 휴대전화 제조업체의 Face ID, 학생 출결 관리 시스템, 소셜 미디어 사(社)의 사진 업로드 알고리즘, 직원 출입 시스템 등을 들 수 있다. 학습자와 연관된 사례일수록 학습자들은 안면인식 기술이 얼마나 중요한지, 활용도가 얼마나 높은지, 특히, 미래에 얼마나 유망한 기술일지를 인지할 수 있다.

한편, 포렌식 사이언스에서 활용되는 안면인식 기술로는 CCTV, 교통 카메라, 소셜 미디어 혹은 경찰관이 직접 찍은 사진 등 다양한 출처의 사진에서 특정 사람을 식별하기 위한 머그샷 데이터베이스 조사가 있다. 또한, 콘서트, 스포츠 행

사 등의 대규모 행사에서 얼굴 인식을 사용해 범죄 관련 수배 가능성이 있는 사람을 식별하기 위해서도 사용된다. 실제로 FBI의 차세대 식별 시스템에서는 3천만 개 이상의 얼굴 데이터베이스를 포함하고 있다고 알려져 있다[77].

2차시에서는 '인공지능의 판단 과정 인식'을 이해하는 것이 학습의 세부 목표이다. 본 차시에서는 리치픽처 기법을 기반으로 지능형 CCTV가 얼굴을 인식하는 과정을 이해한다. 플로우차트에서 사용되는 단말, 처리, 입출력, 흐름선 등의 기호를 사용하여 안면인식 과정을 도식화하였다. 또한, 이러한 인식 과정 학습 후, KEEP-STOP-BEGIN 학습법을 통해 학습자가 이러한 안면인식 기술의 장점과 단점, 개선 사항을 모색할 수 있도록 유도한다. 학습자들은 이러한 활동을 통해 정보보안 관련 첨단기술을 이해하고 나아가 관련 문제를 인식하고 해결하며 학습한 내용을 본인의 것으로 전환할 수 있는 기회를 제공받는다.

3차시에서는 '안면인식 기술 체험'을 주제로 1차시에서 학습한 안면인식 시스템의 작동 원리를 체험해본다. 본 단계에서는 다각형의 합동 성질을 이용한 안면인식 기술의 원리를 간접적으로 체험해보는 활동을 한다. 학생들의 얼굴을 직접 촬영하여 얼굴의 특징점을 OHP 필름에 찍고 이를 연결하여 자기 얼굴에 있는 다각형을 찾아보는 활동을 하며 친구들과 비교하여 사람마다 다르게 인식되는 다각형들에 대해 이해하고 안면인식 기술이 실제로 어떻게 작동하는지 학습할 수 있다. [표 Ⅳ-4]는 본 논문의 안면인식 핵심원리 교육 프로그램의 지도안을 나타낸다[78].

[표 Ⅳ-4] 안면인식 핵심원리 교육 프로그램 지도안

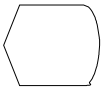
주제	안면인식 핵심원리 교육	
학습 목표	안면인식 기술 원리를 이해할 수 있다.	
차시	교수학습 활동	
1차시	도입	안면인식 기술 원리 사례 영상 시청
	안면인식 기술 원리 및 개념 이해	- 안면인식 작동 원리 - 안면인식 활용 사례 - 포렌식 사이언스에서 활용되는 안면인식 기술
2차시	인공지능의 판단 과정 인식	- 순서도, 리치픽처 기법 기반 지능형 CCTV 안면인식 과정 이해 - KEEP-STOP-BEGIN 학습법 적용 안면인식 기술의 장단점, 개선 사항 모색
3차시	안면인식 기술 체험	- OHP 필름으로 학급 동료의 얼굴을 촬영하여 사람마다 다른 얼굴의 비와 특징점 이해

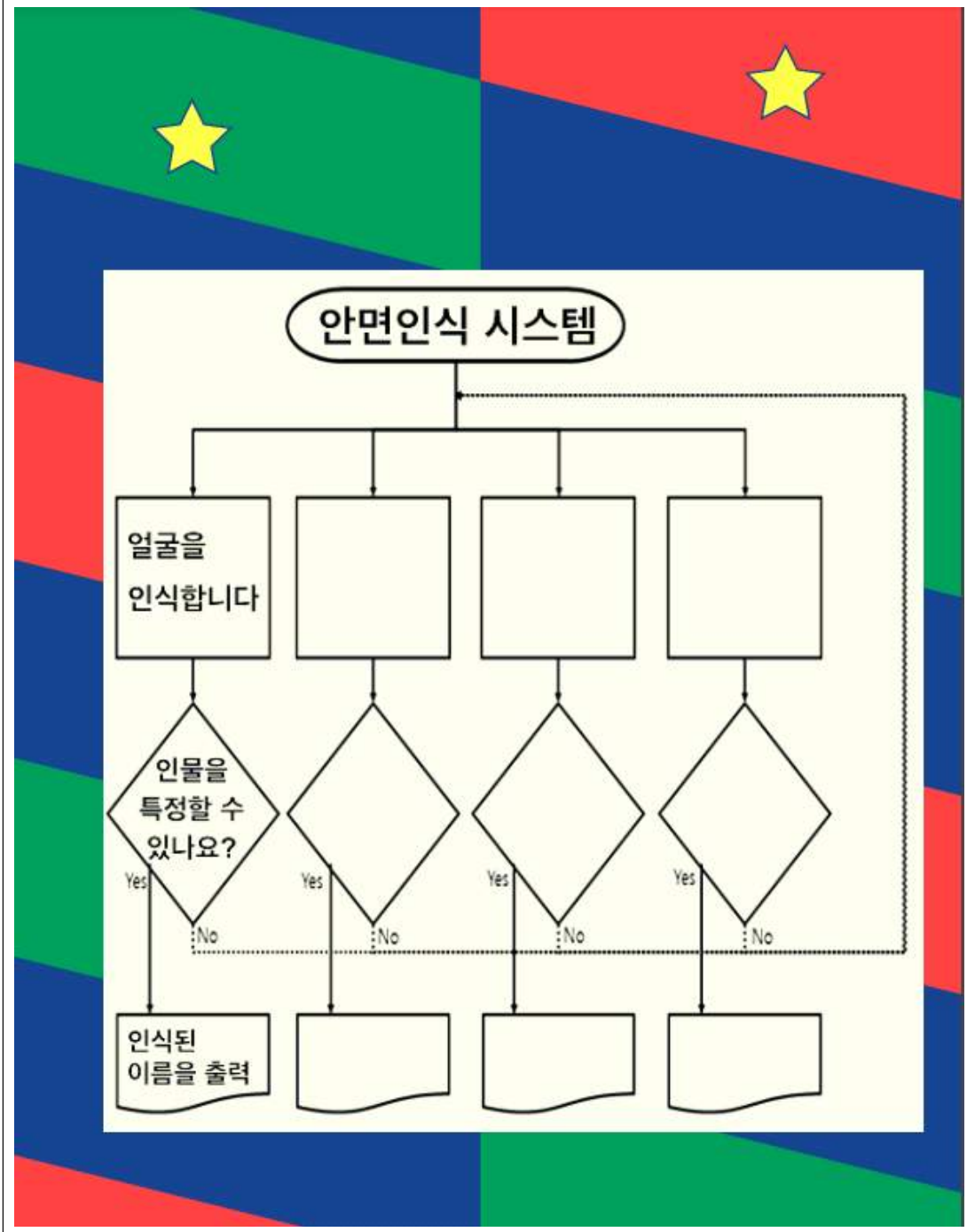
(5) 교육 자료

총 3차시로 구성된 안면인식 기술 원리교육 프로그램에서는 학생들에게 비교적 낯선 첨단기술 교육을 위해 다양한 교수학습자료를 제공하여 학생들의 이해도를 높일 수 있도록 노력한다.

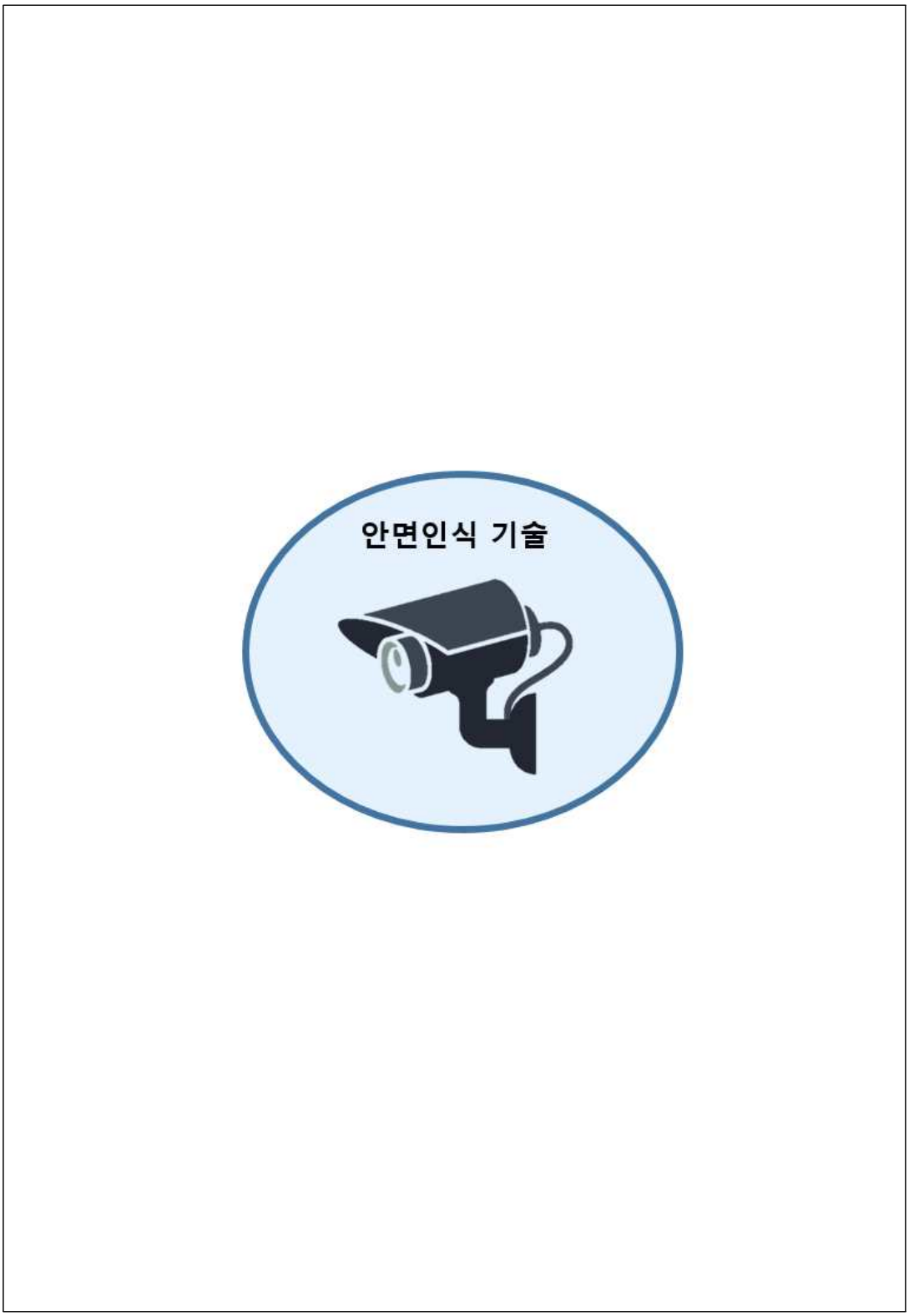
먼저, 2차시에서는 [표 Ⅳ-5]와 같은 순서도 기호를 활용하여 [그림 Ⅳ-3]과 같은 순서도 기반 지능형 CCTV 안면인식 원리 워크시트를 제작하였다. [그림 Ⅳ-4]는 리치픽처를 기반하여 학습자들이 안면인식 기술 원리에 대하여 자신의 의견을 다양하게 펼칠 수 있도록 구상한 학습지이다. 또한, [그림 Ⅳ-5]는 KEEP-STOP-BEGIN 학습법을 이용한 안면인식 기술 논의 워크시트이다. 이러한 다양한 학습지를 통하여 학생들의 창의성 증진과 본인의 생각을 구체적으로 표현할 수 있는 힘을 기를 수 있다.

[표 Ⅳ-5] 안면인식 핵심원리 워크시트 제작에 활용된 순서도 기호

기호	설 명		기호	설 명	
	단말	순서도의 시작과 끝		카드입력	카드리더(card reader)를 통한 입력
	흐름선	작업 흐름을 명시		수동입력	키보드를 통한 입력
	준비	작업 단계 시작 전 준비 (변수 및 초기치 선언 등)		서브루틴	정의하여 둔 부프로그램의 호출
	처리	처리해야 할 작업을 명시 (변수에 계산 값 입력 등)		페이지 내 연결자	한 페이지 내의 순서도 연결
	입출력	일반적인 제이터의 입력 또는 결과의 출력		페이지 간 연결자	페이지가 다른 순서도의 연결
	판단	조건에 따라 흐름선을 선택 (일반적으로 참, 거짓 구분)		화면표시	처리결과 또는 메시지를 모니터를 이용하여 출력
	프린트	프린터를 이용한 출력 (서류 등의 지면에 출력)		결합	기본 흐름선에 다른 흐름선 합류



[그림 IV-3] 순서도 기반 지능형 CCTV 안면인식 핵심원리 워크시트



[그림 IV-4] 리치픽처 기반 지능형 CCTV 안면인식 핵심원리 워크시트

[그림 IV-5] KEEP-STOP-BEGIN 안면인식 기술 논의 워크시트

3차시에서 활용되는 안면인식 기술 체험 워크시트는 [그림 Ⅳ-6], [그림 Ⅳ-7]과 같다. [그림 Ⅳ-6]은 활동을 위한 준비물과 얼굴 촬영 시 유의점을 공지하는데 사용하며, [그림 Ⅳ-7]은 OHP 필름에 인쇄하여 학습자의 얼굴에 대고 서로 얼굴의 주요점이 다름과 안면인식 기술이 얼굴을 인식하는 원리를 체험한다.

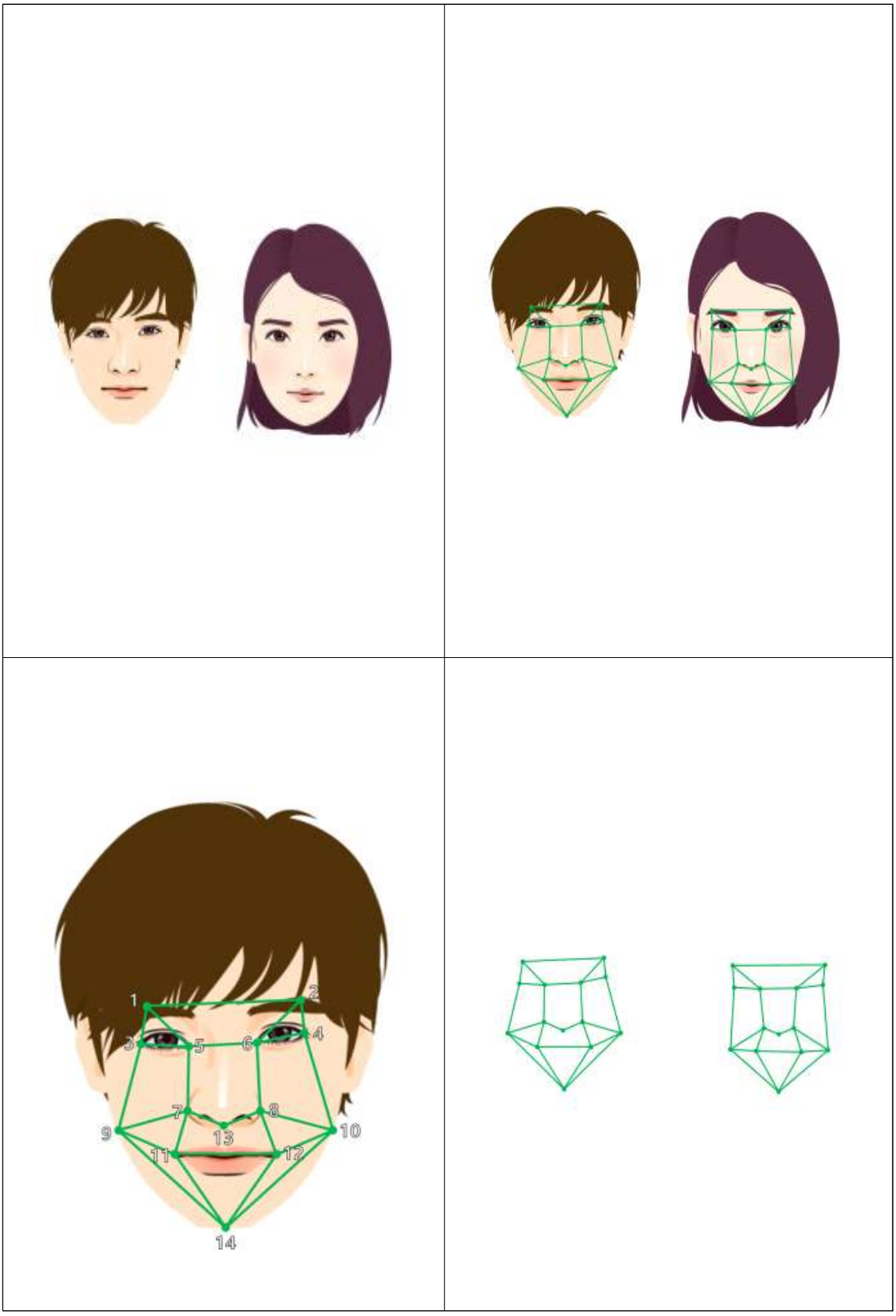
1. 준비물

			
높이 조절이 가능한 삼각 거치대	OHP 필름	네임펜	자

2. 얼굴 촬영 시 유의점

가. 학생들이 촬영할 위치를 명확히 표시한다.
나. 카메라는 학생들의 키에 따라 높이 조절만 하고 촬영하는 거리는 변하지 않도록 고정한 상태를 유지한다.
다. 촬영하는 학생들은 허리를 곧게 펴고 벽에 뒤통수가 닿게 한 상태로 정면을 촬영한다.
라. 촬영 중 눈이 감긴 경우 재촬영을 한다.
마. 얼굴의 긴장을 풀고 무표정인 상태로 촬영한다.
바. 사진을 인쇄할 때는 모든 사진의 전체 크기가 동일하게 편집한다.

[그림 Ⅳ-6] 안면인식 기술 원리 체험 활동 준비 자료



[그림 Ⅳ-7] 안면인식 핵심원리 체험 활동지

4.2.3. 연구 대상자 현장 교원 선정

본 논문에서 제시하는 안면인식 핵심원리 교육을 실증하고 교육의 효과를 확인하기 위하여 현장 교원을 대상으로 교육 프로그램을 시범적으로 적용하였다. 현장 교원은 학생들을 일선에서 가장 가까이 만나는 역할을 수행하며 학생들의 정보보안 인식을 향상하기 위한 교육을 직접적으로 행하는 인물이다[80][81]. 특히, 최근 안면인식 기술을 통해 학생들의 출결 상황을 파악하고 지도에 활용하는 기술이 교육계에 도입되고 있다[40]. 현장에서 직접 교육을 수행하는 교사들은 학생 지도라는 본연의 업무에서도 안면인식 기술에 대한 이해가 수반되어야 한다. 더불어, 본 교육 프로그램이 초등학생을 대상으로 한 교육 프로그램이기 때문에 교사가 선제적으로 교육내용에 대한 숙지가 필요하다. 이를 위하여 본 교육 프로그램은 현장 교원을 대상으로 시범 적용되었다.

본 교육 프로그램을 적용하기 위해 전국의 초등 교원 46명을 교육 대상자로 선정하였고 현장 교원은 일반 교원과 교사연구회에 포함되는 현장 교원으로 구성되었다. 제주에서 가장 많은 17명이 참석하였으며, 그밖에 서울 12명, 울산 3명 등 전국 현장 교원이 참석하였다. [표 Ⅳ-6]은 안면인식 기술 원리교육에 참여한 연구 대상자의 현황이다.

[표 Ⅳ-6] 안면인식 핵심원리 교육 프로그램 연구 대상자

분류		인원(비율(%))	총계(%)
학교급	초등학교	46(100)	46 (100)
	중학교	0(0)	
	고등학교	0(0)	
	기타	0(0)	
소속	일반 교원	42(91)	46 (100)
	교사연구회	4(9)	

지역	강원	0(0)	46 (100)
	경기	2(5)	
	경남	7(16)	
	경북	4(9)	
	광주	0(0)	
	대구	0(0)	
	대전	0(0)	
	부산	0(0)	
	서울	12(26)	
	세종	0(0)	
	울산	3(6)	
	인천	0(0)	
	전남	1(2)	
	전북	0(0)	
	제주	17(36)	
	충남	0(0)	
	충북	0(0)	

4.2.4. 안면인식 핵심원리 교육 프로그램 적용

본 교육 프로그램은 2020년 9월 17일과 9월 24일 이틀에 걸쳐 2회로 나누어 적용되었다. 1회차에 참가한 교원은 33명이며, 2회차에 참가한 교원은 13명으로

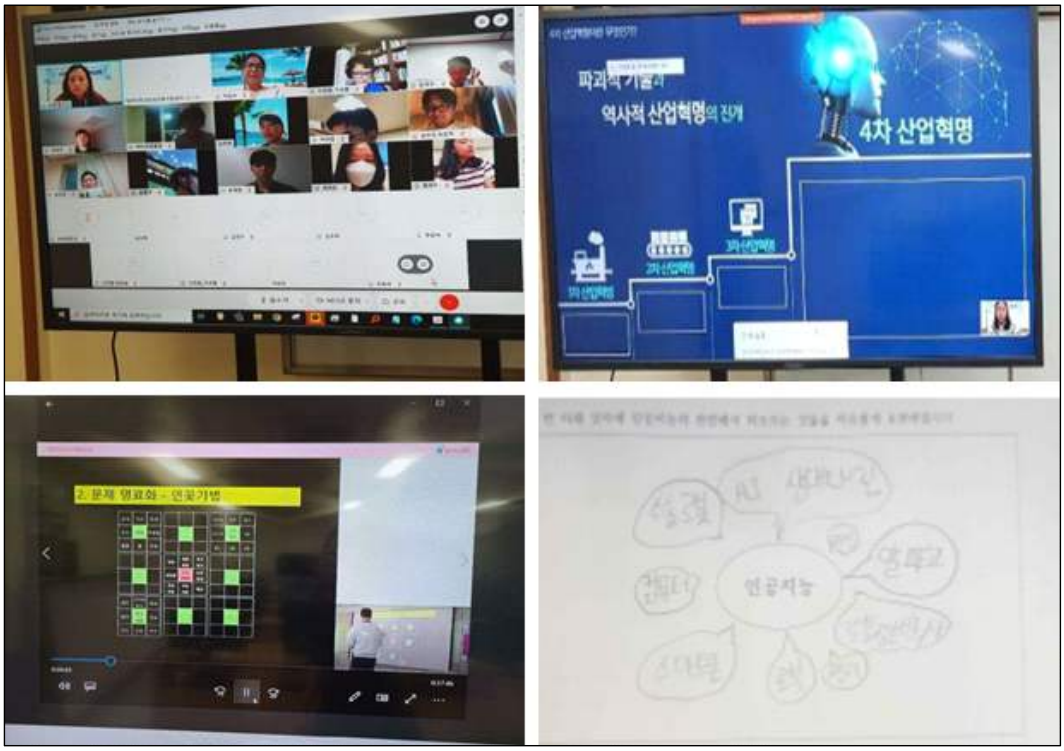
총 46명이다. 해당 교육은 COVID-19의 영향으로 온·오프라인 병행 하이브리드 방식을 통해 수행되었다. 2회로 나누어 적용하였으나 적용된 교육 프로그램 내용은 같다.

교육 프로그램의 내용에 따라 3차시로 시범 수업을 구성하였으며, 1차시에서는 안면인식 기술 원리와 개념을 학습하였으며, 2차시에서는 리치픽처, 순서도, KEEP-STOP-BEGIN 등 다양한 방식을 통해 창의적으로 인공지능의 판단 과정을 이해해보고 안면인식 기술의 장단점과 개선 방안 등에 관한 논의를 시행했다. 2차시는 온라인 화이트보드와 같은 상호작용 소통 도구를 통하여 온라인으로 참석한 교원들도 어려움 없이 활동에 참여할 수 있도록 설계했다. 3차시의 활동은 모둠별로 실제 얼굴의 특징점을 연결하여 안면인식 기술을 체험해보는 활동으로 온라인으로 참여한 교원들은 오프라인으로 참석한 교원들의 활동 모습을 지켜보며 실제 수업에서 어떻게 수업할 수 있는지를 인식하였다. [표 Ⅳ-7]은 현장 교원 대상 시범 적용을 위한 교육 프로그램의 일정표이다.

[표 Ⅳ-7] 현장 교원 대상 안면인식 핵심원리 교육 프로그램 세부 일정

시간	내용	장소
17:50~18:00(10′)	입장 및 환영사	제주대학교 및 온라인 (ZOOM)
18:00~19:00(60′)	**[1차시]** 안면인식 핵심원리 및 개념 이해	
19:00~19:10(10′)	휴식	
19:20~20:00(60′)	**[2차시]** 인공지능의 판단 과정 인식	
20:00~20:10(10′)	휴식	
20:10~21:10(60′)	**[3차시]** 안면인식 기술 체험	
21:10~22:20(10′)	정리	

[그림 Ⅳ-8]은 안면인식 기술 원리교육 시범 적용에 참여한 현장 교원들의 모습과 리치픽처 기법을 활용한 워크시트를 사용한 모습이다.



[그림 Ⅳ-8] 안면인식 핵심원리 교육 프로그램 적용

4.2.5. 안면인식 핵심원리 교육 프로그램 인식조사 결과분석

안면인식 기술 원리교육 프로그램에 대한 효과를 측정하기 위하여 교육을 시작하기 전에 사전 설문 조사를 안내 및 실시하였고 교육을 마치고 난 후에 사후 설문 조사를 시행하였다. 또한 설문 작성에 충분한 시간을 제공함으로써 설문지를 작성하는 데 어려움이 없도록 하였다. 본 논문의 교육 프로그램의 효과성 분석을 위해서 IBM SPSS 24.0 Program이 활용되었으며 분석 기법으로는 기술통계와 대응 표본 t-test를 사용하였다. 조사 도구인 설문지는 [표 Ⅳ-8]과 같다. 설문지는 교육 프로그램에 참여한 연구 대상자의 교육 프로그램에 대한 인식에 대하여 알아보기 위하여 작성되었다. 문항은 총 7개의 문항으로 구성되었으며 모두

5점 척도를 이용한 선다형으로 구성했다. 설문지 문항의 신뢰도 분석을 시행한 결과 신뢰도 계수(Cronhach's alpha) 0.87로 나타나 높은 수치의 내적 일관성을 확보한 것으로 나타났다.

[표 Ⅳ-8] 안면인식 핵심 원리교육 프로그램 인식조사 분석 도구

연번	문항	형태
1	현장 교원 대상 안면인식 기술 원리교육 프로그램 교육이 필요하다고 생각하시나요?	Likert 5점 척도
2	학교에서 초등학생을 대상으로 안면인식 기술 원리교육을 해야 한다고 생각하시나요?	Likert 5점 척도
3	정보보안 교육 범주 안에서 현장 교원의 역할에 대해 인식하고 계시는지요?	Likert 5점 척도
4	안면인식 기술 원리와 개념에 대해 이해하고 계시는지요?	Likert 5점 척도
5	인공지능의 판단 과정을 인식하고 계시는지요?	Likert 5점 척도
6	안면인식 기술 시스템이 사람의 얼굴을 식별하는 단계를 알고 계시는지요?	Likert 5점 척도
7	안면인식 기술을 적용한 사례와 향후 미래 사회에 끼칠 영향에 대해 인식하고 계시는지요?	Likert 5점 척도

[표 Ⅳ-8]의 교육 프로그램 인식조사 분석을 시행한 결과, 교원 대상 안면인식 기술 원리교육의 필요성에 대해 대부분의 현장 교원이 교육 프로그램 적용 이전에도 이미 인식하고 있었으며, 교육 프로그램 적용 후에도 여전히 지속적인 교육이 필요하다고 강조했다. 결과의 평균값이 에서 4.92에서 5.00으로 변화하여, 교육 프로그램 적용 후 모든 교원이 이에 동의하는 것으로 나타났다. 그러나, 유의

수준이 0.05 보다 크게 나타나 유의하지 않은 것으로 나타났다. 이는 이미 정보보안 관련 교육 프로그램의 필요성에 대해 높게 인지하고 있었기 때문으로 보인다.

둘째로 학교 현장에서 초등학생 대상의 안면인식 기술 원리교육의 필요성에 대해서도 사전 결과 평균에서 사후 결과 평균 4.92로 동일하게 나타났으며 유의확률이 1.000으로 유의미한 상관이라고 볼 수 없다. 문항 1과 동일하게 현장에서 안면인식 기술 원리교육의 필요성을 크게 인지하고 있어 교육이 끝난 이후에도 변화 없이 같은 결과를 얻은 것으로 해석할 수 있다.

셋째로 정보보안 교육의 범주 안에서 교원의 역할에 대한 인식은 연수 전 4.54에서 4.77로 증가하였으나, 이 또한 유의미한 결과로 집계되지 않았다. 정보보안과 관련하여 현장 교원들은 본인의 역할에 대해 높은 비율로 이미 인식하고 있었던 것으로 나타났다.

넷째로 안면인식 기술의 원리와 개념 이해에 관한 문항에서는 사전 결과 평균 3.54에서 4.85로 극적인 적용 효과를 나타냈으며, 안면인식 기술의 필요성 인식에 비해 상세한 개념과 원리를 인지하지 못했던 교원들은 본 교육 프로그램을 통해 기술적인 측면에서 안면인식 기술에 관해 이해도가 제고되었음을 확인할 수 있었다. ($p<.001$).

다섯째로 인공지능의 판단 과정에 관한 이해도가 3.00에서 4.77로 변화하였으며 본 교육 프로그램이 미래 유망기술 중 하나인 인공지능 관련 인식을 높일 수 있는 교육이었으며, 유의확률이 $p<.001$로 나타나 통계적으로도 유의한 교육이었음이 증명되었다고 볼 수 있다.

여섯째로 안면인식 기술이 사람의 얼굴을 식별하는 단계에 대한 인지도는 3.23에서 4, 69로 매우 높은 비율로 증가하여 유의확률 또한 $p<.001$로 안면인식 기술에 대한 기술적 이해도 증진에 유의미하게 작용하였음을 알 수 있다.

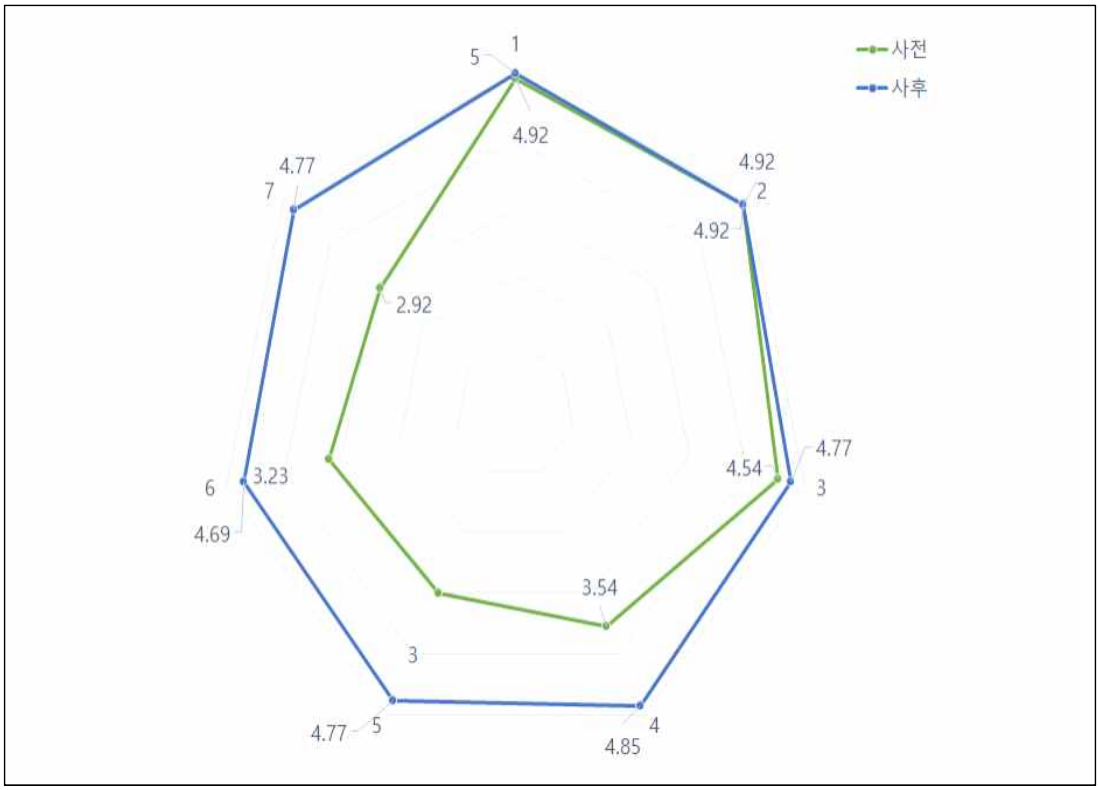
마지막으로, 안면인식을 적용한 사례와 향후 미래 사회에 끼칠 영향에 관한 문항에서는 사전 인식이 2.92로 가장 낮게 기록되었으나 사후 4.77로 매우 높은 비율로 증대되었으며, 통계적으로 유의한 교육이었음을 알 수 있다. 교사들은 비교적 정보보안 분야의 일종인 안면인식 기술 관련 교육이 현장에 필요하다는 점을 인식하고 있었지만, 안면인식 기술에 대한 구체적이고 기술적인 측면에 관해서는 인지하지 못했던 경우가 대다수였다. 본 교육 프로그램이 교원들의 요구(Needs)

를 충족시켜주었으며, 나아가 안면인식과 관련한 정보 제공에 유의한 교육으로 자리했음을 알 수 있다. [표 Ⅳ-9]에서 교육 프로그램에 대한 현장 교원의 인식 조사 결과를 확인할 수 있으며, [그림 Ⅳ-9]는 [표 Ⅳ-9]를 방사형 차트로 도식화 한 결과를 보여준다.

[표 Ⅳ-9] 안면인식 핵심원리 교육 프로그램 인식조사 결과

연번	분류	평균(표준편차)	*t*	*p*
1	pre	4.92(.277)	-1.000	.337
	post	5.00(.000)		
2	pre	4.92(.277)	.000	1.000
	post	4.92(.277)		
3	pre	4.54(.660)	-.898	.387
	post	4.77(.599)		
4	pre	3.54(.877)	-5.516	.000***
	post	4.85(.376)		
5	pre	3.00(1.354)	-5.472	.000***
	post	4.77(.599)		
6	pre	3.23(1.013)	-6.008	.000***
	post	4.69(.630)		
7	pre	2.92(1.256)	-5.821	.000***
	post	4.77(.599)		

*p<.05, **p<.01, ***p<.001



[그림 IV-9] 안면인식 핵심원리 교육 프로그램 인식조사 결과 도식화

결과적으로, 안면인식 기술 원리교육 프로그램 관련 교사의 인식은 대체로 유의미한 결과를 나타냈다고 볼 수 있었다. 특히, 안면인식 기술 원리와 개념 이해, 인공지능의 판단 과정, 안면인식 기술 적용과 미래 사회에 미칠 영향에 대해 구체적으로 인식하는데 본 교육 프로그램이 통계적으로 유의미한 영향을 미쳤음을 확인할 수 있다. 본 교육 프로그램은 이러한 교원 인식조사 결과를 토대로 더욱 다양한 기술적 지식과 흥미로운 방식의 수업 설계로 향후 교육 프로그램을 고도화할 예정이다. 안면인식 핵심원리 교육과 나아가 정보보안 교육 수행에 구체적인 방안을 제시하였다는데 본 교육의 의의가 있다.

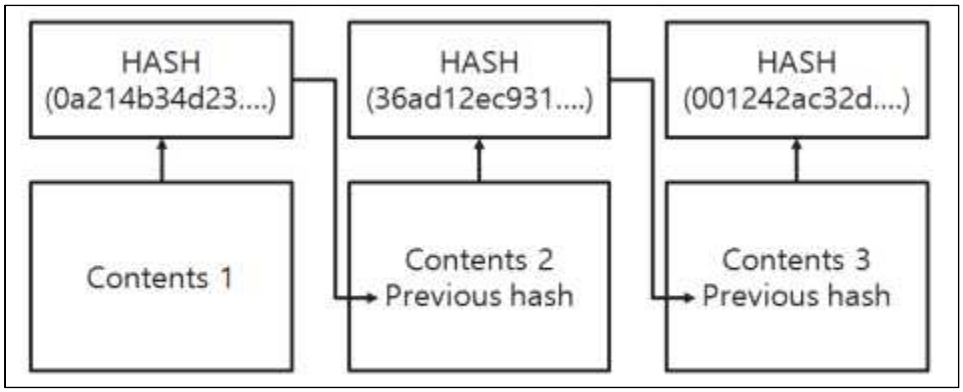
4.3. 블록체인 핵심원리 교육 프로그램

블록체인(Blockchain) 기술은 이 세대의 가장 파괴적이고 유망한 기술 중 하나로 파장을 일으키고 있다. 대부분 사람은 이를 비즈니스 운영 방식에 혁명을 일으키고 수십억 달러 가치의 산업을 창출한 닷컴 시대의 여명에 비유하기도 한다. 특히, 정보보안과 관련하여 혁명적 방식으로 기존의 정보보안 분야에 파란을 일으켜 블록체인을 이해하는 것이 정보보안 교육에서도 매우 중요하게 인식된다. 업계 전문가들은 블록체인의 영향이 인터넷이 우리에게 미친 영향만큼 중요할 수 있다고 확신한다. 따라서, 현장 학교에서도 블록체인 교육이 시행되어야 하며 구체적으로 이를 도입하는 방안을 검토해야 할 시점이 도래했다[82]. 본 교육 프로그램에서 제안하는 초등 정보보안 교육 프로그램 중 두 번째로 게이미피케이션을 적용한 블록체인 핵심원리 교육 프로그램을 제안한다[83][84].

4.3.1. 교육 프로그램에 적용한 블록체인 핵심 기술

블록체인은 기록되는 데이터의 위변조를 방지하고, 무결성을 강화한다는 점에서 많은 화제가 되고 있으며, 상용화를 위한 다양한 연구가 진행되고 있다. 블록체인은 하나의 클라이언트에서 모든 작업을 수행하는 방식과 달리, 네트워크상에 연결된 모든 클라이언트 장치의 컴퓨팅 파워를 이용하기 위한 분산형 네트워크 구조로 구성된 원장 관리 기술을 의미한다. 블록체인은 다수의 클라이언트가 같은 원장을 가지며, 기록되는 데이터를 블록이라는 단위로 관리하여 블록 간의 연결을 해시(Hash)값이라는 것을 이용하여 수행한다. 해시값이란, 문자열의 연산 결과로 복원이 불가능한 완전히 다른 고정된 숫자열로 변환하여 생성된 값을 의미한다. 따라서 특정 블록의 내용이 변경되는 경우, 뒤이어 생성된 블록의 주소로 사용된 해시값과 달라지며, 뒤에 이어지는 모든 블록에 대해 해시 연산을 다시 수행하여야만 내용을 위변조할 수 있다.

하지만 블록체인의 경우, 다음 블록의 생성까지의 소요 시간이 10분이 되도록 설정하며, 10분 간격으로 다음 블록이 되기 위한 암호화 값을 찾는 과정을 수행되도록 한다. [그림 Ⅳ-10]은 상기 기술한 블록체인의 해시 원리를 나타낸다.



[그림 IV-10] 블록체인 해시 원리

이때, 새로운 블록이 추가되는 경우, 암호화 값을 찾는 클라이언트로부터 모든 네트워크상에 이를 알리며, 블록 네트워크상의 반수 이상이 동의하는 경우 새로운 블록으로 추가된다. 이 과정에서 블록에 위변조된 경우가 발생할 수 있다. 이 경우에는 위변조된 블록과 같은 단의 블록들을 비교하여 가장 많은 블록을 정상적인 값으로 인식하여 모든 블록을 다수의 블록의 내용으로 변경한다. 따라서 이때, 블록 네트워크상에 속하는 반절 이상의 블록에 대해 위변조를 수행하는 경우, 블록의 내용을 바꿀 수 있다는 것이 된다. 하지만 시간제한과 함께 블록체인의 위변조를 방지하는 원리는 네트워크에 참여하는 사용자의 수에 있다. 네트워크에 참여하는 사용자의 수가 늘어날수록 위변조가 요구되는 블록이 많아지며, 이 수가 비트코인과 같이 많을 경우, 현재의 컴퓨팅 파워로는 위변조가 불가능해진다.

본 교육 프로그램에서는 이와 같은 블록체인의 원리에서 다음과 같은 두 개의 원리를 적용하였다.

- 블록체인은 해시값이라는 것을 이용하여 서로 연결된다.
- 블록체인의 값은 전체 네트워크의 다수가 동의하는 내용으로 변경된다.

먼저, 해시값을 연산하는 과정을 보이기 위해 각각의 알파벳에 숫자를 설정하고, 이에 대한 값의 연산을 수행하도록 하였다. 또한 수행 결과를 팀원과 공유함으로써 서로 다른 값을 가졌는지 확인함으로써 두 번째 내용을 적용하였다.

4.3.2. 블록체인 핵심원리 교육 프로그램 개발

(1) 개발 배경

블록체인 교육의 중요성을 이해하려면 먼저 기술 자체와 블록체인이 무엇을 할 수 있는지 이해하는 것이 중요하다. 데이터의 위조와 변조 방지를 위한 혁신적인 기술로 업계에서 중요 이슈로 떠오른 블록체인은 데이터를 저장할 수 있는 능력을 갖추고 있지만 저장된 데이터를 변경하거나 변경할 수 없는 분산형 원장(ledger)으로 표현된다. 또한 서버가 네트워크를 지원하는 전통적인 접근 방식을 취하지 않고 전 세계에 분산된 컴퓨터에서 네트워크를 지원한다는 점이 특징이다.

블록체인 기술의 영향은 최근 암호화폐로 유명해진 금융 관련 범위를 넘어서 확장된다. 예를 들어, 분산형 원장 기술을 사용하여 기업을 운영하는 데 사용할 수 있는 안전한 자동화 시스템을 만들 수 있다. 예를 들어, 이 기술을 사용하여 고객이 체크인하는 순간부터 체크아웃하는 순간까지 고객 정보를 처리하는 호텔 시스템을 만들 수 있다. 블록체인 사용의 최신 예 중 하나는 개인 EV(Electronic Vehicle) 충전기를 공개적으로 공유할 수 있도록 하는 스마트 계약으로 촉진되는 P2P 전기 자동차 충전을 들 수 있다. 이 개념은 해당 충전기의 소유자가 다른 EV 소유자가 콘센트를 통해 충전할 수 있도록 하여 충전기를 사용하지 않을 때 추가 현금을 얻을 수 있도록 하는 것이다. 이것은 블록체인 기술의 많은 응용 프로그램 중 하나이다. 이처럼, 블록체인은 다양한 방면에서 그 유용성이 제기된다.

블록체인은 먼저, 저장된 내용이 위조되거나 변조될 경우 아예 다른 값으로 변환되는 해시값과 연산된 값을 해당 블록의 다음 블록에 저장하여 연결된 블록 간 체인과 같은 연결을 만든다. 이러한 원리를 이용하여 연결된 블록 중 중간 블록이 변경될 경우, 해당 블록 이후 생성된 다른 모든 블록의 해시값이 계산되어야 한다. 더불어, 각 사용자가 저장한 데이터가 일치하지 않는다면 다수의 사용자가 저장하고 있는 데이터를 옳다고 판단한다. 이를 합의 알고리즘으로 칭한다. 합의 알고리즘을 형성하고 있는 참여자가 가진 데이터가 과반으로 변경되어야만 블록체인의 위조와 변조가 이루어질 수 있다.

(2) 개발 절차

본 논문에서 제안하는 블록체인 핵심원리 교육 프로그램은 하이브리드 블렌디드 실천모형의 수업 설계 개발 절차와 Livingston & Stoll(1973)이 제안한 학습 게임 모델 개발 절차에 따라 학습 게임을 구성하여 교육 프로그램에 주요 교육 내용으로 구성하였다[85][86][87].

먼저, 하이브리드 블렌디드 실천모형의 준비(Ready) 단계에 해당하는 첫 번째 단계에서는 학습 목표를 '블록체인 핵심원리 이해'로 설정하였다.

두 번째 설계(Set) 단계는 Livingston & Stoll(1973)이 제안한 학습모델 개발 절차에서 제안하는 학습 게임 소재 선정, 학습 게임 구조 디자인이 포함된다. 게임의 소재 지정에서는 단어 합과 연산 결과 비교에 쉬우므로 카드를 활용한 게임으로 구상하였다. 더불어, 게임의 구조를 해시값과 알파벳을 연결하여 제시된 영어 단어에 대한 숫자의 합이 같은 단어를 찾는 것으로 해시값을 표현하였으며, 블록체인의 위조 및 변조 방지 이해를 위해 게임에 참여하는 플레이어인 학습자 모두는 연산한 내용을 모두 공유하고 다른 내용이 공유된다면 반수 이상의 학습자가 연산한 합계로 수정하여 블록체인의 합의 알고리즘 원리를 이해할 수 있도록 설계하였다.

세 번째 단계인 실행(Go) 단계에서는 게임 규칙 제공과 교육 프로그램 자료 개발이 포함된다. 게임의 규칙은 아래와 같이 7단계로 나눠진다.

1. 먼저 4명이 1개의 팀을 이뤄 게임이 진행되며 블록체인 핵심원리 학습자인 플레이어는 순서대로 2개의 단어를 선택하여 단어의 합을 연산해야 하며, 선택한 2개 단어의 합을 계산하여 워크시트에 계산값을 기재한다.

2. 카드에는 모두 다른 영어 단어가 적혀 있고 주의할 점은 사전에 알파벳과 연계된 숫자의 합이 같지만 다른 영어가 적힌 카드 쌍 10개 이상을 사용해

야 한다는 점이다. 카드에 적힌 영어 단어의 합과 같은 카드는 한 쌍만이 존재한다.

3. 플레이어는 자신이 가지고 있는 알파벳 단어의 합을 모든 플레이어에게 공개한다. 이때 같은 단어에 서로 다른 값이 나타난 경우 다수의 학습자가 공통으로 가지고 있는 값을 옳다고 정의한다.

4. 선택한 두 단어에 대해 모든 플레이어가 같은 합을 가지는 것으로 동의하면 카드를 선택한 학습자는 카드를 나눠 갖고 다시 2개의 단어 카드를 선택한다.

5. 1~4번의 과정을 반복하여 제시된 모든 카드를 플레이어 모두가 동의하고 맞춰질 때까지 진행한다.

6. 카드 쌍마다 1점의 점수를 부여한다.

7. 가장 높은 점수를 가진 플레이어가 최종적으로 승리한다.

또한, 본 단계에서는 카드 게임에 필요한 여러 자료와 교육 프로그램에 필요한 자료를 디자인하였다. 여기에는 블록체인 핵심원리 이해 게임의 세부적인 진행 방법 명시 자료나 숫자와 알파벳이 적힌 카드, 단어 합 연산에 필요한 워크시트 등이 포함된다.

마지막 평가(Review) 단계에서는 제작한 학습 게임을 교육 프로그램에 접목하여 시뮬레이션해보고 이 과정에서 발견한 문제점에 관하여 교육 전문가와 기술 전문가의 의견을 수렴하여 학습 게임을 수정하고 보완하였다.

[표 Ⅳ-10]은 블록체인 핵심원리 학습 게임에 초점을 맞춘 교육 프로그램의 개발 절차를 보여준다.

[표 Ⅳ-10] 블록체인 핵심원리 학습 게임 개발 절차

하이브리드 블렌디드 수업 준비(Ready)	⇔	학습 목표 설정 블록체인 핵심원리 이해를 통한 창의적 융복합 정보보안 인재 양성
하이브리드 블렌디드 수업 설계(Set)	⇔	학습 게임 소재 선정 카드 게임을 소재로 한 학습 게임과 블록체인 교육 접목 ↓ 학습 게임 구조 디자인 영어 단어 카드와 숫자를 결합하여 연산하는 방식으로 블록체인의 위조 및 변조 방지원리를 이해하며 합의 알고리즘을 이해
하이브리드 블렌디드 수업 실행(Go)	⇔	게임 규칙 제공 게임 규칙을 7단계로 나누어 자세히 기재 ↓ 교육 프로그램 자료 개발 카드, 워크시트 등 교육 자료 개발
하이브리드 블렌디드 수업 평가(Review)	⇔	검사 및 수정 학습 게임을 중점으로 한 교육 프로그램 운영 및 수정

(3) 교육 프로그램의 체제적 수업 모형 디자인

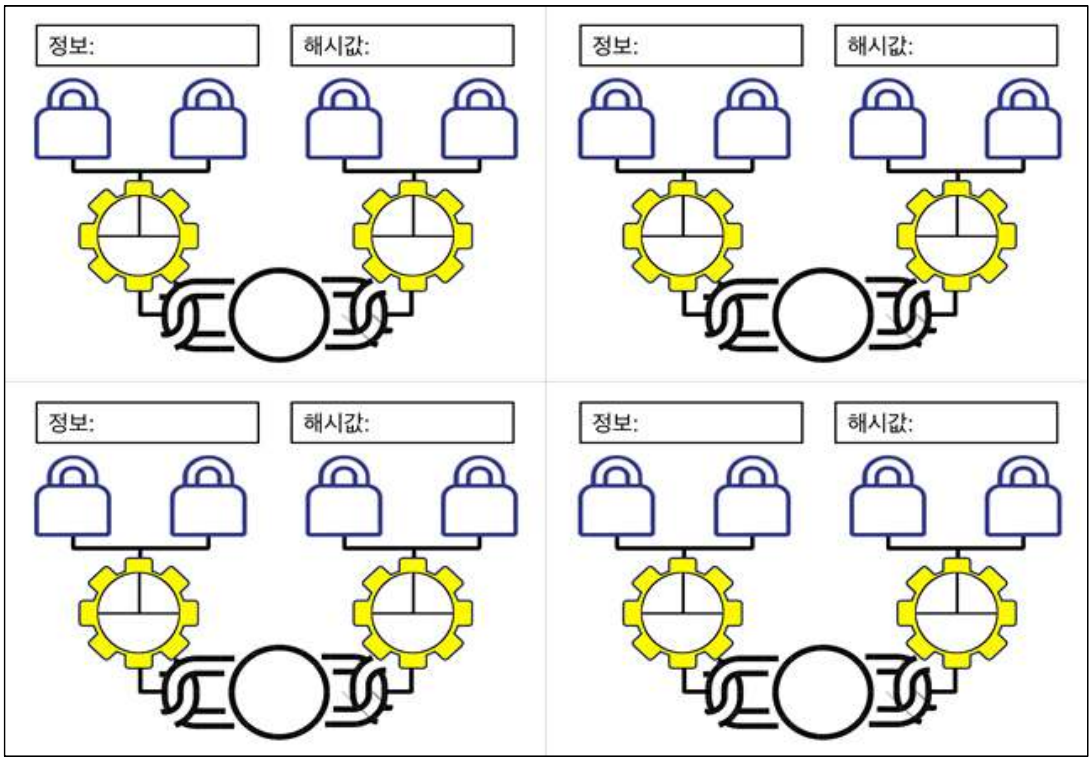
블록체인 핵심원리를 학습할 수 있는 학습 게임 개발 후 이를 중심으로 체제적 수업 모형을 디자인하였다. 본 교육 프로그램은 SW 활용 교육을 받은 초등학생을 대상으로 설계하였으며, 블록체인의 핵심원리를 정보보안의 관점에서 학습하게 된다. [그림 Ⅳ-11]에서 본 교육 프로그램의 수업 모형을 확인할 수 있다.

[그림 IV-11] 블록체인 핵심원리 교육 프로그램 수업 모형

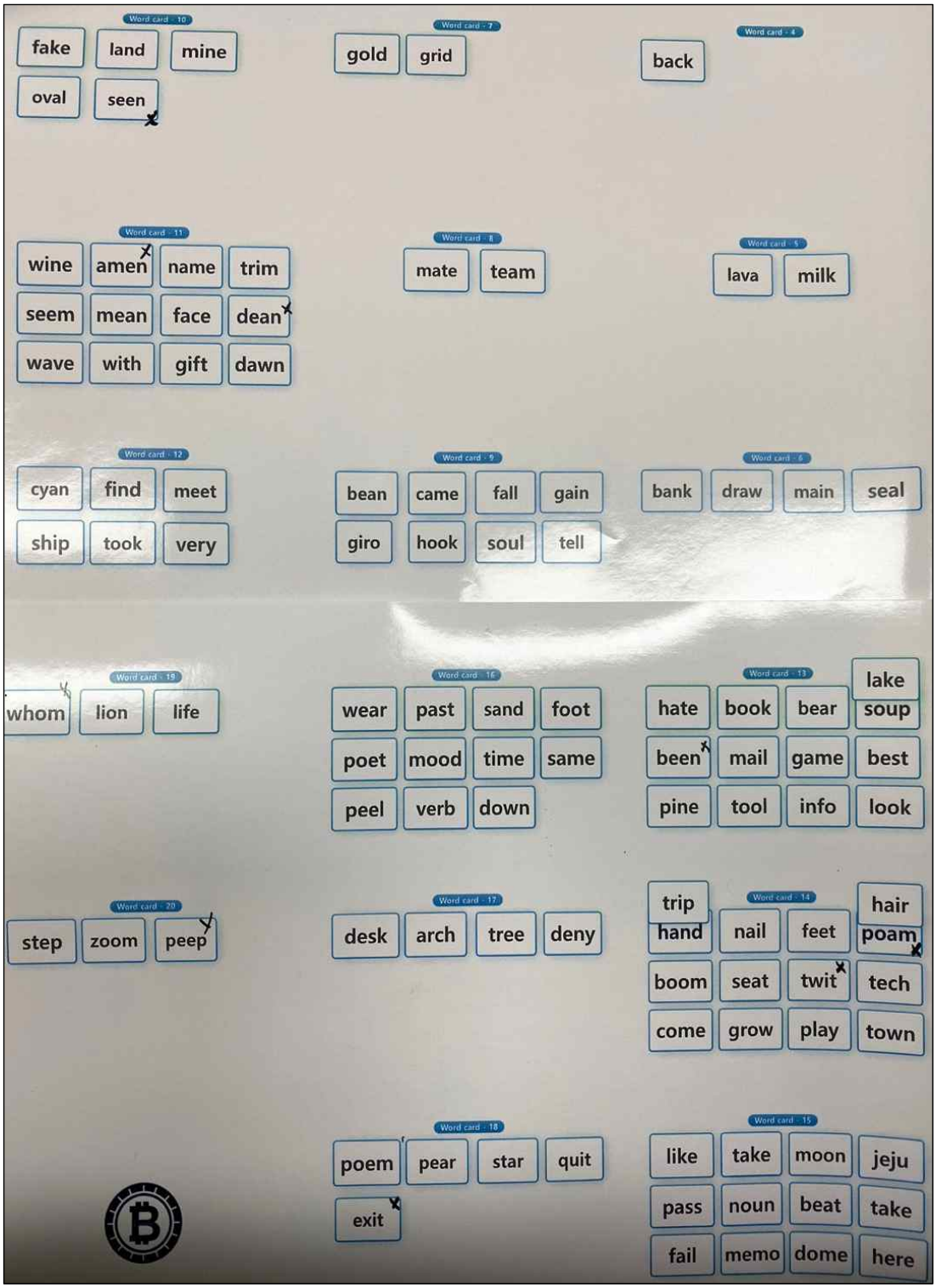
본 수업 모형은 총 10단계로 구성하였으며, 먼저, 학습 목표를 설정하고 주어진 과제를 분석한 다음, 마인드맵을 통하여 학습자의 특성을 분석한다. 이후, 교육의 수행 목표를 진술하고 검사 문항과 교수 전략을 개발한 다음 교육 프로그램을 개발하고 형성 평가를 시행한다. 평가 결과를 바탕으로 프로그램을 수정하고 학습 참여자의 창의적 문제해결력 검증을 시행한다.

(4) 온·오프라인 활용 교육 자료

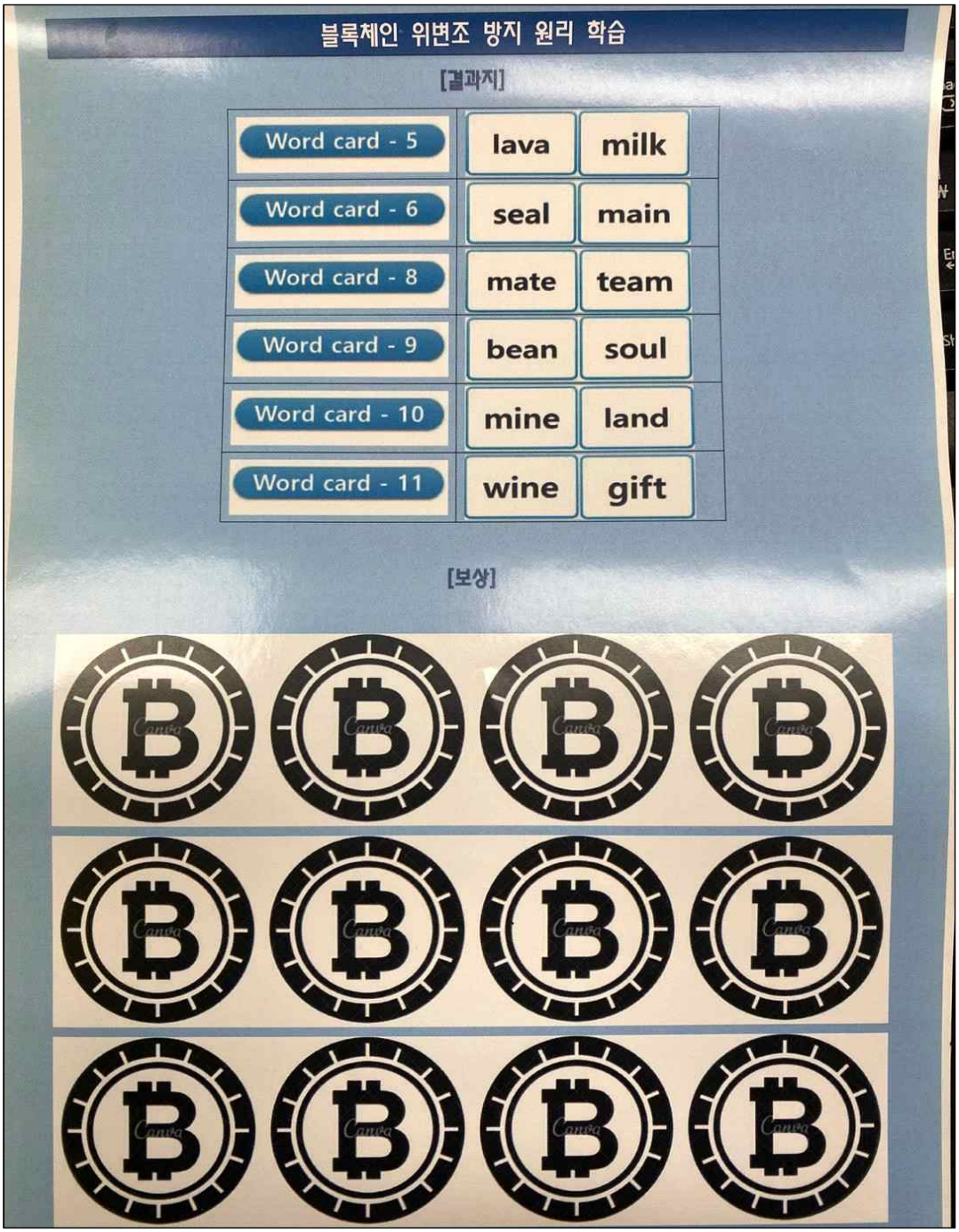
블록체인 핵심원리 교육 프로그램은 온라인과 오프라인 수업 환경에서 모두 활용할 수 있도록 설계하였으며, 먼저, 학습 게임에 필요한 자료들은 카드, 보상으로 제공할 암호화폐가 있다. 학습 게임은 오프라인 교구로 개발하였다. [그림 Ⅳ-12], [그림 Ⅳ-13], [그림 Ⅳ-14]는 블록체인 학습 게임을 위해 개발된 자료이다. [그림 Ⅳ-12]는 단어를 해시값으로 변환하는 게임 카드로 단어는 4음절로 이루어진 단어만 주어진다. [그림 Ⅳ-13]은 [그림 Ⅳ-12]에 주어지는 단어이다. 본 게임은 단어마다 고유의 해시값이 있고 주어진 카드 중에서 같은 해시값을 가진 한 쌍의 단어를 찾는 사람이 코인을 보상으로 받게 되며 [그림 Ⅳ-14]는 정답지와 코인의 이미지 워크시트이다. 보상인 코인은 별도 제작할 수 있지만, 본 정답지에서 잘라서 쓸 수 있도록 편의성을 제공하였다.



[그림 Ⅳ-12] 블록체인 핵심원리 학습 게임 카드



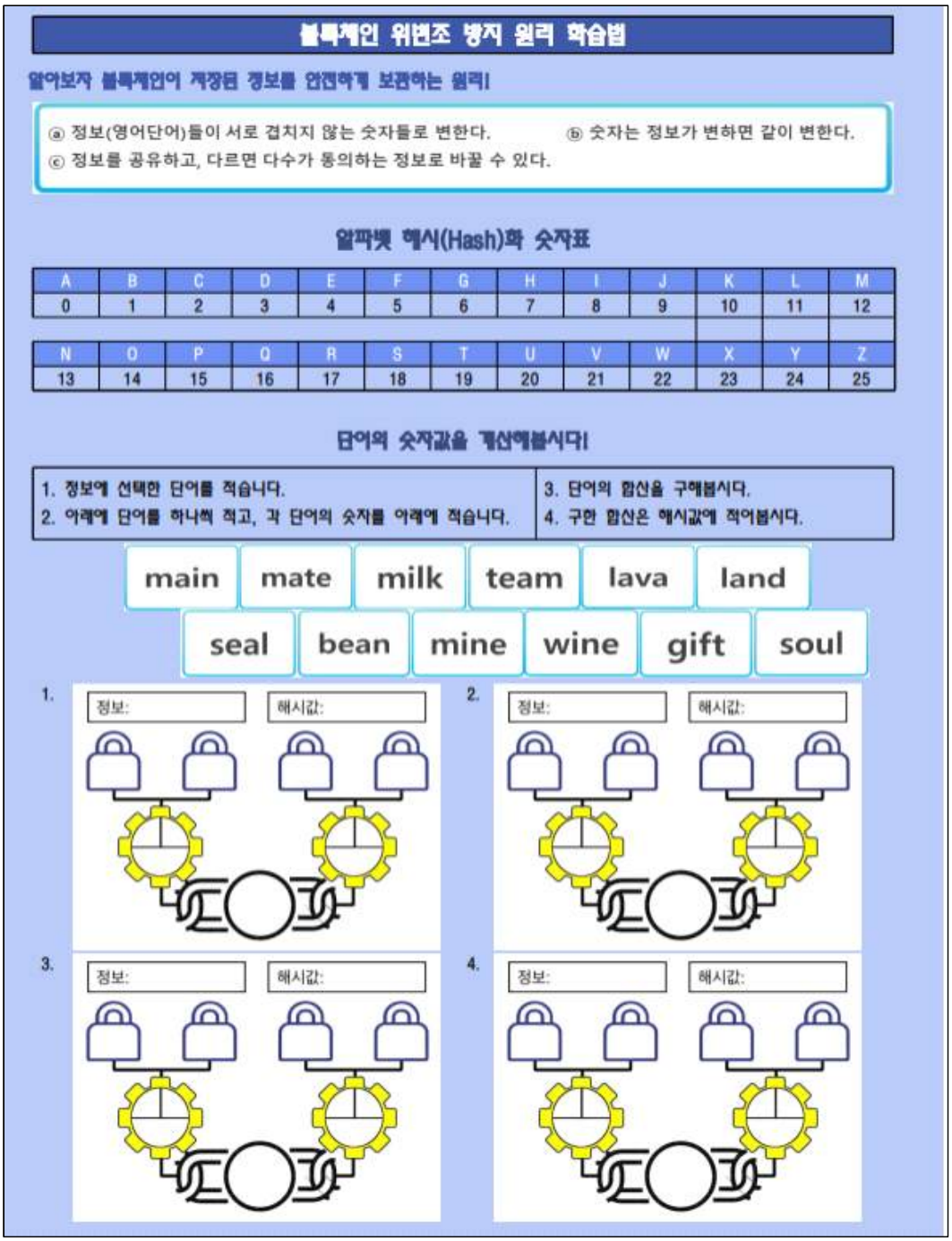
[그림 IV-13] 블록체인 핵심원리 학습 게임 단어 카드

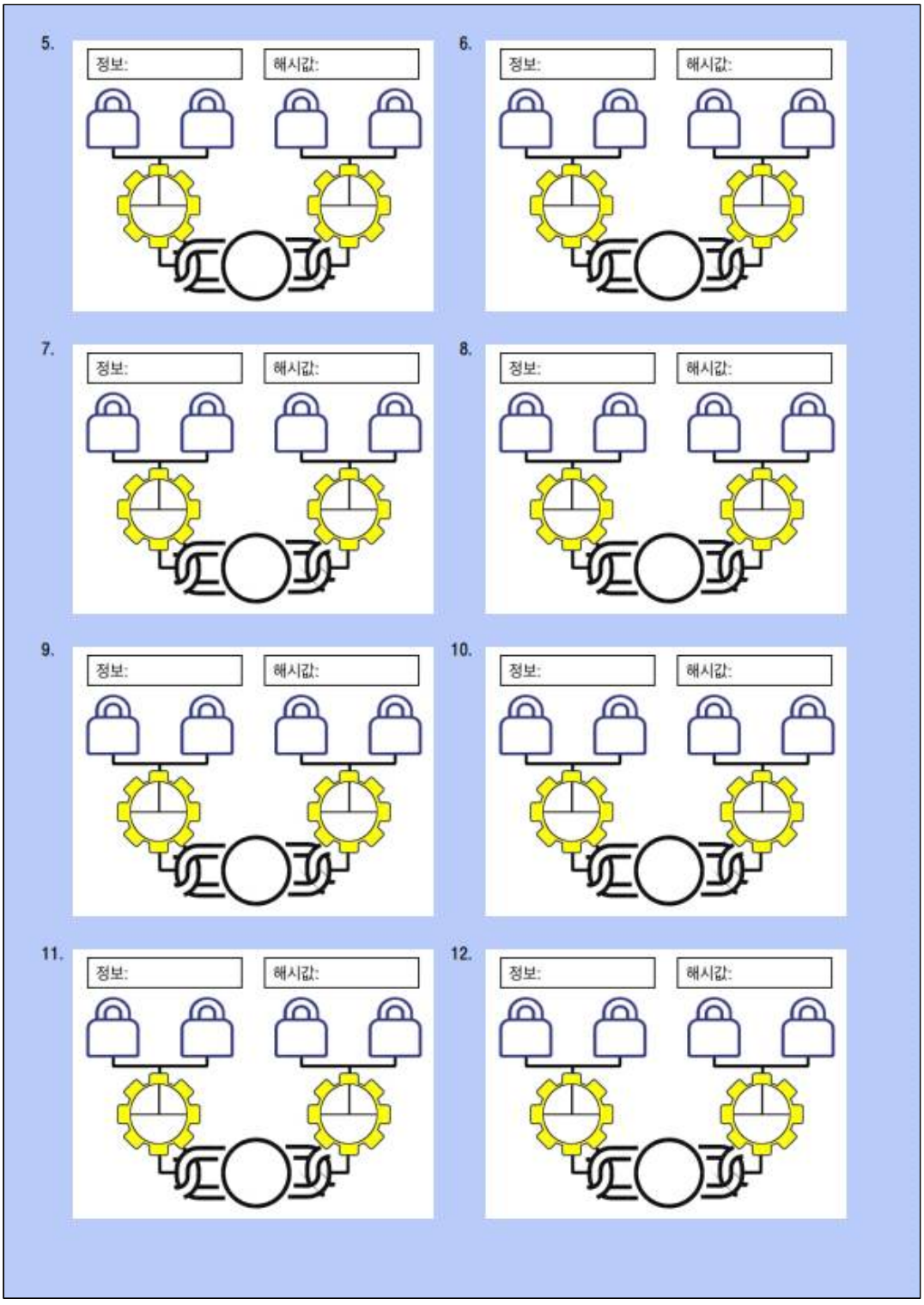


[그림 IV-14] 블록체인 핵심원리 학습 게임 자료

더불어, 교육 프로그램에 학습 게임 접목 시 활용할 수 있는 교수학습자료로 워크시트가 있다. 워크시트에는 블록체인이 저장된 정보를 안전하게 보관하는 원리를 이해하고 결국 위조와 변조가 어렵다는 블록체인의 원리를 이해하도록 설

계했다. [그림 Ⅳ-15]는 블록체인 위조 및 변조 방지원리 워크시트이며, [그림 Ⅳ-16]은 온라인 상호작용 소통 도구인 라이브 워크시트(Liveworksheet)를 사용하여 온라인 교육 환경에서 활용할 수 있도록 설계된 워크시트이다.





[그림 IV-15] 블록체인 위조 및 변조 방지 워크시트

블록체인 위변조 방지 원리 학습법

알아보자 블록체인이 저장된 정보를 안전하게 보관하는 원리!

ⓐ 정보(영어단어)들이 서로 겹치지 않는 숫자들로 변한다. ⓑ 숫자는 정보가 변하면 같이 변한다.
ⓒ 정보를 공유하고, 다르면 다수가 동의하는 정보로 바꿀 수 있다.

알파벳 해시(Hash)화 숫자표

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

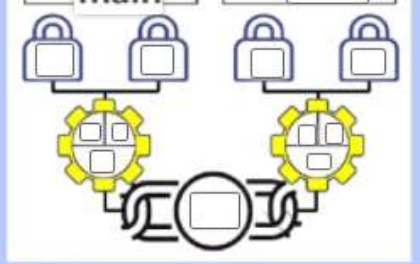
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

단어의 숫자값을 계산해봅시다!

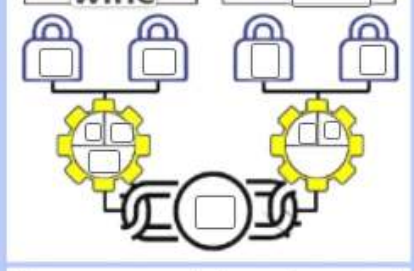
1. 정보에 선택한 단어를 적습니다.
2. 아래에 단어를 하나씩 적고, 각 단어의 숫자를 아래에 적습니다.
3. 단어의 합산을 구해봅시다.
4. 구한 합산은 해시값에 적어봅시다.

	mate	milk	team		land
seal	bean	mine		gift	soul

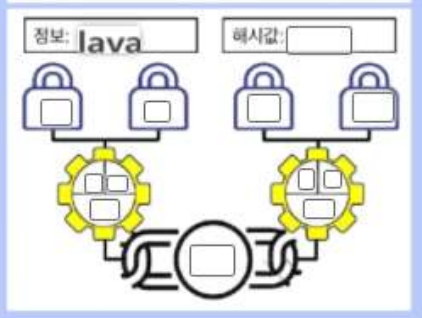
1. 정보: main 해시값:



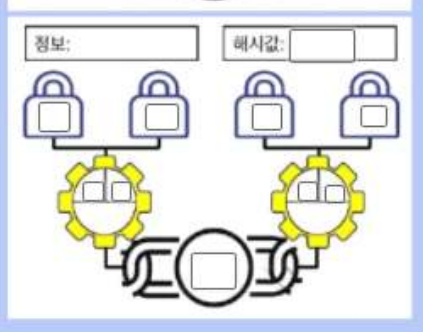
2. 정보: wine 해시값:

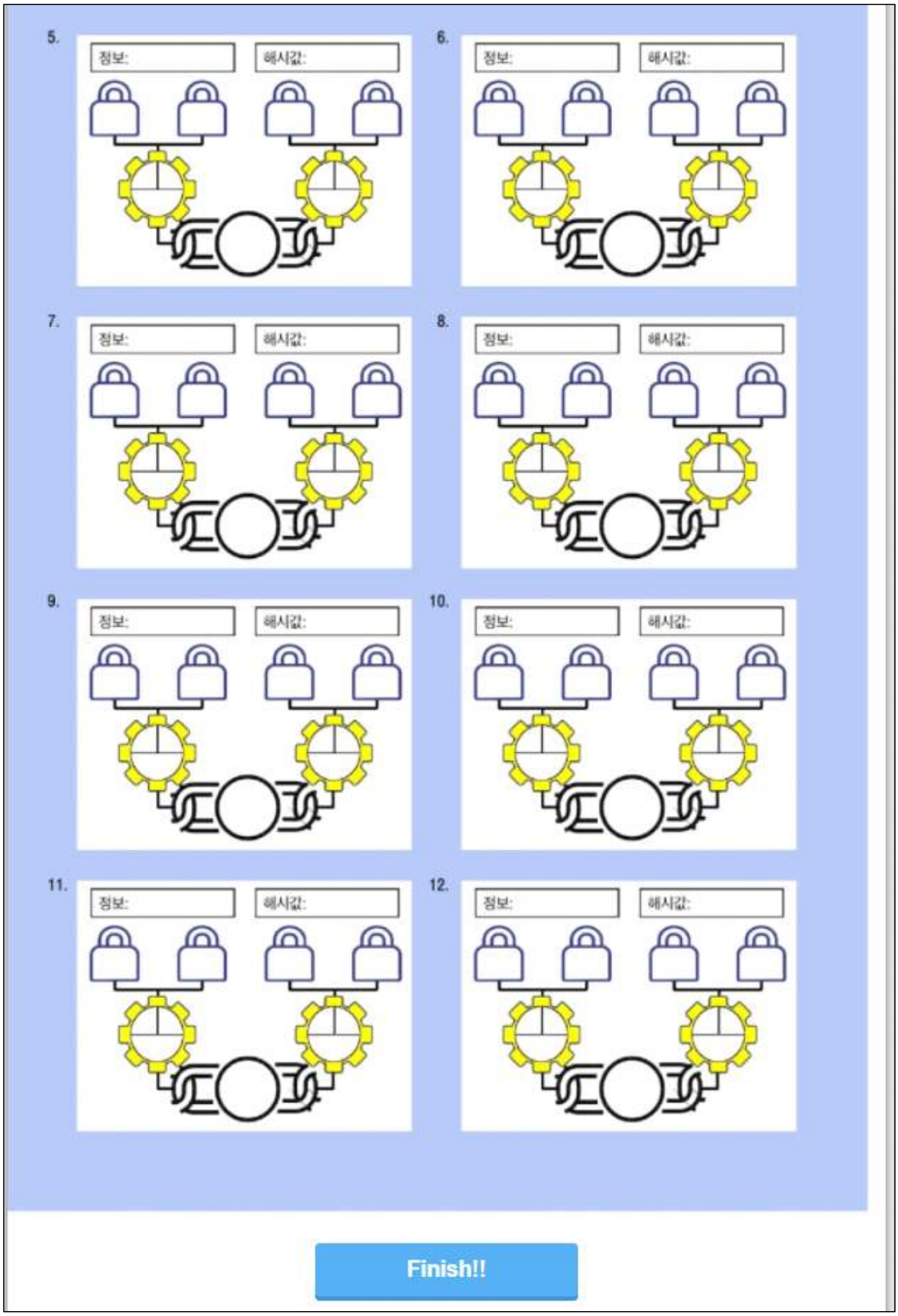


3. 정보: lava 해시값:



4. 정보: 해시값:





[그림 IV-16] 온라인 블록체인 핵심원리 교육 프로그램 활용 라이브워크시트

4.3.3. 연구 대상자 초등학생 학습자 선정

게이미피케이션 요소를 접목한 본 교육 프로그램의 효과성을 분석하기 위하여 본 교육 프로그램의 대상자인 초등학생 학습자를 연구 대상자로 선정하였다[55][56]. 본 교육에 참여한 학생들은 전국의 초등학생 2학년부터 6학년으로 구성되었으며, 총 303명이 본 교육 프로그램에 참여하였다. 가장 많은 인원이 참여한 지역은 제주로 93명이 참석하였으며, 경남지역에서 가장 적은 인원인 35명이 참여하였다. [표 Ⅳ-11]은 블록체인 핵심원리 교육 프로그램에 참여한 연구 대상자의 현황을 나타내고 있다.

[표 Ⅳ-11] 블록체인 핵심원리 교육 프로그램 연구 대상자

학교명 / 학년	기간	학생 수(명)
(경기)ㅇㅇ초등학교/5학년	'21.09	50
(경기)ㅇㅇ초등학교/4학년	'21.09	25
(경남)ㅇㅇ초등학교/2~6학년	'21.09	5
(경남)ㅇㅇ초등학교6학년	'21.09	30
(울산)ㅇㅇ초등학교/5학년	'21.09	18
(울산)ㅇㅇ초등학교/5학년	'21.09	25
(경북)ㅇㅇ초등학교/5학년	'21.09	32
(경북)ㅇㅇ초등학교/5학년	'21.09	25
(제주)ㅇㅇ초등학교/2학년	'21.09	25
(제주)ㅇㅇ국제학교/4~5학년	'21.09	40
(제주)ㅇㅇ초등학교/6학년	'21.09	28
합계		303

4.3.4. 블록체인 핵심원리 교육 프로그램 적용

본 논문에서 제안하는 블록체인 핵심원리 교육 프로그램의 학습 목표인 블록체인 핵심원리 이해를 통한 창의적 융복합 정보보안 인재 양성을 효과적으로 달성할 수 있는지에 대한 효과성 분석을 위해 [표 Ⅳ-11]의 연구 대상자에게 본 교육 프로그램을 적용하였으며, 전국 초등학생을 대상으로 2021년 9월 한 달 동안 303명에게 3차시의 교육 프로그램을 적용하였다. 1차시에서는 블록체인 핵심원리 개념에 대해 교수하였다. 이 과정에서 학생들은 마인드맵을 통해 창의적으로 블록체인을 학습할 수 있으며, 2차시에는 블록체인 학습 게임을 실시하였다. 3차시에는 1, 2차이에서 학습한 내용을 근거하여 교수자가 가상으로 설정한 블록체인 위조와 변조 문제 상황에 대해 창의성을 발휘하여 문제를 해결하는 내용으로 구성되었다. 교육 시간은 학교마다 상이하며, 한 차시에 필요한 시간은 40분이다. [표 Ⅳ-12]는 블록체인 핵심원리 교육 프로그램 적용을 위한 세부 일정이며, [그림 Ⅳ-17]은 교육 프로그램 참여 연구 대상자의 모습이다.

[표 Ⅳ-12] 블록체인 핵심원리 교육 프로그램 적용 세부 일정

시간	내용	장소
10′	입장 및 환영사	각 연구 대상 초등학교 개별 실행
40′	[1차시] 블록체인 핵심원리 개념 이해	
10′	휴식	
40′	[2차시] 블록체인 핵심원리 학습 게임 수행	
10′	휴식	
40′	[3차시] 블록체인 문제 해결	
10′	정리	

[그림 IV-17] 블록체인 핵심원리 교육 프로그램 적용

4.3.5. 블록체인 핵심원리 교육 프로그램 창의적 문제해결력 조사 결과분석

본 교육 프로그램을 적용함으로써 초등학생이 블록체인에 대한 핵심원리를 이해하여 실생활을 살아갈 때 마주치는 정보보안과 관련한 여러 문제를 여러모로 바라보고 이전에 생각하지 못했던 방식으로 문제를 해결할 수 있는 능력을 길러주는 것이 중요하다.

따라서, 본 논문에서 제안하는 블록체인 핵심원리 교육 프로그램의 적용 효과 분석을 위해 교육 시작 전과 후에 창의적 문제해결력에 대한 설문 조사를 시행하였다. 창의적 문제해결력은 학생들의 문제 발견 및 분석, 아이디어 생성, 실행 계획, 실행, 설득 및 소통, 혁신 성향을 파악할 수 있도록 총 24개의 문항으로 조사 도구를 구성하였다. 모든 문항은 5점 척도를 이용한 선다형 구성이었으며, 22

개의 문항의 신뢰도 분석 결과 신뢰도 계수(Cronbach's alpha) 0.794로 높은 내적 일관도를 확보하였다. 효과성 분석을 위하여 IBM SPSS 24.0 Program을 사용하였으며, 분석 기법으로는 기술통계(Descriptive statistics)와 사전-사후 t-검정을 활용하였다. [표 Ⅳ-13]은 분석에 사용된 창의적 문제해결력 조사 도구이다.

[표 Ⅳ-13] 블록체인 핵심원리 교육 프로그램 창의적 문제해결력 조사 분석 도구

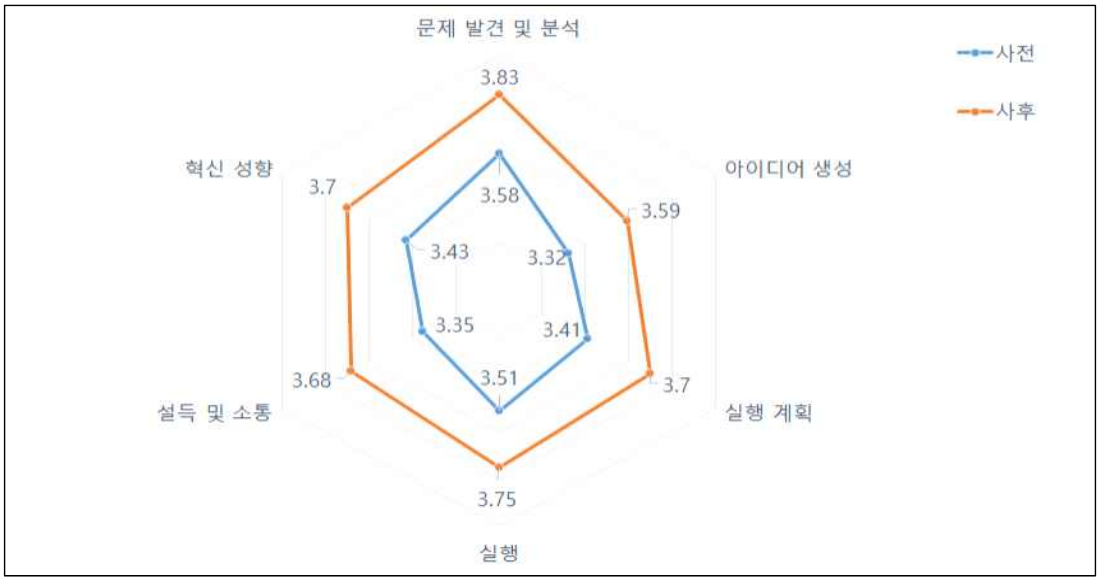
영역	문항 내용 일부	형태	문항 수	Cronbach's α
문제 발견 및 분석	'나는 '그것은 왜 그럴까'와 같은 질문을 스스로 많이 한다.', '나는 문제의 의미를 여러 측면에서 파악하려고 노력한다.', '나는 문제 해결을 하기 전에 문제를 정확히 이해하려고 노력한다.'	Likert 5점 척도	4	.784
아이디어 생성	'나는 독창적인 아이디어가 요구되는 과제를 잘하는 편이다.', '나는 짧은 시간에 아이디어를 많이 생각해낼 수 있다.', '나는 번뜩이는 아이디어로 주변 사람을 놀라게 하는 경우가 많다.'	Likert 5점 척도	4	.815
실행계획	'나는 다양한 문제 해결안들을 분석하여 가장 효과적인 문제 해결안을 잘 선택해낸다.', '나는 문제 해결에 필요한 아이디어에 대해 구체적으로 계획하여 실행에 옮긴다.', '나는 아이디어를 평가하기 위한 판단 기준을 명확하게 세운다.'	Likert 5점 척도	4	.794
실행	'나는 아이디어를 행동으로 옮기는 것을 좋아한다.', '나는 머릿속에 떠오른 아이디어를 실제로 구현하는 것을 좋아한다.', '나는 추진력이 좋다는 얘기를 많이 듣는다.'	Likert 5점 척도	4	.847
설득 및 소통	'나는 남을 설득하는 일에 자신이 있다.', '나는 발표력이 좋다는 이야기를 많이 듣는다.', '나는 내 생각을 다른 사람이 쉽게 이해할 수 있도록 잘 표현한다.'	Likert 5점 척도	4	.754
혁신 성향	'나는 새로운 아이디어를 잘 다듬어 유용하게 쓰일 수 있도록 만든다.', '나는 문제를 해결하는데 새로운 아이디어를 체계적으로 도입한다.', '나는 새로운 아이디어에 대해 다른 사람들이 동의하도록 노력한다.'	Likert 5점 척도	4	.916
총계			24	.794

본 교육 프로그램의 효과성 분석을 시행한 결과, 초등학생의 창의적 문제해결력 사전-사후 비교를 살펴보면, 사전 검사에서는 127.88점을 기록하였으며, 사후 검사에서는 138.18점으로 통계적으로 유의한 차이로 상승했음을 알 수 있다. 전체 평균에 대해서는 사전 3.41, 사후 3.71로 역시 사후 평균이 증가하였다. 문항별 가장 높은 평균치를 기록한 요소는 설득 및 소통 요소였으며 0.32로 집계되었다. 한편, 가장 낮은 평균치를 기록한 요소는 실행 요소로 0.24로 집계되었다. 그러나 모든 문항에서 통계적으로 유의한 결과를 기록하여 본 교육 프로그램의 창의적 문제해결력에 대한 효과가 검증되었음을 알 수 있다. [표 Ⅳ-14]는 블록체인 핵심원리 교육 프로그램의 창의적 문제해결력 조사 분석 결과를 보여주며, [그림 Ⅳ-18]은 이를 도식화한 결과이다.

[표 Ⅳ-14] 블록체인 핵심원리 교육 프로그램의 창의적 문제해결력 조사 분석 결과

구분	분류	평균(표준편차)	평균 차	*t*
전체 합	pre	127.88(21.20)	10.29	-5.18***
	post	138.18(24.20)		
전체 평균	pre	3.41(.56)	.30	-5.28***
	post	3.71(.73)		
문제 발견 및 분석	pre	3.58(.62)	.25	-4.35***
	post	3.83(.69)		
아이디어 생성	pre	3.32(.87)	.26	-4.23***
	post	3.59(.77)		
실행 계획	pre	3.41(.68)	.29	-5.11***
	post	3.70(.60)		
실행	pre	3.51(.83)	.24	-3.81***
	post	3.75(.75)		
설득 및 소통	pre	3.35(.79)	.32	-4.47***
	post	3.68(.81)		
혁신 성향	pre	3.43(.62)	.27	-4.69***
	post	3.70(.69)		

*p<.05, **p<.01, ***p<.001



[그림 Ⅳ-18] 블록체인 핵심원리 교육 프로그램 창의적 문제해결력 조사 도식화

본 논문에서 제안하고 있는 블록체인 핵심원리 교육 프로그램은 초등 정보보안 교육 프로그램의 일종으로 학생들의 창의적 문제해결력을 높이어 창의적 정보보안 융복합 인재 양성에 이바지하고자 하였다.

본 교육 프로그램은 전국의 초등학생에게 적용한 결과, 문제 발견 및 분석, 아이디어 생성, 실행 계획, 실행, 설득 및 소통, 혁신 성향의 모든 요소에서 골고루 유의미한 영향을 미쳤음을 확인할 수 있었다. 향후 블록체인 핵심원리 교육 프로그램 설계 시, 실행 요소가 가장 낮은 폭으로 증가하였음을 염두에 두어 학생들이 창의적으로 문제 해결을 할 때 실행성을 높여 문제 해결에 더욱 적극적으로 임할 수 있도록 구상하여 발전해 나아갈 예정이다.

4.4. 정보보안 해킹 핵심원리 교육 프로그램

4.4.1. 교육 프로그램에 적용한 네트워크 해킹 핵심 기술

본 논문에서는 초등 고학년을 대상으로 전반적인 네트워크의 흐름을 이해하고, 이 과정에서 발생하는 외부의 공격을 이해함으로써 해킹의 원리 이해를 유도하는 데 목적을 가진다. 따라서 해킹 게임에 이용된 네트워크 장비와 전반적인 흐름에 관한 내용을 서술한다. 일반적으로 사용되는 인터넷은 네트워크에 연결되기 위해 수많은 기기를 걸쳐 연결되며, 이 과정에서 적용되는 장비는 OSI 7계층에 의해 분류할 수 있다. 여기서 OSI 7계층이란 네트워크에서 통신이 일어나는 과정을 7단계로 정의한 것으로 실제 사용되는 구조와 차이는 존재하지만, 기본적으로 네트워크의 구성을 구분하는 지표이기도 하다. OSI란 국제 표준화 기구(ISO, International Organization for Standardization)에 의해 정의된 모델로, 물리 계층, 데이터 링크 계층, 네트워크 계층, 전송 계층, 세션 계층, 표현 계층, 응용 계층의 7가지 계층으로 구분된다. 각 계층의 정의는 [표 Ⅳ-15]와 같다.

[표 Ⅳ-15] OSI 7 Layer 개요

Layer	설 명
물리 계층 (Physical layer)	네트워크 통신의 가장 기본이 되는 것으로 하드웨어 전송 기술을 의미한다.
데이터 링크 계층 (Datalink layer)	프로토콜 집합인 PPP(Point to Point)를 이용하여 신뢰성 있는 데이터 전송을 위한 계층으로 CRC(cyclic redundancy check) 기반의 흐름 제어와 오류 제어가 요구된다.
네트워크 계층 (Network layer)	노드간의 이동 과정에서 경로를 찾기 위한 계층으로, 데이터를 네트워크를 이용하여 전송하고, 서비스 품질 제공을 위한 수단을 제공한다.
전송 계층 (Transport layer)	종단 간 사용자의 연결을 위해 사용되는 네트워크 구성 요소 및 프로토콜을 통해 서비스를 제공하는 계층을 의미한다.

세션 계층 (Session layer)	종단 사용자의 프로세스 통신 관리를 위해 사용되는 계층으로 TCP/IP 세션 생성 및 종료를 수행한다.
표현 계층 (Presentation layer)	코드 번역기능인 인코딩이나 데이터의 암호화 동작을 수행하는 계층을 의미한다.
응용 계층 (Application layer)	응용 프로세스와 직접적으로 관계하여 서비스를 수행하는 계층을 의미한다.

(1) 스위치(Switch)

스위치는 데이터링크 계층(L2)에서 통신을 위해 사용되는 네트워크 장치로 이더넷 스위치(Ethernet switch)로도 불린다. 네트워크 장비의 물리적 주소(Media Access Control Address, MAC Address)를 이용하여 다른 네트워크 장비로 데이터를 전달하는 장치를 의미한다. 스위치는 일반적으로 사용자 단에서 허브 다음이나 혹은 사용자와 직접적으로 연결된다. 스위치 간에 연결된 장비는 LAN(Local Area Network) 환경을 구축하여 로컬 통신망을 이용할 수 있다.

(2) 라우터(Router)

라우터는 네트워크 계층(L3)에서 네트워크 간의 네트워크 패킷을 전송하는 장치를 의미한다. 목표가 되는 위치까지의 논리적 경로를 설정하여 네트워크 간 중계 역할을 수행한다. 일반적으로 접근성이 좋은 라우터 장비는 대충에서 사용되는 AP(Access Point)로 무선공유기로도 불린다. 라우터는 다수의 LAN(Local Area Network)에 의해 구축된 네트워크이며, 다른 네트워크와 연결하여 로컬 통신망 간의 연결을 수행한다. 로컬 통신망을 외부의 다른 네트워크와 연결하는 네트워크는 WAN(Wide Area Network)이라 한다. 또한 외부에서 들어오는 트래픽에 대한 1차적인 보안 기능을 수행하는 장치이다.

(3) 방화벽(Firewall)

네트워크 방화벽은 사전에 정의된 규칙에 따라 들어오는 네트워크 트래픽을 차단하는 데 목적을 두는 장비로, 침입 차단 시스템으로도 불린다. 방화벽의 역할은 외부 네트워크로부터 내부 네트워크로 진입하려는 트래픽에 대해 신뢰성이 낮은 트래픽을 차단하는 데 있다. 차단 정책은 IP 수준에서 진행하는 차단 정책부터 트래픽에 대한 상세한 정책 설정까지 다양하게 적용된다. 방화벽은 일반적으로 라우터와 스위치 사이에 설치되어 사용되며, 보안 정책에 따라 라우터와 외부 네트워크가 연결되는 사이 지점에 설치될 수도 있다.

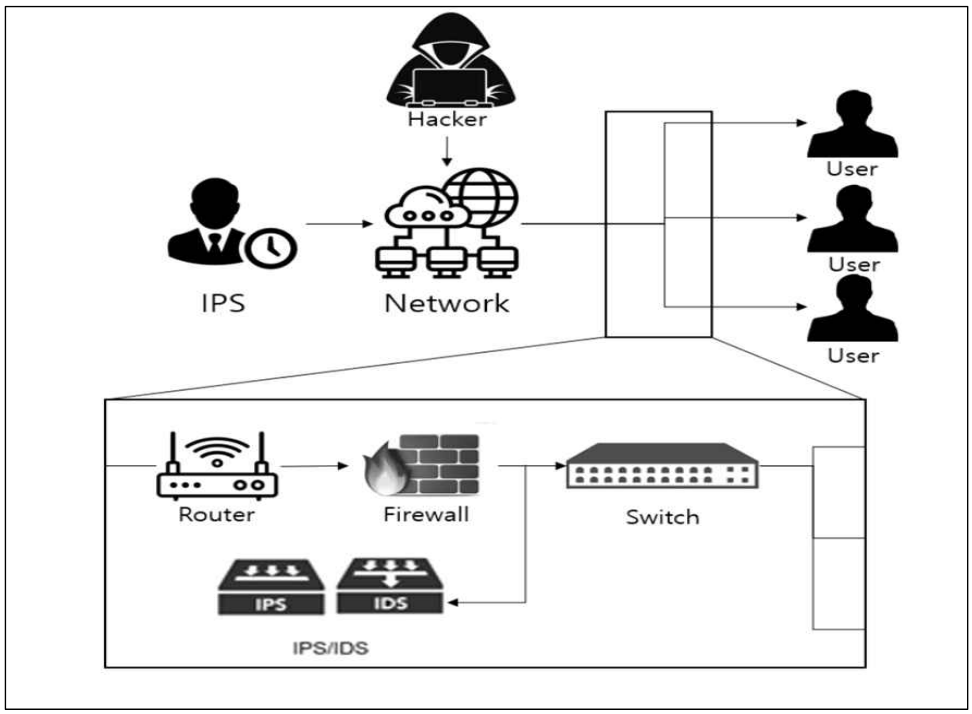
(4) 침입 탐지 시스템(Intrusion Detection System, IDS)

침입 탐지 시스템은 외부 네트워크에서 내부 네트워크로 들어오는 트래픽에 대하여 스캔하고, 해당 트래픽에서 공격 의도를 파악하는 것을 목적으로 하는 시스템을 의미한다. 가장 많이 적용되는 방식은 트래픽의 특징으로부터 악성코드를 탐지하는 시그니처 기반의 탐지 방식이다. 침입 탐지 시스템은 방화벽에서 탐지하지 못한 악의적 트래픽에 대한 탐지를 목적으로 일반적으로 사용자 네트워크단과 방화벽 사이에 설치되어 사용된다. 침입 탐지 시스템은 트래픽에 대한 검사는 수행할 수 있으나 악의적 의도를 가진 트래픽에 대한 차단과 같은 능동적 기능을 제공하지 않는다.

(5) 침입 방지 시스템(Intrusion Prevention System, IPS)

침입 방지 시스템은 외부 네트워크에서 내부 네트워크로 들어오는 트래픽에 대해 모니터링하고, 악의적 활동이 발견되는 경우 차단이나 제거와 같이 능동적인 대응을 수행하는 장비를 의미한다. 악의적 활동에 대한 탐지만을 수행하는 침입 탐지 시스템의 발전된 모습으로, 통신 과정에서 발생하는 모든 트래픽에 대해 검사를 수행한다. 침입 방지 시스템은 방화벽보다 상위의 데이터에 있는 악성 의

도까지 판별할 수 있으나, 방화벽에 비해 더 높은 성능을 요구하기 때문에 일반적으로는 방화벽의 뒤에 위치하여 통과한 트래픽에 대해서만 탐지를 수행한다. 하지만 방화벽보다 앞에 설치되어 들어오는 모든 트래픽에 대한 탐지 수행을 목적으로도 사용된다. [그림 Ⅳ-19]는 이러한 네트워크의 흐름도를 보여준다.



[그림 Ⅳ-19] 일반적인 네트워크 흐름도

이에 해당하는 일반적인 네트워크의 흐름은 위의 그림과 같다. 종단 사용자는 인터넷 서비스를 제공하는 인터넷 서비스 제공자(Internet Service Provider)가 호스팅하는 서버에 접속하여 데이터를 요청한다. 이때, 종단 사용자 단말은 데이터를 스위치를 통하여 로컬 네트워크(LAN)에 진입한다. 이후, 스위치는 IP 주소를 통해 MAC 주소를 알려주는 ARP(Address Resolution Protocol)를 통해 로컬망에 대상이 존재하는지를 확인한다. 로컬 네트워크상에 대상이 없는 경우, 스위치는 다른 네트워크와의 연결을 위해서 라우터로 연결을 요청하며, 라우터는 IP에 기반하여 대상 라우터로 경로를 구성한다. 이후, 대상의 네트워크에서는 IP 주소와 MAC 주소를 이용하여 목적지에 도달하고, 목적지의 서버는 사용자에게 데이터를 동일한 과정을 거쳐 전송한다.

외부의 공격자 또한 대상을 공격하기 위해서는 내부망에 침투하여야 하며, 일반적으로 외부망과 가장 인접한 라우터에 접근하게 된다. 이후 라우터의 보안 기능에 의해 탐지되지 않는 경우 공격자의 트래픽은 방화벽으로 진입한다. 방화벽은 설정에 따라 트래픽에 대한 차단을 수행하며, 트래픽이 방화벽을 통과하는 경우, 침입 탐지 시스템과 침입 방지 시스템으로 트래픽이 전송된다. 이 과정에서 침입 탐지 시스템은 사용자에게 전송되는 트래픽을 스캔하는 것이며, 침입 방지 시스템은 사용자에게 가는 트래픽이 먼저 시스템을 거쳐 간다는 차이가 존재한다. 즉 공격자는 내부망에 침투하기 위해서 다양한 네트워크 장비를 거쳐야만 하며, 이 과정을 본 교육 프로그램에서는 교육과정으로 설계하였다.

4.4.2. 해킹 핵심원리 교육 프로그램 설계

(1) 개발 절차

본 논문의 해킹 원리 핵심원리 교육 프로그램은 학습 게임을 중심으로 하이브리드 블렌디드 실천모형의 수업 설계 개발 절차와 Livingston & Stoll(1973)이 제안한 시뮬레이션 교육 게임 제작 절차를 참고하여 개발되었다[87]. [표 Ⅳ-16]은 해킹 원리 핵심원리 교육 프로그램의 개발 절차를 보여준다.

전반적으로는 학습 목표를 설정하고 소재를 선정하여 구조와 자료를 설계한 다음 규칙 세운 후 작성된 규칙에 따라 개발된 학습 게임과 교육 프로그램을 실행하고 수정하였다. 개인 컴퓨터와 태블릿 등 디지털 기기를 활용할 수 없는 환경에서도 정보보안 교육을 시행할 수 있도록 언플러그드 교육 프로그램으로 설계하였다[88][89].

[표 IV-16] 해킹 원리 핵심원리 교육 프로그램 개발 절차

[표 Ⅳ-15]의 해킹 원리 핵심원리 교육 프로그램의 개발 절차를 살펴보면, 먼저, 하이브리드 블렌디드 실천모형의 준비(Ready) 단계에 해당하는 첫 번째 단계에서는 구체적으로 학습 목표를 설정하였다. 학습 목표는 해킹 원리학습을 통한 정

보보안 언플러그드 교육으로 설정하였다.

두 번째 설계(Set) 단계는 Livingston & Stoll(1973)이 제안한 학습모델 개발 절차에서 제안하는 학습 게임 소재 선정, 학습 게임 구조 디자인이 포함된다. 학습자료 선정에서는 시뮬레이션 게임 모델에 정보보안 해킹 원리학습을 적용하여 세부적인 학습의 구성 방안을 정립했다[60][90][91]. 학습 게임 구조로는 게임 말과 리소스, 게임판을 설계하였으며, 외부 요인에 대한 타겟을 설정했다.

세 번째 실행(Go) 단계에서는 게임 규칙을 제공하며, 교육 프로그램 자료를 개발한다. 학습 게임의 규칙을 게임의 목표, 절차, 역할에 따라 작성하였으며, 교육 프로그램의 자료로는 워크시트, 미션시트와 같은 교수학습자료를 개발하였다.

마지막 평가(Review) 단계에서는 마지막으로 개발된 교육 프로그램을 시범적으로 적용해보고 수정 보완하도록 하였다.

(2) 학습 게임 단계별 전개 내용

해킹 핵심원리 학습 게임은 Hack, Defense, Fix의 3단계에 걸쳐 해커 X가 출구까지 무사히 나갈 수 있도록 미션을 수행하도록 설계하였는데, 학습 게임에 참여하는 플레이어인 학습자는 방향키, 회전 패널, 데이터 파일, 알람, 허니팟 등 다양한 구성을 통해 해킹 시도를 저지하는 경험을 통해 해킹을 간접적으로 이해하고 방어의 중요성을 습득할 수 있다[92]. 학습 게임에서는 방향키는 라우터를 의미하며, 회전 패널은 트래픽을 의미한다. 또한, 데이터 파일은 클라이언트, 알람은 IDS/IPS를 대치하며, 허니팟은 정보보안에서 사용하는 용어를 그대로 사용하였으며, 네트워크에 공격이 있는지를 알아채는 도구이다. [표 Ⅳ-17]은 학습 게임의 구성 요소와 정보보안에서 대치되는 개념이다.

[표 IV-17] 학습 게임 내 구성 요소 역할과 시스템

구성 요소	주요 역할	대치 시스템
해커	게임 플레이어	-
방향키	해커의 앞, 뒤, 좌, 우 방향을 결정할 수 있는 키	라우터
회전 패널	방향을 시계 방향과 반 시계 방향으로 돌릴 수 있는 패널	트래픽
데이터 파일	해커가 빼내기를 원하는 정보	클라이언트
알람	해커 침입 알림 시스템	IDS/IPS
허니팟	해킹 실패를 유인하는 장애물	허니팟
출구	해킹 성공	-

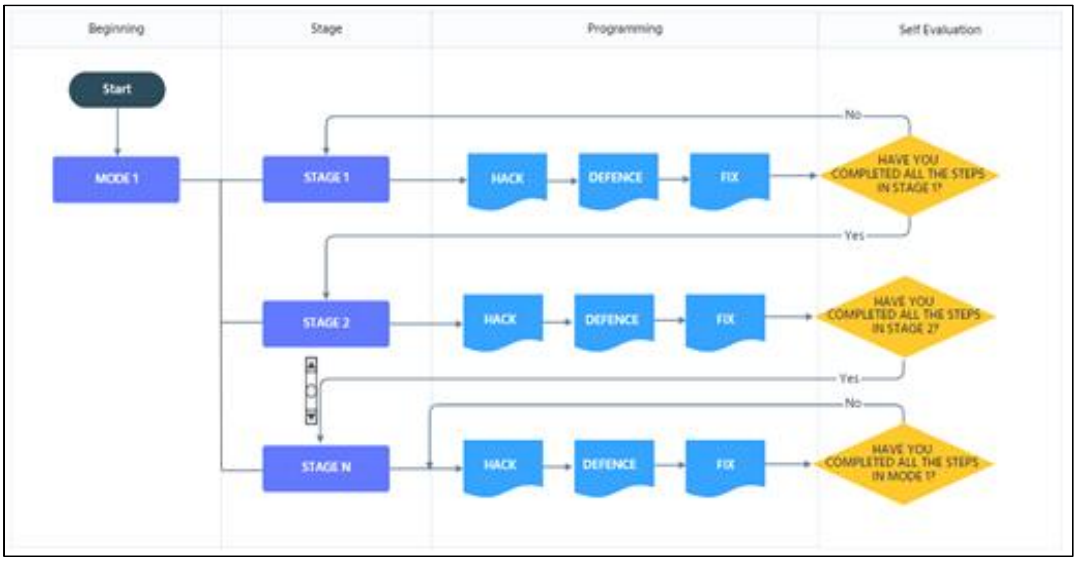
해킹 원리 학습 게임의 단계는 Hack, Defense, Fix의 3단계로 구성되어 있으며, 단계별 설명으로는 다음과 같다. Hack에서는 방향키 3개를 이용하여 코드를 만든다. 해커 X가 데이터 파일을 가지고 출구에 도달하도록 게임판을 구성하여 이동 방향을 결정한다. 플레이어는 작성한 코드대로 테스트해본다. 이때 트래픽의 방향키에 맞춰 한 칸씩 회전한다. 해커 X가 데이터 파일을 집어서 마지막에 이동할 지시대로 출구에 도착하면 학습자는 다음 스테이지로 넘어갈 수 있다.

다음 스테이지인 Defense에서는 Hack에서 코딩한 프로그램을 분석하고 취약점을 찾는 것이 목표이다. 해커는 프로그램을 바꾸고 바이러스를 감염시킬 수 있는 방법으로 나가는데 방어자인 플레이어는 해커가 안전하게 탈출할 수 없도록 허니팟으로 해커를 유인해야 한다. 학습자는 Hack에서 설정해놓은 방향키 3개와 교사가 설정한 변수의 순서를 변경하여 출구에 도달해야 한다. 교사가 정한 횟수를 넘기거나 목적지가 아닌 곳에 도달하면 실패로 본다. 학습자가 미션지가 제시한 설정에 따라 게임판을 조작하고 워크시트 위 방향키와 회전 패널을 움직여서 해커 X가 허니팟에 도착하면 이 단계를 넘어갈 수 있다. 플레이어는 작성한 코드를 남겨두고 Fix로 넘어간다.

Fix에서는 공격자가 이동하는 경로에 알람을 설치하고 공격자가 침입하려는 시도를 파악하는 것이 목적이다. 학습자인 플레이어는 해킹을 방해하는 방어자로

알람을 설치하며, 알람에 해커가 도달하면 허니팟으로 이동할 수 있도록 구성해야 한다. 해커가 알람을 지나치지 않거나 알람을 지나쳤으나 허니팟에 도달하지 못하면 실패로 간주한다. 단, 해킹 프로그램 추적 시 해커 X가 허니팟에 도달하기 전 알람이 울려야 한다. Defense에서 코딩한 프로그램이 Hack에서 코딩한 프로그램을 방해하지 않고 출구에 도달하면 플레이어가 이길 수 있다.

학생들은 게임에 참여하면서 자연스럽게 학생들은 정보보안의 다양한 요소와 해킹의 원리를 이해할 수 있다. [그림Ⅳ-20]은 해킹 원리학습 게임의 플로우이다.

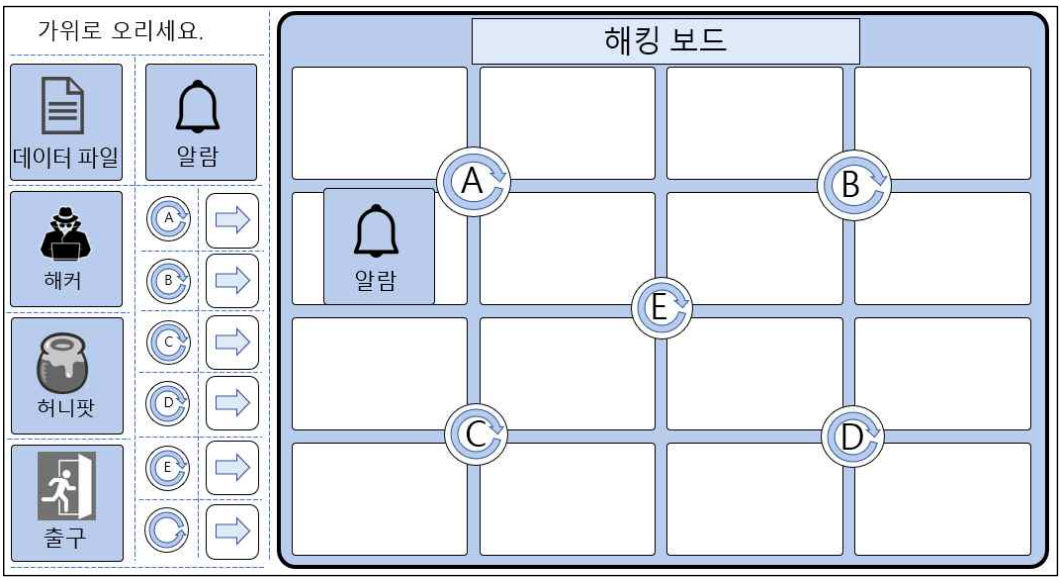


[그림 Ⅳ-20] 해킹 원리 핵심원리 학습 게임 플로우

(3) 교수학습 자료

본 교육 프로그램을 수업에 활용하기 쉽도록 다양한 교수학습 자료를 개발하였는데, 개발한 자료로는 학습 게임 교구, 워크시트, 미션지 등을 포함한다. 학습 게임에 필요한 교구로는 보드판, 회전 패널, 방향키, 데이터 파일, 해커, 허니팟, 출구, 알람을 표시하는 게임 말이 있다. 워크시트는 Hack, Defense, Fix 단계를 표기하는 표와 해킹 보드로 구성되어 있다. [그림 Ⅳ-21], [그림 Ⅳ-22]는 해킹 원리 핵심원리 교육 프로그램에 대한 교수학습 자료이다.

[그림 IV-21] 해킹 원리 핵심원리 학습 미션지 자료



[그림 IV-22] 해킹 원리 핵심원리 학습 워크시트 자료

4.4.3. 연구 대상자 학교 관리자 선정

본 논문에서 제안하는 해킹 원리 핵심원리 교육 프로그램을 효과적으로 현장에 적용하기 위해서는 학교 관리자가 교육의 필요성을 인지하고 향후 교육에 대한 이해와 지원이 필요하다. 학교 관리자는 학교 업무를 총괄하면서 학교의 행정과 교육과정을 감독하는 교장과 학교의 운영과 학생 지도를 담당하는 교감을 의미하며, 학교 조직의 비전을 변경하고 학교 전체의 교육 문화에 영향을 미칠 수 있다[93][94]. 학교 관리자의 이러한 특성은 본 교육 프로그램이 초등학생 학습자 외에도 공교육에 해킹 원리를 이해하는 정보보안 교육을 안정적으로 착근하는데 크게 이바지할 것이다. 이에, 학교 관리자를 본 연구의 대상자로 선정하였다[95].

그러나, COVID-19의 영향으로 본 교육 프로그램은 제주 지역의 초등학교 교장으로 연구 대상자를 한정하였다. 이에, 학교 관리자를 본 연구의 대상자로 선정하였으며, 총 2번에 걸쳐 시범적으로 교육 프로그램을 적용하였다. 1회차에는 43명이 참가하였으며, 2회차에는 26명이 참여하여 총 69명의 제주 지역 교장 대상 교육으로 진행하였다. [표 Ⅳ-18]은 연구 대상자의 일반적 특성이다.

[표 Ⅳ-18] 해킹 원리 핵심원리 교육 프로그램 연구 대상자

분류		인원(비율(%))	총계(%)
학교급	초등학교	69(100)	69 (100)
	중학교	0(0)	
	고등학교	0(0)	
	기타	0(0)	
	강원	0(0)	
	경기	0(0)	
	경남	0(0)	
	경북	0(0)	
	광주	0(0)	

지역	대구	0(0)	69 (100)
	대전	0(0)	
	부산	0(0)	
	서울	0(0)	
	세종	0(0)	
	울산	0(0)	
	인천	0(0)	
	전남	0(0)	
	전북	0(0)	
	제주	69(100)	
	충남	0(0)	
	충북	0(0)	
직급	교감	0(0)	69 (100)
	교장	69(100)	
	장학관	0(0)	

4.4.4. 해킹 핵심원리 교육 프로그램 적용

제주 지역 초등학교 교장 69명을 연구 대상자로 선정하여 2020년 11월 5~6일에 본 교육 프로그램을 적용하였으며, 3차시에 걸쳐 교육 프로그램을 설계하였다. 1차시에는 해킹 핵심원리와 시스템을 교수한다. 2차시에는 개발된 학습 게임을 수행해본다. 이때 1차시에서 학습한 원리와 기술을 자연스럽게 습득할 수 있는 기회를 제공한다. 연구 대상자들은 해커 입장과 방어자의 입장을 간접적으로 체험해보며, 라우터, 트래픽, IDS/IPS, 클라이언트, 알람 등 다양한 요소를 이해할 수 있었다. 3차시에는 1, 2차시에서 학습한 내용을 토대로 학교 교육에서 정보보안 교육이 왜 필요한지, 앞으로 정보보안이 얼마나 중요하게 작용할 것인지, 학교 교육에서 이를 수행해야 하는 이유와 중요성에 대해 논의하는 시간을 가진

다. [표 Ⅳ-19]는 해킹 핵심원리 교육 프로그램 적용을 위한 세부 일정이며, [그림 Ⅳ-23]은 교육 프로그램 적용에 참여한 연구 대상자의 모습이다.

[표 Ⅳ-19] 해킹 핵심원리 교육 프로그램 세부 일정

시간	내용	장소
12:50~13:00(10′)	입장 및 환영사	제주 J-CUBE
13:00~14:00(60′)	[1차시] 해킹 원리 핵심원리의 이해	
14:10~14:20(10′)	휴식	
14:20~15:20(60′)	[2차시] 해킹 원리 학습 게임 체험	
15:20~15:30(10′)	휴식	
15:30~16:30(60′)	[3차시] 해킹 원리 핵심원리 학습의 중요성	
16:30~16:40(10′)	정리	

[그림 Ⅳ-23] 해킹 원리 핵심원리 교육 프로그램 적용

4.4.5. 해킹 핵심원리 교육 프로그램 만족도 조사 결과분석

해킹 핵심원리 교육 프로그램의 적용 효과를 분석하고자 적용 종료 후 연구 대상자를 대상으로 만족도 조사를 시행하였으며, 양적 및 질적 연구를 통해 조사 결과를 분석하였다. 만족도 조사의 도구로는 Likert 5점 척도로 구성한 12문항으로 설계하였으며, 문항의 내용으로는 해킹 원리 핵심원리 콘텐츠 이해 도움도, 교육 프로그램 만족도, 강사진의 적절성, 교육의 필요성, 본인의 참가 성실도, 행정절차의 적절성, 교육 시설 만족도, 교육 지원 적합성, 교육 시간(일정) 편성의 적합성, 프로그램별 구성 및 내용 만족도로 구성하였다. 질적 연구를 위해 FGD(Focus Group Discussion)를 실시하였으며, 교육 프로그램 만족도 대한 개방적 의견을 수집하였다. 양적 연구 분석을 위해서는 IBM SPSS 24.0 program을 활용하였으며, 기술 통계분석의 요약된 통계량을 계산하는 평균 분석을 시행하였다. 질적 연구 분석에서는 집단 심층 면접을 통해 더욱 심층적인 현장의 의견을 수집하였다. [표 Ⅳ-20]은 양적 연구에 활용된 만족도 조사 도구이다.

[표 Ⅳ-20] 해킹 핵심원리 교육 프로그램 만족도 조사 도구

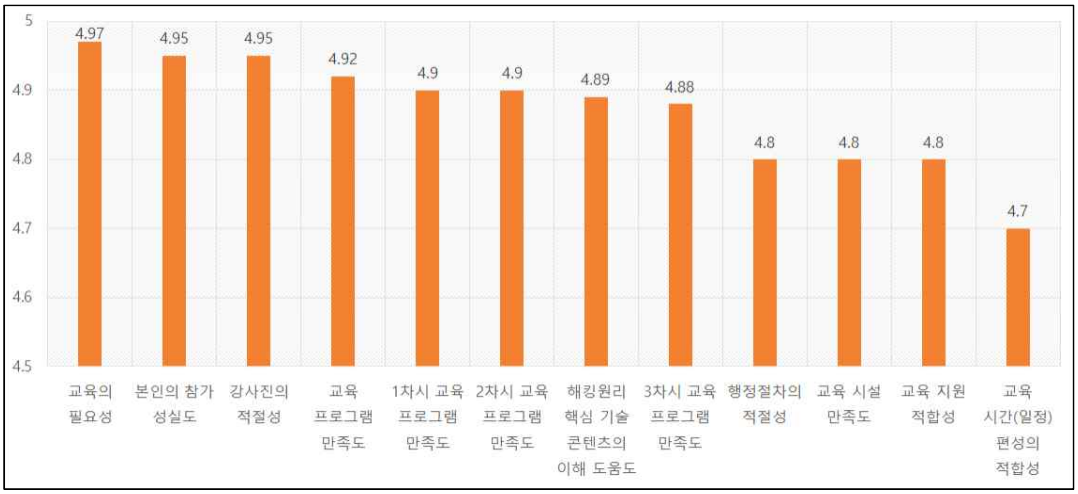
연번	문항	형태
1	해킹 원리 핵심원리 콘텐츠의 이해 도움도	Likert 5점 척도
2	교육 프로그램 만족도	Likert 5점 척도
3	강사진의 적절성	Likert 5점 척도
4	교육의 필요성	Likert 5점 척도
5	본인의 참가 성실도	Likert 5점 척도
6	행정절차의 적절성	Likert 5점 척도
7	교육 시설 만족도	Likert 5점 척도
8	교육 지원 적합성	Likert 5점 척도
9	교육 시간(일정) 편성의 적합성	Likert 5점 척도
10	1차시 교육 프로그램 만족도	Likert 5점 척도

11	2차시 교육 프로그램 만족도	Likert 5점 척도
12	3차시 교육 프로그램 만족도	Likert 5점 척도

[표 Ⅳ-21]에 따르면, 전체적인 교육 프로그램 만족도는 평균 4.87점으로 매우 높게 집계되었으며, 세부적으로 가장 높게 집계된 문항은 교육의 필요성 문항으로 4.97의 만족도를 기록하였다. 한편, 가장 낮게 집계된 문항은 교육 시간(일정) 편성의 적합성 문항으로 4.70으로 집계되었다. 평균적으로 모든 문항은 4.87의 높은 만족도를 나타냈다. 이를 통해, 본 교육 프로그램이 학교 관리자들에게 본 논문에서 제안하는 교육의 필요성을 높게 인식하고 있음을 보여주었으며, 특히, 해킹 핵심원리의 이해와 해킹 핵심원리 학습 게임을 체험해 본 경험에 대해 매우 긍정적으로 평가하고 있는 것으로 판단된다. [그림 Ⅳ-24]는 만족도 조사 결과를 높은 평균부터 내림차순으로 도식화하여 나타낸 것이다.

[표 Ⅳ-21] 해킹 핵심원리 교육 프로그램 만족도 조사 결과

연번	문 항	평균	표준 편차
1	해킹 원리 핵심원리 콘텐츠의 이해 도움도	4.89	0.87
2	교육 프로그램 만족도	4.92	0.75
3	강사진의 적절성	4.95	0.95
4	교육의 필요성	4.97	0.57
5	본인의 참가 성실도	4.95	0.79
6	행정절차의 적절성	4.80	0.64
7	교육 시설 만족도	4.80	0.66
8	교육 지원 적합성	4.80	0.72
9	교육 시간(일정) 편성의 적합성	4.70	0.78
10	1차시 교육 프로그램 만족도	4.90	0.82
11	2차시 교육 프로그램 만족도	4.90	0.71
12	3차시 교육 프로그램 만족도	4.88	0.85
	총 계	4.87	0.69



[그림 IV-24] 해킹 핵심원리 교육 프로그램 만족도 조사 도식화

한편, 질적 연구를 위해 실시한 FGD를 통하여 수집된 교육 프로그램에 대한 학교 관리자의 주요 의견은 다음과 같다.

관리자를 대상으로 한 연수가 꾸준하게 이루어지면 감사하겠습니다.

- ○○초등학교 교장 김○○

질 좋은 교육 프로그램을 계획하고 추진해 주셔서 감사합니다, 수고하셨습니다.

- ○○초등학교 교장 박○○

첨단기술을 통해 해킹되는 사건을 빠르게 인식하는 방법과 실생활에서 정보보안 수칙을 지켜 해킹 피해를 줄이는 방법에 대한 강의와 철학적이며 실제적인 접근 방식에 대해 알고 싶습니다.

- ○○초등학교 교장 김○○

좋은 교육, 좋은 내용, 쾌적한 환경, 친절한 안내 운영 감사히 받고 마무리합니다.

- ○○초등학교 교장 이○○

시간이 짧아 아쉬웠습니다. 구체적이고 좀 더 심화된 교육 기회가 있다면 참가하겠습니다. 정말 감사합니다.

- ㅇㅇ초등학교 교장 황ㅇㅇ

학교 관리자들은 해킹과 관련한 정보보안 교육은 더 높은 학년 군에서 다뤄야 할 내용으로 인식하고 있었으나, 해당 교육 프로그램을 경험한 후 초등학교 수준에서 해킹 핵심원리 교육의 필요성에 대해 절실히 느꼈다고 밝혔다. 또한, 그들은 더 구체적인 해킹 예방 방법과 학생들이 실생활에서 실천할 수 있는 수칙에 대한 교육을 추가로 요구하였다. 한편, 교육 시간과 수준에 대해 아쉬움을 드러낸 의견도 집계되었는데, 교육 시간을 확장하고, 수준별 학습을 통해 심화한 내용을 교수할 수 있도록 향후 교육 프로그램의 방향을 수정할 필요가 있다.

4.5. 초등 정보보안 교육 프로그램 실증 결과분석

본 4장에서는 초등 정보보안 교육 프로그램을 총 세 가지로 나누어 제안하였다. 모든 교육 프로그램은 하이브리드 블렌디드 실천모형에 따라 설계되었으며, 다양한 창의적 기법을 적용하여 낯선 콘텐츠를 흥미로운 방식으로 받아들이고 이해할 수 있도록 설계한 것이 특징이다. 모든 프로그램은 각각 다양한 연구 대상자를 대상으로 적용되었으며, 효과성 분석을 위해 양적 및 질적 분석이 시행되었다. 조사의 결과는 IBM SPSS 24.0 Program을 활용하여 분석되었다.

본 논문에서 제안하는 초등 정보보안 교육 프로그램의 첫 번째로는 안면인식 핵심원리 교육 프로그램을 들 수 있다. 본 교육 프로그램은 전국의 현장 교원 46명에게 적용되었으며, 7문항으로 설계된 교육 프로그램 인식조사를 수행하여 교육 프로그램의 효과성을 분석하였다. 그 결과, 교사들의 안면인식 기술 원리, 인공지능의 판단 과정, 안면인식 기술 시스템의 안면인식 단계 관련한 기술적 이해도가 유의한 수준으로 상승하여($p<.001$) 본 논문에서 제안하는 첫 번째 정보보안 교육 프로그램인 안면인식 핵심원리 교육이 교원의 인식 제고에 유의한 영향을 미쳤으며, 이러한 교육이 현장에 필요함을 인식할 수 있는 계기가 되었다.

두 번째로 제안한 교육 프로그램은 블록체인 핵심원리 교육 프로그램이다. 본 교육 프로그램은 학습 게임을 기반으로 설계되었으며, 전국의 초등학생 303명을 대상으로 시범 적용되었다. 총 24문항으로 구성된 창의적 문제해결력 조사 도구를 활용하였으며, 대응 표본 t-검정 결과 문제 발견 및 분석, 아이디어 생성, 실행 계획, 실행, 설득 및 소통, 혁신 성향 모든 요소에서 통계적으로 유의한 상승률을 보였다(p<.001). 이는 본 교육 프로그램을 적용하면 초등학생이 정보보안과 관련한 예상하지 못한 문제를 만났을 때 창의적인 방식을 통해 문제를 해결할 수 있는 역량을 기르는데 이바지할 수 있다는 것을 보여준다.

마지막으로는 블록체인 핵심원리 교육 프로그램과 같이 해킹 원리를 간접적으로 체험해볼 수 있는 학습 게임을 중심으로 교육 프로그램을 설계한 해킹 핵심원리 교육 프로그램이다. 이는 제주 지역에 거주하는 총 69명의 초등학교 학교관리자를 대상으로 적용되었으며, 12문항으로 설계된 만족도 조사 도구와 FGD를 통해 현장 의견을 분석하였다. 분석 결과, 전체적인 교육 프로그램 만족도는 평균 4.87점으로 매우 높게 집계되었다. 특히, 교육 프로그램 1, 2, 3차시에 대한 만족도는 평균 4.89로 나타나 교육 프로그램의 내용 구성이 해킹 핵심원리를 이해하는 데 효과적으로 작용했음을 보여준다. 더불어, 토론을 통해 관리자들은 해당 교육 프로그램이 초등학교 수준의 해킹 원리교육의 필요성을 인식하기에 적합했다는 의견이 다수 집계되었다. 그러나, 교육 시간이 짧고 수준의 구별이 명확하지 않다는 의견을 드러낸 경우도 나타났다. 이는 향후 본 해킹 핵심원리 교육 프로그램의 교육 시간을 확장하고, 수준별 학습을 통해 기본적 원리 교육과 해킹 기술에 대한 심화 교육을 나누어 설계할 필요가 있음을 시사한다.

본 세 가지 교육 프로그램은 효과성 검증 결과를 바탕으로 향후 보다 나은 교육 프로그램으로 수정 및 고도화할 예정이며, 중·고등학생 및 다양한 연구 대상자를 대상으로 확장 설계할 필요가 있다. 또한, 학습자 요구도 분석을 통해 수준별 학습을 시행하여 심화 학습을 요구하는 영재 학생 및 정보보안 관련 핵심 인재 양성에 더욱 이바지하는 교육 프로그램으로 세부적 설계가 요구된다.

V. 결 론

정보화 사회에서 정보에 대한 가치가 높아짐에 따라 관련 범죄가 급증하고 있지만, 사용자의 연령대는 낮아지고 이에 대한 대비는 미흡하다. 다양한 분야에서의 ICT와 소프트웨어 기술이 접목된 모든 것의 디지털화(化)인 시대에 직면한 문제들은 다양한 지식의 영역을 넘나드는 융합적이고 창의적인 사고력과 실천력이 있어야 한다. 초등학생에게 정보보안 교육을 위해서 전문적 지식 등을 전달하는 전문 정보교육은 학습자의 학습 성취도를 낮추게 되는 원인이 될 수 있어서 본 연구는 초등학생들의 정보보안 교육의 이해 수준을 고려하여 게임을 하면서 자연스럽게 정보보안의 개념 등을 익힐 수 있는 게이미피케이션을 도입한 블록체인 기술의 핵심원리를 파악할 수 있는 학습 교구를 개발 하였고, 또한 많은 청소년들의 주요 관심사인 해킹 원리학습을 보드게임으로 경험 해 보아 자연스럽게 네트워크 해킹의 전문 용어 및 핵심 기술 등을 학습할 수 있도록 하였다. 또한 이는 학습자 스스로가 정보를 보호할 수 있는 능력 함양을 할 수 있도록 기술적인 부분을 더 쉽게 접할 수 있는 시나리오 기반 교육 프로그램이다. 이러한 문제 해결 역량을 컴퓨팅 사고력의 함양에서 모색하였다. 컴퓨팅 사고력은 앞서 언급한 언플러그드 컴퓨팅에서도 보여주는 대로 컴퓨터의 작동 원리를 통한 여러 활동 중에서 정보교육과의 연관성을 찾았다. 정보교육 과정은 학습자의 의사소통 능력, 문제 해결 능력, 창의력 등 고급 사고력을 각 활동에 적용하는 교육을 통하여 컴퓨팅 사고력을 탐구하고 신장시킬 수 있다는 점에 착안하여 해킹 게임으로 보안 로직 학습 교구를 구상하였고 학습자가 해커가 되어 스스로 알고리즘을 학습하고 각 단계를 완수하도록 하였다. 논문에서 제시한 해커 게임은 초등학교 고학년 수준의 학습자가 학습할 수 있도록 하였다. 기술적인 시스템의 설명 및 역할보다는 각 아이콘이 의미하는 공격· 방어의 의미를 습득하는 것에 중점을 두어 학습의 흥미를 잃지 않도록 하였다. 또한 단계를 거듭할수록 흥미보다는 정보보안의 기술 알고리즘을 구상하여 최종적으로 컴퓨팅 사고력 신장의 그 목적을 두고 있다. 향후, 초·중등생 뿐만 아니라 일반인 그리고 교육 전문가 및 관련 기술 전문가에게 시범 수업을 운영하여 검증하고 사전·후 검사 및 만족도 검사를 계획하고 실행하여 체계적인 효과성 및 만족도 분석을 통하여 완성도 있는 정보보안 학습 교구의 역할을 다할 수 있도록 지속적인 연구를 진행할 것이다.

참 고 문 헌

[1] 김충배. (2020). 초등 실과, 중등 정보 교과의 정보보안 교육과정 분석 및 개선방향 제언. 한국컴퓨터정보학회논문지, 25(10)

[2] 김진호. (2020). 청소년들의 SNS 이용에 따른 정보보안의식 분석에 관한 연구. 석사학위논문, 숭실대학교.

[3] Eyvind Garder B. Gjertsen, Erlend Andreas Gjære, Maria Bartnes, Waldo Rocha Flores. (2017). Gamification on Information Security Awareness and Training. Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017), 59-70.

[4] Jinsu Kim, Sungwook Jung, Sangik Oh, Won-chi Jung, Doik Hyun, Yujin Jung, Eunsun Choi, Namje Park. (2021). De-identification Mechanism of Block Network Image Privacy Information based on Risk Level. Advances in Dynamical Systems and Applications, 16(1), 173-180.

[5] 정유진, 박남제. (2021). 창의융합 인재 양성을 위한 3년간의 초·중등 관리자 연수 프로그램 운영. 한국융합학회논문지, 12(3), 177-186.

[6] 최계영. (2012). 스마트 시대 ICT 패러다임의 변화. TTA Journal, 143, 10-15.

[7] 기획재정부 정책조정국 정책조정총괄과. (2020). 한국판 뉴딜 추진방향. 비상경제 중앙대책본부. 20(2).

[8] 한국인터넷진흥원. (2021). 해킹사고 건수. 과학기술정보통신부. 사이버침해대응과 공개.

[9] 박경아. (2019). 청소년의 개인정보보안 인식이 보안의도와 보안행동에 미치는 영향에 관한 연구, 한국산업정보학회논문지, 24(4), 79-98

[10] 여성가족부 청소년정책관 청소년정책과, 과학기술정보통신부·한국지능정보사회진흥원.(2021). 2021 청소년 통계.

[11] 박진하. (2012). 효율적인 정보보안 교육설계 및 수행방안. 석사학위논문. 건국대학교.

[12] Keliang Zhou, Taigang Liu, Lifeng Zhou. (2015). Industry 4.0: Towards future industrial opportunities and challenges, 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2147-2152.

[13] Ebert, Christof, Carlos Henrique C. Duarte. (2018). Digital Transformation. IEEE Softw, 35(4), 16-21.

[14] 이성훈. (2013). ICT를 이용한 생활 밀착형 디지털 컨버전스에 관한 연구. 디지털융복합연구, 11(11), 429-434.

[15] 강철희. (2010). 패러다임 전환 관점에서 본 ICT 기술 발전전략. 한국방송학회 세미나 및 보고서, 85-91.
[16] 한학수. (2012). 디지털 컨버전스 시대의 특징 : 그 패러다임과 정책 방향. 디지털정책연구, 10(1).
[17] OECD. (2021). Smart policies for smart products, A policy maker's guide to enhancing the digital security of products. STI Policy Note
[18] 한국인터넷진흥원. (2021). 2021년 주요 이슈 전망, 2020 KISA report, vol.11.
[19] 최동진. (2019). 5G 시대의 차세대 IoT 보안. 기획시리즈 - 차세대 보안, 정보통신기획평가원
[20] PwC Strategy and World Economic Forum. (2019). 5G for the Fourth Industrial Revolution
[21] 권순홍, 이종혁. (2020). 자율 주행 자동차 보안 위협 및 기술 동향. 정보보호학회지, 30(2), 31-39.
[22] 김효빈. (2019). 에너지 안전 관리 시스템 보안위협 및 공격 가능 시나리오 분석. 석사학위논문, 순천향대학교.
[23] 한국전자통신연구원. (2018). 4차 산업혁명과 보안 패러다임 변화. ICT신기술
[24] Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. International Journal of Production Research, 58(11), 3381-3398.
[25] 김철. (2015). 초등학생을 위한 알고리즘 교수 학습방법과 평가. 한국정보교육학회논문지, 19(4), 489-497.
[26] Hyundai motor company(2021). 2020년 개인정보 지키기 위한 인터넷 안전 습관 기르기. https://kids.hyundai.com/kidshyundai/
[27] Mordor Intelligence Pvt Ltd. (2021). City Surveillance Market - Growth, Trends. COVID-19 Impact and Forecasts (2021 - 2026)
[28] 김정선, 송태민. (2014). 빅데이터 기술수용의 초기 특성 연구: 기술이용자 및 기술활용자 측면의 조절효과를 중심으로. 한국콘텐츠학회논문지, 14(9), 538-555.
[29] 장현서, 송태환, 장성훈, 정유진, 박남제. (2018). 블록체인을 통한 포그 컴퓨팅 보안 해결방안, 교육적 제안. 한국정보과학회 학술발표논문집, 966-946.
[30] 김동칠, 박성주, 양창모. (2020). 지능형 영상보안시스템 기술 표준화 동향. 한국통신학회지(정보와통신), 37(8), 25-31.
[31] KT GiGAeyes. (2021). 스마트한 CCTV란?. https://raycat.net/4135
[32] 삼성SDS. (2021). 2021년 사이버보안 7대 트렌드. 삼성SDS Cyber Security Conference 2021

[33] 이글루 시큐리티. (2021). 보안정보 악성코드 분석 리포트, 2022년 보안 위협 기술 전망보고서, http://www.igloosec.co.kr/index.do
[34] 김동희. (2016). 융합시대의 사이버보안 거버넌스 구축방안에 관한 연구. 박사학위논문, 고려대학교
[35] 시큐리티월드(2021). 보안뉴스. 2021년 상반기 주요 보안위협 트렌드 5가지, https://www.boannews.com/media/view.asp?idx=99335
[36] 김지한. (2020). 샘플 데이터로 표현되는 사이버-물리 시스템의 취약점 분석 및 검출 불가능한 공격에 대한 방어 기법. 박사학위논문, 서울대학교.
[37] 윤상필. (2021). 보안취약점의 사회적 인식과 법·기술적 대응전략. 박사학위논문, 고려대학교.
[38] 박대우. (2013). IP-PBX에 대한 해킹공격과 포렌식 증거 추출. 한국정보통신학회논문지, 17(6), 1360-1364.
[39] 박기홍, 노시영. (2012). 클라우드 서비스에 대한 포렌식 측면의 수사 방법. 한국산업정보학회논문지, 17(1), 39-46.
[40] 박흠. (2009). 사이버 범죄 수사를 위한 사이버 포렌식 범주 온톨로지. 한국정보통신학회논문지, 13(8), 1687-1692.
[41] 김대욱. (2019). 컴퓨팅 사고력에 기초한 유아를 위한 언플러그드 코딩의 개념과 전략. 문화기술의 융합, 5(1), 297-303.
[42] 박민정, 이기혁, 채상미. (2021). 국내 정보보호 교육 표준 프레임워크 개발; 연령 및 직무 맞춤의 이원화(Two-track) 교육과정을 중심으로. 정보보호학회논문지, 31(5), 1083-1095.
[43] 곽지은. (2020). 마이스터·특성화 고등학교 보안 학과 교육 과정 분석 및 웹·네트워크 보안 공격 실습 교육용 소프트웨어의 설계. 석사학위논문, 이화여자대학교.
[44] 교육부(2015), 2015 개정 교육과정 별책, 총론 및 10실과(기술가정), 정보과 교육과정
[45] 유지연. (2021). 사이버보안 정규교육화를 위한 주요국 교육체계 비교분석 연구. The Journal of the Convergence on Culture Technology (JCCT), 7(1)
[46] CISA. (2021). K-12 Cybersecurity Learning Standards_1.0. cyber.org
[47] 성경모. (2014). 프랑스 ICT 산업의 인재혁신 동향: 민간 주도의 기수, ECOLE 42. 동향과 이슈, (9), 1-21.
[48] Lee, D. (2021). The Trends of Domestic and Overseas Cyber Security Training. Journal of the Korea Institute of Information and Communication Engineering, 25(6), 857-860.
[49] 우호성, 김자미, 이원규. (2017). 해외 고등정보 표준교육과정 기반의 국내 대학 교육과정 비교분석. 컴퓨터교육학회 논문지, 20(1), 27-38.

[50] 김자미, 이원규. (2014). 영국의 교육과정 개정으로 본 정보교과의 지식과 문제해결력에 대한 쟁점. 컴퓨터교육학회논문지, 17(3), 53-63.
[51] 조윤영, 정종필. (2016). 사이버안보 (cybersecurity) 를 위한 중국의 전략: 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로. 21세기정치학회보, 26(4), 151-177.
[52] 정재훈, 김선회, 남동수, 이태욱. (2012). 21 세기 학습 능력 신장을 위한 다학문적 맞춤형 교육과정 모형 연구. 한국컴퓨터정보학회논문지, 17(11), 197-206.
[53] 제주대학교. (2015). 2015 융합인재교육 STEAM 프로그램 '사이버보안전문가'. 제주대학교.
[54] 유상희. (2020). '학습목표에 대한 학생의 반응 중심 맞춤형 수업설계 모형' 탐색. 한국어문교육, (31), 37-76.
[55] 최은선, 정유진, 현도익, 주연수, 김미진, 박남제. (2021). 인공지능 기초 의사결정나무학습을 위한 창의적 교육 프로그램 개발. 제2회 한국 인공지능 학술대회, 111-112.
[56] Owens, L., Kadakia, C. (2020). Designing for Modern Learning: Beyond ADDIE and SAM. American Society for Training and Development.
[57] Ali, C. A., Acquah, S., Esia-Donkoh, K. A comparative study of SAM and ADDIE models in simulating STEM instruction.
[58] Jung, H., Kim, Y., Lee, H., Shin, Y. (2019). Advanced instructional design for successive E-learning: Based on the successive approximation model (SAM). International Journal on E-learning, 18(2), 191-204.
[59] 남기덕, 윤형섭. (2015). 게임 구성요소를 중심으로 한 게임 분석 방법에 대한 고찰. 한국게임학회논문지, 15(5), 19-28.
[60] 단효운, 임광혁, 김수균. (2014). 중국에서의 교육용 게임 분석. 한국콘텐츠학회 종합학술대회 논문집, 351-352.
[61] 임동성. (2015). 시나리오 기반 위협 탐지를 지원하는 확장된 통합로그 관리체계. 석사학위논문, 전남대학교.
[62] 김문선, 이만희. (2021). 사이버 공격 훈련 시나리오 표현을 위한 Stage 기반 플로우 그래프 모델 연구. 정보보호학회논문지, 31(5), 1021-1030.
[63] Hirsch, S., Burggraf, P., Daheim, C. (2013). Scenario planning with integrated quantification‐managing uncertainty in corporate strategy building. foresight.
[64] 김주영 (2005). 토론학습을 위한 블렌디드-러닝(Blended-Learning) 수업모형 개발 연구. 석사학위논문. 서울대학교 대학원.

[65] 정주영. (2008). 블렌디드-러닝(Blended-Learning) 전략을 활용한 토론학습이 중학교 사회과의 학업성취도와 학습흥미도에 미치는 효과. 석사학위논문. 고려대학교 교육대학원.
[66] 한국과학기술기획평가원(KISTEP). (2021). 미래유망기술 선정에 관한 연구 비대면사회의 미래유망기술, 기관-2020-015
[67] Kang, H. (2020). 국내 인증 기술 및 서비스 현황. Review of KIISC, 30(3), 31-36.
[68] 정보통신정책연구원. (2021). 최근 생체 인식 산업 동향과 시사점, 이슈 분석 188호
[69] 김희완, 신중원, 김동수. (2012). 온라인게임에서 개인정보보호 감리 모형. 디지털정책연구, 10(3), 23-37.
[70] 정유진, 김진수, 박남제. (2019). 초등학생 대상 블록체인 기술의 위변조 방지 핵심원리 이해와 교육방안 설계. 정보교육학회논문지, 23(6), 513-320.
[71] 보안뉴스. (2021). 사이버보안, 세계 경제를 위협하는 두 번째로 큰 위협 요소, https://www.boannews.com/media/view.asp?idx=94787
[72] 한동일. (2021). 실시간 얼굴검출 연구 동향. 기술동향칼럼, IDEC Newletter. 8-13
[73] Bledsoe, W. W. (1964). Facial recognition project report. Panoramic research inc.
[74] Yang, M. H., Kriegman, D. J., Ahuja, N. (2002). Detecting faces in images: A survey. IEEE Transactions on pattern analysis and machine intelligence, 24(1), 34-58.
[75] Dawoud, N. N., Samir, B. B., Janier, J. (2011). Fast template matching method based optimized sum of absolute difference algorithm for face localization. International Journal of Computer Applications, 18(8), 0975-8887.
[76] Doik Hyun, Eunsun Choi, Yujin Jung, Namje Park. (2021). Development and Effects of Intelligent CCTV Robot Education Program Applying the Rich Picture Teaching Method. International Journal of Pharmaceutical Research, 13(2), 936-943.
[77] 사이언스 타임즈. (2017). 디지털 포렌식, 안면인식 프로그램, Sciencetimes. https://www.sciencetimes.co.kr/news/
[78] 정유진, 김진수, 박남제. (2020). 리치픽처 기법을 적용한 지능형 CCTV 알고리즘 창의교육 프로그램 개발 및 효과. 한국융합학회논문지, 11(4), 125-131.
[79] 김경환, 신상우, 황영아, 문미경. (2020). 스마트글라스기반 안면인식을 통한 학생지도 MR시스템. 차세대융합기술학회논문지, 4(1), 86-93.
[80] 정유진, 박남제, 최근배. (2021). 포스트 코로나 시대의 메타버스 플랫폼과 교원 역량 강화. 2021 공학교육학술대회, 105-106.

[81] Eunsun Choi, Yujin Jung, Namje Park. (2021). Strategies to Teach Elementary School Students the Principles of Blockchain Technology by Implementing Gamification. Ilkogretim Online - Elementary Education Online, 20(3), 1205-1211.
[82] 이동혁, 김상춘, 박남제. (2020). 포스트코로나 시대의 언택트 교육 환경을 대비한 블록체인 기반의 온라인 학습 플랫폼. 한국정보기술학회논문지, 18(11), 109-121.
[83] 고대훈, 박남제. (2016). 게이미피케이션 메카니즘을 적용한 양자역학 원리를 배우는 STEAM 프로그램 개발. 정보교육학회논문지, 20(5), 507-518.
[84] 고영해, 박남제. (2014). 육각형 셀기반 모의해킹 활동을 통한 효과적인 정보보안 학습교구 개발. 한국정보과학회 학술발표논문집, 654-656.
[85] 팀벨, 이안 위튼, 마이크 펠로우스. (2015). CS UNPLUGGED 언플러그드 컴퓨팅. 2015 컴퓨터과학 언플러그드.
[86] 허영. (2019). 초등학교 언플러그드 코딩교육을 위한 프로그램 개발. 기초조형학연구, 20(1), 586-596.
[87] Livingston, S. A., Stoll, C. S. (1973). Simulation games :An introduction for the Social Studies teacher, Tress Press.
[88] 이명숙. (2020). 디지털 트랜스포메이션 시대의 언플러그드를 적용한 컴퓨팅 사고력에 대한 효과성 분석. 디지털융복합연구, 18(3), 35-42
[89] 장윤재, 김동형, 김한성, 이원규, 김현철. (2011). 정보보호 교육을 위한 언플러그드 활동의 개발 및 유용성 평가. 14(1), 55-67.
[90] 배은숙. (2020). 한국사 게이미피케이션을 위한 서양사 전략 게임 분석. 대구사학, 141, 199-330.
[91] 이성훈, 이경택. (2019). 드론 동작 원리 이해를 위한 수업용 교구 및 교수학습자료 개발. 한국기술교육학회지, 19(2), 94-117.
[92] 정유진, 박남제. (2021). 사이버 공격 및 방어 해킹 원리 언플러그드 학습교구 디자인. 한국정보기술학회논문지, 19(5), 111-119.
[93] Yujin Jung, Eunsun Choi, Namje Park. (2020). Development Gifted and Creative Education Training Model for School Leaders. The 16th Asia-Pacific Conference on Giftedness 2020. 247-250.
[94] Yujin Jung, Namje Park. (2020). Artificial Intelligence Learning Environment Education Model. Proceedings of International Conference on Innovation Convergence Technology(ICICT 2020), 57-59.
[95] 정유진, 최은선, 박남제. (2020). 3년간의 초·중등학교 관리자 창의교육 교원연수 프로그램 효과성에 관한 실증. 2020년도 한국멀티미디어학회 추계학술발표대회 논문집, 23(2), 19.

ABSTRACT

Development and Demonstration of Elementary School Information Security Core Principle Education based on Hybrid Blended Practice Model

Yujin Jung

Convergence Information Security
Graduate School, Jeju National University
Jeju, Korea

(Supervised by professor Yung-cheol Byun)
(Supervised by professor Namje Park)

The development of information systems is leading modern society to an era of digital transformation in conjunction with the advanced information and communications technology platform. Put differently, contemporary society is gradually transforming into an information society with cutting-edge content. As the value of information increases, so do hackers' techniques in taking advantage of unfair profits. However, education on information ethics and information protection that must be provided to people as members of the information society is still not sufficiently conducted.

In the atmosphere of social change, in the 2015 curriculum, information education was designated as an essential subject and revised to keep up with the social change.. Moreover, the importance of such curriculum is expected to gradually increase in order to cultivate talented people in accordance with the gradually developing future society. However, information education is

currently operated at the discretion of schools or teachers during creative experience activities. Furthermore, information security education is also limited to Netiquette-centered information ethics education because it is difficult for teachers to know what to teach students in order for them to practice information security due to the absence of regular subjects.

In particular, in the case of elementary school students, the Internet utilization rate is very high. Moreover, there is a dire need for information protection education as cybercrime against elementary school students increases rapidly. Furthermore, in the case of elementary school students with weak awareness of information protection or security, it is common to easily inform others of the information about themselves and the people around them, and use such information without any guilt. Therefore, it is a common opinion from a national point of view that education on information security is necessary to protect and prevent students from engaging in cybercrime.

In this situation, professional information education that delivers professional knowledge to elementary school students for information security education can cause learners to lower their learning achievement. Hence, this paper devised and applied for an easily accessible education program. In this paper, three educational programs were developed and demonstrated. The first is a teaching tool that can grasp the core principles of blockchain technology that applies gamification. This allows elementary school students to naturally learn the concept of information security while playing games in consideration of their understanding of information security education.

The second proposed educational program allows learners to naturally learn network hacking jargon and core technologies. This is done by devising attack and defense scenarios and experiencing hacking principles in board games, which are the main interests of many teenagers. In addition, this is a scenario-based education program that makes it easier for learners to access technical parts to cultivate their ability to protect information. Moreover, it

aims to strengthen the learners' computing and thinking skills by helping them understand the role of security equipment applicable to the network by configuring panels that act as security equipment applied in a network environment to perform attacks.

The third is one of the new technologies of the future and is an educational program that allows students to learn the facial recognition technology of intelligent CCTV, which is very familiar and widely-used to our society. In combination with cybersecurity forensics, it is designed to make it easier for students to access complex principles by using rich techniques that use pictures, sketches, symbols, signs, and icons to express hidden issues in complex situations as images.

For stable education for elementary school students, as mentioned above, instructors or field teachers should be educated to easily access the problematic principles and correct concepts of information security. To this end, the vision and goals of the school organization vary according to the perception and will of the school manager, which affects the educational culture of the entire school. As such, it is necessary to change the perception and develop the competency of the school manager first. This is because school managers exercise a wide range of powers that cover the curriculum component of the entire education, budget, and administrative support, which have a significant impact on the education implementation in the school environment. In this study, we designed the educational programs to easily identify, accurately recognize complex concepts, protect students' information, and further present directions to become information security experts. Although the educational program proposed in this paper may not reach the level of textbooks for information security education in schools, it is designed at the level of alternative curriculum. In addition, as mentioned earlier, this program was first conceived to strengthen the instructors' competence through school teacher and administrator training prior to field education for

elementary school students.

To analyze the effectiveness of the hacking principle education program, training sessions were planned for school principals . A total of 69 principals participated in three educational training sessions twice. As a result, high satisfaction of 4.87 was recorded, and the focus group discussion analysis results confirmed the requirement of hacking principle education in school. Furthermore, to analyze the effectiveness of the education program for learning facial recognition technology principle composed of three lessons, various teaching and learning materials were provided to field teachers as part of the training. A total of 46 teachers participated in this program. Through two training sessions and effectiveness analysis, meaningful results were obtained to upgrade future educational programs with various technical knowledge and attractive instructional design. Additionally, blockchain core principle education was designed to be used in online and offline class environments. Education was conducted for 303 elementary school students from 2nd to 6th grades nationwide. As a result of the corresponding sample t-test, there was a statistically significant increase in all items performed. The verification results, such as high satisfaction through various subjects of these three educational programs, show the possibility of future development of this study for easily conceiving the difficult technical principles of cybersecurity for elementary school students through various learning tools.

Keywords : Core principles of information security technology, convergence education, hacking principles learning, blockchain principles learning, facial recognition technology, cybersecurity.