JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 29 No. 4, pp. 73-82, April 2024
https://doi.org/10.9708/jksci.2024.29.04.073

A Study on Strategic Development Approaches for Cyber Seniors in the Information Security Industry

Seung Han Yoon*, Ah Reum Kang*

*Student, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea
*Professor, Dept. of Cyber Security, Pai Chai University, Daejeon, Korea

[Abstract]

In 2017, the United Nations reported that the population aged 60 and above was increasing more rapidly than all younger age groups worldwide, projecting that by 2050, the population aged 60 and above would constitute at least 25% of the global population, excluding Africa. The world is experiencing a decline in the rate of increase in the working-age population due to global aging, and the younger generation tends to avoid difficult and challenging occupations. Although theoretically, AI equipped with artificial intelligence can replace humans in all fields, in the realm of practical information security, human judgment and expertise are absolutely essential, especially in ethical considerations. Therefore, this paper proposes a method to retrain and reintegrate IT professionals aged 50 and above who are retiring or seeking career transitions, aiming to bring them back into the industry. For this research, surveys were conducted with 21 government/public agencies representing demand and 9 security monitoring companies representing supply. Survey results indicated that both demand (90%) and supply (78%) unanimously agreed on the absolute necessity of such measures. If the results of this research are applied in the field, it could lead to the strategic development of senior information security professionals, laying the foundation for a new market in the Korean information security industry amid the era of low birth rates and longevity.

▸ **Key words**: Population Decline, Cyber Seniors, AI, Information Security Industry, Security Control, On-tact Education and Training

• First Author: Seung Han Yoon, Corresponding Author: Ah Reum Kang
*Seung Han Yoon (nuricaps@naver.com), Dept. of Cyber Security, Pai Chai University
*Ah Reum Kang (armk@pcu.ac.kr), Dept. of Cyber Security, Pai Chai University
• Received: 2024. 02. 22, Revised: 2024. 04. 01, Accepted: 2024. 04. 17.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

[요 약]

2017년 UN에서는 전 세계적으로 60세 이상 인구는 모든 젊은 연령층보다 빠르게 증가하고 있으며, 2050년까지 60세 이상 인구는 아프리카를 제외한 전 세계 인구의 최소 25%를 구성할 것으로 예상하였다. 세계는 전반적으로 고령화로 인해 일을 할 수 있는 인구의 증가율이 감소하고 있으며, 청년층은 힘들고 어려운 직업을 선호하지 않고 있다. 이론적으로는 인공지능을 겸비한 AI가 모든 분야에서 사람을 대신할 수 있다고 하지만 윤리적인 판단 등 현실 세계의 정보보호 분야에서는 사람의 판단과 노하우가 절대적으로 필요하다. 이에, 본 논문에서는 IT 종사자 중 50대 이상 퇴직자 또는 전직을 희망하는 사람을 대상으로 재교육을 통해 현업으로 유입시키는 방법을 제안하고자 한다. 연구를 위해 수요 부분의 정부·공공기관 21곳과 공급 부분의 보안관제전문업체 9곳을 대상으로 설문하였으며 설문 결과 공급(78%)와 수요(90%) 모두가 절대적으로 필요하다는 데 의견을 모았다. 향후 이 연구 결과를 토대로 현장에 적용한다면 인구 저출산 100세 시대에 정보보호분야 시니어의 전략적 육성으로 대한민국 정보보호산업의 초석이 될 신규시장을 발굴할 수 있을 것이다.

▸ **주제어**: 인구감소, 사이버 시니어, AI, 정보보호산업, 보안관제, 온택트 교육훈련

I. Introduction

2021년 12월 기준 세계 인터넷 사용자 수는 약 70%인 4,901백만 명으로 20년 전 5억 6천만 명에서 폭발적인 증가세를 나타내고 있다[1]. Statista 통계 플랫폼에 따르면 전 세계 IoT 연결 장치는 2020년 97억 개에서 2030년에는 290억 개 이상으로 거의 3배 가까이 증가할 것으로 전망하고 있으며[2], Table 1. 의 2022년 Cybersecurity Ventures 보고서에 따르면 2030년까지 전 세계 사이버 범죄 피해액이 17.9조 달러에 달할 것으로 예측한다[3].

Table 1. Estimated Damage Cost of Cyber Attacks

Year	Estimated Annual Cost of Damage from Cyberattacks Worldwide (USD)	Year-On-Year Growth Rate
2024	$9.5 trillion	19.0%
2025	$10.5 trillion	10.5%
2026	$11.3 trillion	7.6%
2027	$12.4 trillion	9.7%
2028	$13.8 trillion	11.0%
2029	$15.6 trillion	13.0%
2030	$17.9 trillion	15.0%

통계청의 조사에 따르면 세계 인구는 2022년 79억 7천만 명에서 2070년 103억 명으로 증가 예측이며, 한국 인구는 2022년 5천2백만 명에서 2070년 3천8백만 명으로 감소할 것으로, 2072년 나이별 인구 구성비는 유소년인구(0~14세) 6.6%, 생산연령인구(15~64세) 45.8%, 고령인구(65세 이상) 47.7%로 예측하였다[4].

전 세계적으로는 2027년이면 사이버보안 인력 수요와 공급의 격차가 327만 명에 이를 것으로 예측하였고[5], 2022년 정보보호 인력 현황조사에 따르면 정보보호 인력 수는 138,568명으로 기업당 평균 2명인 것으로 조사 되었고, 2028년까지 매년 3,500~7,000명이 부족한 것으로 예측되었다[6].

또한 정보보안 기업의 73%, 인력의 67%가 서울에 편중되어 있으며 2020년 침해사고는 2018년 대비 1.5배 증가하였고 대부분 서울 외 지역에서 73%를 차지한 것으로 발표되었다[7].

2022년 공공기관 경영정보 공개 시스템인 알리오에 따르면 공공기관 370개 중 서울 등 수도권(서울, 경기, 인천)에 164(44.3%)개, 206(55.7%)개는 지방에 있다[8].

한국은 2003년 1.25 인터넷 대란으로 KISA에 인터넷 침해사고 대응 지원센터를 설립하였고 2008년 국방·외교·행정 등 10대 핵심 부문 보안관제센터 설립을 완료하고 2009년 대통령령으로 중앙행정기관 및 공공기관 보안관제센터 구축을 의무화하였으며, 2022년 국가 정보보호 백서에 따르면 전국 보안관제센터 수는 44개이며, 보안관제전문업체 수는 20개로 꾸준히 증가세를 나타내고 있다[9].

하지만, 사이버 침해 대응센터 운영 실태와 개선 과제 보고서에 따르면 관제(모니터링, 통제)요원의 교대근무 등의 힘든 작업 환경으로 이직률이 높아 책임성을 기대하기 어렵고 이상 이벤트가 급증하고 있으나 이를 분석할 전문 관제 인력이 부족하여 인공지능 관제시스템 등을 구축 또는 구축을 고려하고 있으나 예산과 분석 인력 확보의 어려

움이 있다고 조사 되었다[10].

결론적으로는 전 세계적으로 인구수 증가와 4차 산업혁명 등으로 IoT 연결 장치 수가 지속해서 증가함에 따른 사이버 범죄 피해액도 증가할 것이고 사이버보안 인력 수요와 공급 격차가 지속해서 심화할 것으로 예측되나, 국내 정보보호 인력수는 부족하고 대부분의 정보보안 기업 및 인력이 서울에 편중되어 있어 지방에 있는 보안관제센터에서의 전문 인력수급난이 심화하고 있다. 구체적으로 보안관제 전문기업은 관제 인력 확보의 어려움과 지방 파견 비용 부담에 비해 수익성이 낮으며, 관제 인력은 계약 등 고용 불안과 교대근무로 인한 보안관제 업무 기피, 낮은 임금을 그리고 보안관제 사업을 통해 관제 인력을 원하는 수요 기관은 예산 부족과 검증되지 않은 인력 투입과 투입된 인력의 잦은 교체 불만을 나타냈다.

이에, 본 연구에서는 설문을 통해 보안관제 전문 공급업체와 보안관제 수요 기관의 애로사항을 분석하여 시니어 대상 정보보호 전환교육 후 현장에 투입하는 등 해결 방안을 제시하고, 더 나아가 정부에서 사이버 시니어를 적극적으로 육성할 수 있도록 사이버 시니어의 전략적 교육훈련 프로그램을 제시하고자 한다.

연구의 흐름은 다음 Fig 1.과 같다.

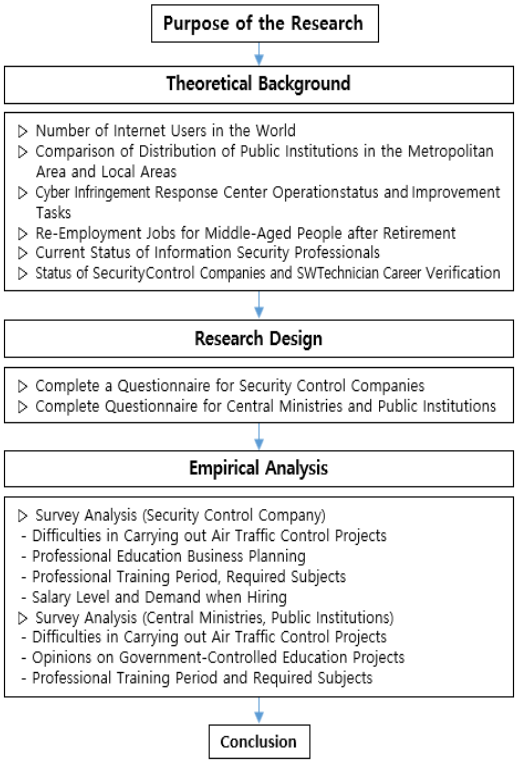

Fig. 1. Research Flow

II. Related Research

2.1 Concept of Old People and Seniors

노인은 일반적으로 64세 이상의 연령대를 가리키는 용어로 사용되며 생애의 다양한 단계를 거쳐 왔기 때문에 다양한 경험과 지식을 가지고 있다. 시니어(Senior)란 일반적으로 50세 이상의 계층을 통상적으로 뜻하며[11]. 영어권 국가에서는 시니어 시티즌(Senior Citizen)이라는 표현을 하여 은퇴한 노인 또는 연금을 받는 노인을 대신하고 있다.

2.2 Domestic Trends

한국은 노인들의 다양한 능력과 경험을 존중하고 활용하는 데 관심을 가지고 2004년부터 노인 일자리 사업을 시작했다. 노인 일자리 사업의 일자리 유형은 공공형(공익활동, 재능 나눔 활동), 사회 서비스형, 민간형(시장형 사업단, 취업 알선형, 시니어 인턴십, 고령자 친화 기업)으로 사회공헌 성격의 봉사와 생계를 위한 근로로 이루어져 있다.

한국은 2004년부터 노인 일자리 사업이 시작되었으나 사업이 시작되는 시점에서 노인 일자리의 개념, 일의 성격을 명확히 제시하지 않았고 지속해서 노인 일자리 사업이 확대되는 과정에서도 '일'이라는 개념 자체가 갖는 노동적 성격을 어떻게 규정할 것인가에 대한 방향성을 제시하지 못했고 여전히 그 개념은 불명확한 채로 남아 있다고 지적하였다[12].

한국은 저출산、고령화가 급속하게 진행되면서 경제 성장 동력이 약화하고, 개인에게는 평균수명 연장과 더불어 안정적인 노후 생활에 대한 우려가 커지고 있다.

중장년층 은퇴 후 재취업 및 일자리 만족도 결정요인에 대한 45세 이상 75세 이하, 총 429명을 대상으로 분석한 결과 재취업자는 가구원 수가 많고 은퇴 이전에 제조업에 종사하였거나 저숙련 일자리에서 종사한 경우가 많았고 남자가 여자보다 은퇴 후 재취업하는 경향을 보였으며 연령과 가구 총소득은 재취업에 부정적인 영향을 주는 것으로 나타났다[13].

고령자 재취업의 영향 요인에 관한 연구[14]. 에서는 재취업을 제약하는 영향 요인은 무엇인가를 검증하기 위해 전남지역 내의 광양시에 소재한 제조회사에 재취업한 55세 이상을 대상으로 재취업에 미치는 영향 요인을 설문하였는데 인구통계학적 요인으로 성별, 나이, 학력이 고령자의 재취업에 통계적인 유의성을 나타내지 않아 영향을 미치지 못했고, 인적 자본 요인에서는 직업훈련 도움 정도만 재취업에 영향을 미치는 것으로 나타났고, 건강 상태, 직업훈련 여부, 직업 훈련기간은 재취업에 영향을 미치지 못

하는 것으로 나타났다. 노동시장 분절 요인에서는 직급, 직장만족감, 급여 만족도의 3가지 변수만 재취업에 영향을 미쳤고 직업탐색 활동 요인에서는 구직횟수와 재취업의 목적이 고령자의 재취업에 영향을 미쳤다[15].

고령화사회의 노인 소득 보장 정책의 방향에 관한 연구에서는 은퇴 후 약 30년 이상을 노인으로 살아가야 하는 현실 속의 노인복지에 대한 노인 보건의료 문제나 노인 부양 문제뿐만 아니라 경제적으로 안정되고 행복한 노후 생활을 보내기 위해서는 공적 기금만으로 부족하므로 국가 차원의 정책 결정과 그에 따른 제도와 법률의 제정 및 정비가 필요하고, 노인에게 맞는 직종을 다변화해 노인 일자리 창출을 위한 다각적인 방안과 제도적 장치를 마련하는 등 노인 직업훈련기관을 설립하여 날로 변해가는 사회에서 최신의 정보와 전문지식을 습득하도록 교육훈련을 통하여 적성에 맞는 직종에 취업할 수 있도록 해야 한다고 하였다[16].

2005년부터 2019년까지 발행된 시니어 산업에 관한 499건의 신문 기사 분석을 중심으로 시니어 산업에 관한 동향 분석 연구에 따르면 시니어 산업에 관한 관심의 비중이 지속해서 증가하고 있고 시니어 산업에 대한 사회적인 인식 변화, 전문가 육성과 고령자들의 인력 활용이 필요하다는 것을 보여주고 있다. 연구를 통해 제시한 정책과제는 다음과 같다. 첫째, 시니어 산업의 사회적 인식 제고를 위한 산업 영역별 선도기업의 발굴과 육성이 필요하다. 둘째, 최근 4차 산업혁명의 시대에 접어든 시대적 분위기를 반영한 사이버 산업 관련 정책 및 제도 개선이 이루어질 필요가 있다. 셋째, 시니어 산업을 이끌어가는 기업체, 기관, 개인 등 개별적 산업 단위의 적극적인 마케팅활동이 이루어져야 한다. 마지막으로, 시니어 산업 분야의 전문인력을 양성하고, 고령자들의 숙련된 경험과 기술을 활용할 필요가 있다[17].

신 노년 고용 수요 및 욕구 설문조사에서는 수요처인 전국 5인 이상 기업체(500 표본) 대상 온라인 설문조사를 실시한 결과 60+고령자 고용 경험에 대해서는 71.2%가 현재 60세 이상 고령자 고용(계속 32.9%, 신규 15.7%, 둘 다 51.4%)한다고 답하였고 고용 이유로는 Fig. 2.와 같이 고령자의 기술지식 전수(A), 고령자 적합 업무(B), 인력난 해소(C), 우수한 업무태도(D), 낮은 이직률(E), 회사의 이윤 창출에 기여(F), 인건비 절감(G) 등이었다.

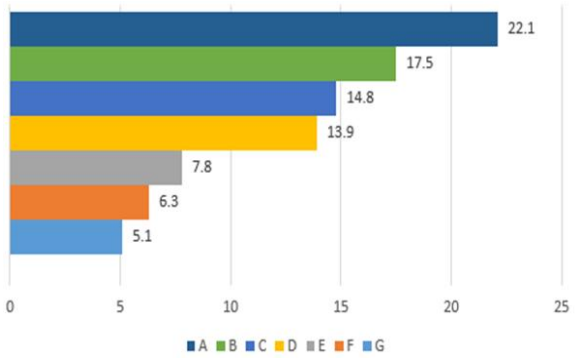

Fig. 2. Reasons for Employing Older Workers

고용 시 어려움에는 고령자 적합 직종(직무) 부족, 높은 산재 위험 등 작업 안전 문제, 고령 근로자 역량/자질 부족 등이었다. 고용 시 우선 고려 사항으로는 업무태도 및 경험, 직무 연관성으로 성별, 학력, 특히 나이에 대한 중요도는 상대적으로 떨어졌다. 고령자에게 원하는 역량으로는 의사소통 및 조직 이해(업무 이해, 의사 표현), 문제해결 및 대인관계(문제처리 능력, 팀워크 능력, 갈등관리) 등이며, 고령자 고용 관련 선호하는 정부 지원으로는 인건비/장려금 지원, 세제감면/지원, 사회보험료 감면/지원 등으로 조사되었다[18].

2.3 Overseas Trends

2015년 UN에서는 과거의 나이 기준을 100세 시대에 맞춰 재조정할 것으로 제안한 바 있다. 즉, 0~17세는 '미성년자', 18~65세는 '청년', 66~79세는 '중년', 80~99세 '노년', 100세 이후는 '장수 노인'으로 분류할 것을 제안하였다. 또한 2017년 UN에서는 전 세계적으로 60세 이상 인구는 모든 젊은 연령층보다 빠르게 증가하고 있으며, 2050년까지 60세 이상 인구는 아프리카를 제외한 전 세계 인구의 최소 25%를 구성할 것으로 예상하였다.

싱가포르는 2050년까지 인구의 38%가 60세 이상이 될 것이고 세계에서 세 번째로 높은 기대 수명을 갖게 될 것으로 예측하였고 물가 상승과 상대적인 사회 복지 부족으로 인해 공식 은퇴 연령(70세 이상)을 훨씬 넘어서 일해야 할 필요성이 대두되었다. 이를 위해 정부는 나이가 생산성의 걸림돌이라는 통념을 불식시키고 노인에 대한 가치관과 태도를 재정비하기 위해 대중의 경각심을 높여야 하고, 노년층에 대한 관행에 대해 고용주와 직원을 교육하고 노인에 대한 긍정적인 태도를 강화하기 위한 워크숍을 개최해야 하며, 고령 근로자가 모든 산업 분야의 기업이 활용해야 하는 엄청난 양의 지혜, 전문지식 및 경험을 제공한다는 점을 그리고 개인의 경우 노후에 재정적 안정을 유지

하기 위해 더 오래 일할 준비가 되어 이어야 하는데 “늙을 때까지 살고, 늙을 때까지 배운다”라는 중국 속담처럼 고령 근로자는 건강을 유지하고 고용할 수 있는 상태를 유지하기 위해 자신을 업그레이드하며 자신의 강점을 인식하고 최적화해야 하며 정부가 지식과 기술을 향상하기 위해 마련한 계획과 과정을 적극적으로 활용해야 한다고 하였다[19].

미국의 경우 약 29%인 900만 명이 은퇴 후 업무에 종사하는 것으로 조사되었다[20].

III. Strategic Training of Seniors in the Information Security Field

세계는 지속적인 고령화로 인해 일을 할 수 있는 사람이 계속 감소하고 있으며 청년층은 힘들고 어려운 직업을 선호하지 않고 있다. 전 세계적으로 ChatGPT 등 AI가 사람을 대신할 수 있다고 하지만 정보보호 분야에서는 사람의 판단과 노하우가 절대적으로 필요하다. 이에 IT 종사자 중 소프트웨어 초급기술 자격을 가진 50대 이상 퇴직자 또는 전직을 희망하는 사람을 대상으로 재교육을 통해 현업으로 유입시켜 인구 저출산 100세 시대에 정보보호 분야 시니어의 전략적 육성으로 정보보호산업의 인력난을 해소하기 위한 목적으로 본 연구는 시작되었으며, 이를 위해 수요 부분의 정부.공공기관 보안관제 담당자와 공급 부분의 보안관제전문업체[21]를 대상으로 설문하여 시니어가 필요한 영역과 교육 프로그램을 제안하였다.

또한, 정보보호 분야 시니어의 확산을 위해서 소프트웨어기술자에 해당하는 사람으로 50대 이상 퇴직자 또는 전직을 희망하는 사람에 대해 사이버 시니어의 용어를 정립하였다.

한국소프트웨어산업협회에 따르면 2020년 기준 국내 SW 기술자는 195,206명이고 사이버 시니어에 해당하는 50대 이상은 42,093명으로 전체의 22%에 해당하며 이는 고령화로 지속 증가할 것으로 예상된다[22].

3.1 Survey of Security Control Companies

정부는 2011년 7월 1일부터 국가 사이버안전 관리 규정 제10조의2에 따른 국가 공공기관 보안관제센터 운영을 지원할 보안관제 전문기업 20개 업체를 지정하고 있다. 본 논문을 작성하기 위해 한국정보보호산업협회(KISIA)를 통해 20개 업체에 이메일을 보내 설문조사를 실시하였고, 이 중 8개 업체는 오프라인에서도 설문조사를 병행하였다.

아래는 설문에 응답한 주요 보안관제 9개 기업(SK쉴더스, 이글루코퍼레이션, 안랩, 한국통신인터넷기술, 파이오링크, LG CNS, Cyber One, 씨엠티정보통신, 한전KDN)의 설문 내용을 분석한 결과이다.

주요 설문은 8문항으로 관제 사업 유형별(원격, 파견)비율, 관제 사업수행 시 애로사항, 사이버 시니어 대상 보안관제 전문교육 사업 기획, 사이버 시니어 대상 전문교육 기간, 전문교육 시 필수로 이수해야 하는 과목, 사이버 시니어 채용 시 급여 정도, 사이버 시니어 연간 예상 수요와 기타 의견이다.

설문 항목별 세부 응답 내용을 살펴보면 관제 사업 유형별 비율은 파견 관제 55%, 원격관제 45%로 보안관제 대상 기관에 사람을 보내서 관제하는 파견 관제가 18% 더 많다.

관제 사업수행 시 애로사항으로는 초급기술자 공급부족, 초급기술자 직무 변경 또는 이직, 보안관제를 중요업무로 보지 않는 인식에 문제가 있다고 78%가 응답하였고 발주기관 예산 부족도 67% 응답하였다.

사이버 시니어 대상 보안관제 전문교육 사업 기획 필요성에 대해서는 78%가 필요하다고 응답하였고 11%가 보통, 11%가 필요하지 않다고 응답하였다.

사이버 시니어 대상 전문교육을 2개월에 100시간 진행하면 부족하다 81%, 보통이다 6%, 적당하다 13%로 응답하였다.

전문교육 시 필수로 이수해야 하는 과목의 중요도를 묻는 말에는 이상 행위탐지 > 초동 대응 > 윤리교육 > 초동 분석 > 관제 보고서 작성 > 예방 활동 순으로 응답하였다.

사이버 시니어 채용 시 급여 정도를 묻는 말에는 업무 가능 역량에 따른 지급이 67%, 기술 인력의 자격 기준에 따른 변동이 22%, 무조건 초급기술자 수준 급여 11%로 응답하였다.

마지막으로 사이버 시니어 연간 채용 예상 수요로는 1명-5명이 67%, 10명 이상이 11%, 그 외는 응답하지 않았다.

기타 의견으로는 시니어의 체력 등을 고려할 때 현장대리인 또는 품질관리자 등 주간 업무를 제공하고 야간 근무가 필요한 경우에는 건강검진 등 사전 준비가 필요하다고 응답하였다. 또한 사이버 시니어 대상 전문교육 이외 주기적 보안교육과 정보보호 윤리교육 등 특히 사이버 시니어의 마음가짐 및 권위 의식 탈피 교육 등을 병행해야 함을 강조하였다. 공공기관 지방 이전에 따른 보안관제센터가 생겨나면서 수도권 외 지역에서 관련된 전문성을 가진 인력을 찾는 것에 매우 큰 어려움을 가지고 있는데 사이버 시니어 인력양성 프로그램이 활성화되어 관제 인력을 공

급하는데 조금이나마 해소될 수 있기를 바란다고 하였다. 또한 관제 업무 외 컨설팅 업무를 담당할 시니어 채용도 필요하다고 강조하였다. 반면에 부정적인 의견도 있었다. 본 프로그램이 정보보안 분야의 인력 수급 문제에 대한 대안으로는 효과적으로 판단 되나 시니어 채용에 대한 주변 환경 인식에 대한 개선이 필요하다고 하였고, 전문 인재가 부족하여 시니어까지 양성한다는 인식보다는 폭넓은 인재 범위 확장의 개념으로 인식이 되었으면 좋겠다는 의견이 있었다.

3.2 Survey on Security Control Project Ordering Organizations

보안관제사업 발주기관은 국가·공공기관 21곳을 대상으로 설문을 진행하였으며, 설문 응답 기관은 다음과 같다. 한국과학기술정보연구원, 공정거래위원회, 국민권익위원회, 국방과학연구소, 우정사업정보센터, 한국중부발전, 한국사회보장정보원, 한국산업기술보호협회, 한국전력거래소, 한국토지주택공사, 한전KPS, 경상남도교육청, 국가정보자원관리원, 국가철도공단, 국회도서관(서울), 국회도서관(부산), 산림청, 한국서부발전, 한국수자원공사, 한국조폐공사, 한국교통안전공단이다.

주요 설문은 6문항으로 관제 사업예산 및 투입 인력 수, 관제 사업수행 시 애로사항, 사이버 시니어 대상 보안관제 교육 사업에 대한 의견, 사이버 시니어 대상 전문교육 기간(2개월 100시간), 전문교육에 필수적으로 이수해야 하는 과목, 기타 의견이다.

관제 사업예산을 묻는 말에는 10억 이상이 62%, 10억 미만이 38%로 응답하였다.

관제 사업에 투입되는 인력은 5명 미만 10%, 10명 미만 43%, 15명 미만 19%, 20명 미만 24%, 20명 이상이 5%로 응답하였다.

관제 사업수행 시 애로사항으로는 초급관제요원의 빈번한 교체 67%, 투입된 초급관제요원의 역량 부족 62%, 사업예산 부족에 따른 인력 수급 문제 52%, 투입된 초급 관제요원의 인성 문제 10%로 응답하였다.

사이버 시니어 대상 보안관제 전문교육 사업에 관한 질문에는 매우 필요 57%, 조금 필요 33%, 보통 5%, 조금 불필요 5%로 응답하였다.

전문교육 진행 시 2개월(100시간) 집합교육이 적당한가의 질문에는 매우 적당 43%, 조금 적당 29%, 보통 14%, 조금 부족 5%, 매우 부족 10%로 응답하였다.

전문교육 진행 시 필수적으로 이수해야 하는 과목으로는 이상 행위 탐지(경보 확인 및 처리) > 초동 분석(정규표현식, 탐지규칙, 공격자 식별 등) > 초동대응(방화벽, 웹 방화벽 등 차단 중심) > 정보보호 윤리교육 > 관제 보고서 작성 > 예방 활동(외부기관 평가 항목 관리)순으로 응답하였다.

기타 의견으로는 기관의 정보시스템 이해와 업무 적응에 3개월 이상 소요되며, 기본적인 보안 업무를 위해 6개월 이상 소요되므로 잦은 인력 변동은 큰 애로사항으로 안정적인 인력공급과 시니어의 기술 노하우를 활용한다면 정말 많은 도움이 될 것으로 예상한다고 하였고, 기타 전문교육 선호 과목으로 보안관제 관련 법, 제도 및 가이드라인 교육이 필요하다고 하였고, 보안관제 인력 수급 부족의 주원인이 야간관제이므로 이를 우선하여 할당하는 것이 필요하며, 사이버 시니어 양성 프로그램은 현실적으로 아주 적절하다고 판단되며 신속하고 규모 있는 실행이 필요하다고 응답하였다.

고려 사항으로는 보안관제 사업 부서에서 시니어 관제요원 채용을 적극적으로 검토할 수 있도록 체계적인 지원 방안이 필요하다고 하였고, 사이버 시니어와 보안관제 업무 담당자(PM)간의 나이 차이로 인한 업무지시 등의 어려움과 사이버 시니어의 야간 보안관제 가능 여부 등이며, 보안관제가 중요한 업무임에도 불구하고 업계에서의 인식은 아무나 할 수 있는 높은 수준의 역량이 필요하지 않은 업무 등으로 인식되는 경향이 크며, 본 설문의 경우도 시니어가 최대 2개월의 교육만 받으면 관제 업무를 할 수 있다고 설계되어 있는데 관제 업무에 대한 전반적인 인식 개선과 업무에 대한 새로운 정의가 있을 때 전문인력 수급이 원활할 것으로 생각한다고 응답하였다. 사이버 시니어의 나이 기준을 분명히 설정하여야 하며, SW 초급기술자 기준으로 임금을 지급하기 위해서는 관계 법령의 정비와 기술자 등록 관리 절차가 마련되어야 하고, 50대 이상 퇴직자라도 사이버보안 전문가의 경우 별도 관리가 필요하다고 응답하였다.

향후 시니어 전문인력 양성 확대 측면에서 보안관제 이외에도 취약점 진단 등 수준 있는 교육이 필요하며, 수도권 등 대도시 이외의 지역에도 다양한 분야의 전문인력 양성이 필요하다고 응답하였다.

3.3 Professional Education Proposal for Cyber Seniors

정부, 공공기관, 출연연, 전력회사 등 21개 보안관제 발주기관으로부터 접수한 설문을 받은 결과, 기관별로 요구하는 교육 과목의 우선순위를 파악할 수 있었다. 다음과 같은 6개 과목을 기준으로 각 기관에서 우선순위를 선정하

여 사이버 시니어에게 필요한 과목을 구분하였다. ① 정보보호 윤리교육, ② 이상 행위 탐지(경보 확인 및 처리), ③ 초동대응(방화벽, 웹 방화벽 등 차단 중심), ④ 초동 분석(정규표현식, YARA, 공격자 식별 등), ⑤ 관제 보고서 작성, ⑥ 예방 활동(외부 기관 평가 항목 관리)

다음 표는 설문조사 결과 식별된 1순위-6순위의 과목 현황이다.

Table 2. Priority Survey Results by Subject

Subject	Score	Ranking	Ratio(%)
① Abnormal Activity Detection (Alarm Confirmation and Processing)	4.53	1	30
② Initial Analysis(Regular Expressions, YARA, Attacker Identification, Etc.)	4.42	2	25
③ Initial Response(Focused on Blocking Firewalls, Web Firewalls, Etc.)	4.25	3	20
④ Information Protection Ethics Training	3.20	4	15
⑤ Create Security Control Report	2.90	5	5
⑥ Prevention Activities (Management of External Agency Evaluation Items)	1.95	6	5

Table 2. 는 과목의 우선순위에 대해 1순위에 6점의 가중치를 부여하였으며 순위가 내려갈수록 1점씩을 감소하여 적용하였다. 그 결과 과목별로 산정한 점수를 반영하면 다음과 같은 순서로 순위를 매길 수 있다. ▶1위 ② 이상 행위 탐지(4.53), ▶2위 ④ 초동 분석(4.42), ▶3위 ③ 초동 대응(4.25), ▶4위 ① 정보보호 윤리교육(3.20), ▶5위 ⑤ 관제 보고서 작성(2.90), ▶6위 ⑥ 예방 활동(외부 기관 평가 항목 관리)(1.95)

보안관제 업무에 필요한 기술력을 갖추어야 하는 과목으로 예상할 수 있는 바와 같이 1위~3위 과목의 점수가 높게 나왔으며, 다른 과목에 비해 교육훈련의 비중을 높일 수 있도록 배치하는 것이 필요하다. 교육 과목의 비중을 다음과 같이 적용할 수 있으며, 이는 관제 수요 기관으로서 제시한 설문 데이터를 기반으로 차별화된 교육과정을 설계할 수 있다.

교육과정은 공통 과정, 실전형 훈련장 과정 연계, 프로젝트, 테스트의 과정으로 추진하며 각 과목에 대해 지식 습득 과정과 실전형 훈련장 과정으로 나누어 실시한다.

Table 3. Table 4.는 사이버 시니어의 보안관제 역량을 갖출 수 있도록 온라인과 오프라인(집체)을 포함한 교육훈련 과정(안)이며, 전체 교육 시간이 결정되면 과목별로 비중에 맞추어 차별화한 배정이 가능한 계획이다.

Table 3. Online and Offline Education and Training Courses

Division	Pro.	Detailed Subjects and Explanations	
on	C.M	• Online Training Course to Acquire Knowledge in 6 Subjects ① Abnormal Activity Detection (Alarm Confirmation and Processing) (15%) ② Initial Analysis (Regular Expressions, YARA, Attacker Identification, Etc.) (12%) ③ Initial Response (Focused on Blocking Firewalls, Web Firewalls, Etc.) (10%) ④ Information Protection Ethics Training (15%) ⑤ Preparation of Security Control Report (5%) ⑥ Prevention Activities (Management of External Agency Evaluation Items) (5%)	
	O.T	• Scenario-Based Training Course using GNS3	
		Common training	① Establishment of an On-Tact Training Environment
			② Establishment of Web Server, DNS Server/Sinkhole Establishment
			③ Firewall Construction, IDS (Snort) Installation, Web Firewall Installation
		Special training	① Attacks (Metasploit, Sliver, Koadic, Havoc C2)
			② Defense (Powershell, Detection /Blocking Rules (Snort, Yara))
	O.A	• Assess Trainee Competency for Individualized Training Through Online Testing Platform	
off	KISA	• This is a Practical Training Course to Respond to Cyber Threats to Perform Security Control Tasks and is Linked to Project Execution. It is a Practical Training Course Tailored to the Intermediate Level. ① Threat Event Identification/Initial Response/ Analysis/Response training ② Infringement Incident Investigation Training ③ CTF-Based Attack Defense Training ④ Real-Time Attack Defense Training	
	P.I	• Practical Training through Project Implementation through Group Formation to Handle Security Control Tasks	
	F.E	• An Exam will be Conducted at a Group Training Center Based on the Project Performance Results and the Content of the Remote Online Evaluation Previously Taken. • Cyber Senior Certificate is Issued to Trainees Who have Achieved the Minimum Score as a Result of the Test	

*C.M=Common Course, O.T=On Tact Training, O.A=Online Assessment, KISA=KISA Practical Training Center Linkage Course, P.I=Project Implementation, F.E=Final Evaluation

Table 4. Intermediate Level Practical Training Course

Practical Training to Respond to Cyber Threats	• Cyber Threat Response to Perform Security Control Tasks - Intermediate Level Practical Training Course Linked to Project Implementation ① Threat Event Identification/Initial Response/ Analysis/Response Training ② Infringement Incident Investigation Training ③ CTF-based Attack Defense Training ④ Real-Time Attack Defense Training
Project Implementation	• Practical Training through Group Project Performance
Collective Education and Training	• Conduct Offline Tests Based on Project Performance Results and Online Evaluation Contents

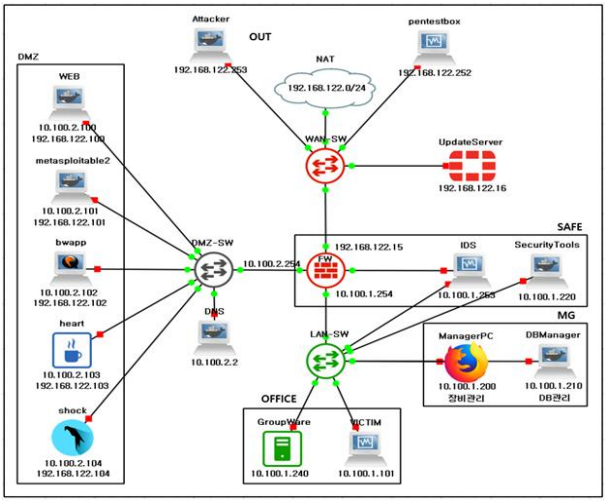

Fig. 3. Scenario-Based Training Course Using GNS3[1)]

사전적 의미의 온택트는 '온라인'과 '컨택트'의 합성어로 온라인에서 소통하거나 교류하는 것이다. 본 연구에서는 온라인 동영상 교육과 실습을 병행하는 것을 온택트 교육훈련으로 정의하였다.

Fig. 3.는 시나리오 기반의 온택트 교육훈련 토폴로지로 언제 어디서나 PC만 있으면 동영상 프로그램을 보고 자기주도형 교육훈련에 참여할 수 있다. 본 연구에서는 윈도우 10 OS 기반에 RAM 32GB, SSD(500GB)를 사용하였다. 온택트 사이버훈련장을 구축하기 위한 최소 사양으로는 윈도우 10 OS 기반에 RAM 16GB, SSD(200GB 여유공간)를 제안하고자 한다.

Table 5. List of Resources used to Build the Training Ground

No.	Classification	Image	Size	Hostname	Zone
1	Server	Docker	1.39GB	WEB	DMZ
2	Server	Docker	1.51GB	Metasploitable2	DMZ
3	Server	Docker	441MB	Bwapp	DMZ
4	Server	Docker	279MB	Heart	DMZ
5	Server	Docker Docker	389MB	Shock	DMZ
6	Server	Docker	1.39GB	DNS	DMZ
7	Server	Docker	672MB	ManagerPC	MG
8	Server	Docker	56MB	DBManager	MG
9	Server	Docker	449MB	GroupWare	OFFICE
10	Server	Virtualization	36.6GB	VICTIM	OFFICE
11	Server	Docker	672MB	UpdateServer	OUT
12	Server	Docker	2.53GB	Attacker	OUT
13	Server	Virtualization	20.8GB	Pentestbox	OUT
14	Server	Docker	2.53GB	SecurityTools	OUT
15	IDS	Docker	1.39GB	Snort2.9.7.0	SAFE
16	Firewall	Virtualization	2.42GB	Pfsense 2.7.2	SAFE
17	Web Firewall	-	-	Modusecurity 3.0.12	-

Table 5. 는 온택트 사이버훈련장 구축에 사용된 리소스이다. 오픈소스 기반의 무료 리소스를 사용하였으며 윈도우의 경우 1시간 제한이 있는 실험용 이미지를 활용하였다.

교육생이 직접 온택트 훈련 환경을 구성하고 웹서버 및 DNS 서버/DNS 싱크홀을 직접 구축해 봄으로써 원리를 이해할 수 있으며, 오픈소스 기반의 방화벽과 IDS 그리고 웹 방화벽을 설치하여 보안장비의 동작 원리 숙지와 공격에 대한 탐지 및 차단 정책을 만들어 직접 차단을 수행함으로써 정보보호 역량을 강화할 수 있다.

또한, 해커들이 사용하는 도구로 공격 기법을 학습하고 탐지/차단규칙을 생성하여 방어함으로써 해커의 우회 기법 차단 및 검증되지 않은 정책을 실제 운영 서버에 적용함에 따른 위험성을 감소시킬 수 있게 된다.

IV. Conclusions

한국인터넷진흥원에 따르면 2023년 국내 침해사고 신고 건수는 1,277건으로 전년 대비 12% 증가하였다. 공격 유형별 침해사고 신고 통계를 살펴보면 DDoS 공격이 전년 대비 약 2배로 증가하였으며, 서버 해킹(45.7%), 악성코드 감염(23.5%) 순이다.

1) GNS (Graphical Network Simulator)3 is a network software emulator released in 2008. It allows a combination of virtual and real devices and is used for the purpose of simulating complex networks.

6월부터 8월까지 솔루션 개발 업체의 중앙 업데이트 서버를 장악하여 고객사 솔루션 서버를 대상으로 악성 파일을 유포하는 형태의 공급망 공격이 확인되었다.[23]

이처럼 코로나-19 종식 이후에도 원격작업, 화상회의, 클라우드 보급이 지속해서 유지됨에 따라 사이버 범죄는 끊임없이 증가하는 등 사회적 문제로 이어지고 있다.

최근 해커 동향을 살펴보면 랜섬웨어로 수익을 올리고 그 수익으로 사회공학 기법을 발전시키거나 정보 유출 등 고급 해킹 기법 연구에 투자하고 있으나 24시간 365일 주·야로 근무하는 보안관제 담당자들은 자리를 비울 수 없어 교육훈련 참여 기회가 다른 직무에 비해 매우 적고 지방일수록 더 심하다.

본 연구에서는 이러한 사회적 문제해결 필요성을 인지하여 사이버 시니어를 활용한 보안관제 전문기업 및 수요기관의 어려움을 대처할 수 있는 대응 방안으로 사이버 시니어의 전략적 교육훈련 프로그램을 제안하였다. 본 연구의 참고자료에서는 고령화에 따른 시니어를 적극적으로 육성해야 하고 보안관제 분야의 인력난이 심화되고 있어 해결방법이 필요하다고만 하였으나, 본 연구에서는 수요자와 공급자의 설문조사를 근거로 전문적인 쿼리큘럼을 제안하였고 언제 어디서나 사용할 수 있는 온택트 사이버훈련장 이라는 효율적인 방안을 제시하였다.

향후 본 연구에서 제안된 사이버 시니어의 전략적 교육훈련 프로그램을 수정·보완하고 실제 사이버 시니어 교육훈련에 적용한 후 효과에 대해 분석할 필요가 있다.

더불어 실전과 같은 훈련으로 사이버 침해사고를 줄일 수 있는 효과적인 시나리오 기반의 교육훈련 콘텐츠에 관한 연구가 지속해서 이루어져야 할 것이다.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2020R1I1A1A01061146).

REFERENCES

[1] Korea Internet Companies Association (2023), “2022 Internet Industry Regulation White Paper”, pp. 51-52, 2023.

[2] “Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2021, with Forecasts from 2022 to 2030”, Statista, 2023, *https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide*

[3] Cybercrime Magazine, “Mastercard On Fighting Cybercrime And Mastering Cybersecurity”, 2022., *https://cybersecurityventures.com/mastercard-on-fighting-cybercrime-and-mastering-cybersecurity*

[4] Statistics Korea, “Future Population Projections: 2020-2072”, press release, pp. 4, 2021.

[5] Go-Eun Yoon, “China will have a Shortage of 3.27 Million Cybersecurity Talents by 2027”, *https://www.yna.co.kr/view/AKR20220908170700074*

[6] Cyber Security Talent Center, “2022 Information Security Manpower Status Survey”, KISA, Dec. 2022.

[7] Min-Kwon Gil, “73% of Information Security Companies, 67% of Manpower Concentrated in Seoul… Nurturing of Local Information Security Industry in Full Swing”, *https://www.dailysecu.com/news/articleView.html?idxno=143973*

[8] Sang-don Park, “Relocation to Regional Areas was Promoted for Balanced Development, but… 44% of Public Institutions are still in the Metropolitan Area”, *https://www.yna.co.kr/view/AKR20220522057600003*

[9] Joint Korea Communications Commission, Ministry of Public Administration and Security, and Ministry of Knowledge Economy, “2009 National Information Protection White Paper”, pp. 21, Apr. 2009.

[10] Jeong-Min Choi, “Cyber Intrusion Response Center Operation Status and Improvement Tasks”, National Assembly Research Service, pp. 37-40, Dec. 2021.

[11] Sang-Ran Seo, “A formative Semiotic Study on the Signification of Active Seniors’ Credit Card Design”, Korea Design Trends Society, Vol. 42, pp. 123, 2014. DOI : 10.21326/ksdt.2014..42.011

[12] Ki-Hoon Park, “Utilization of the Labor Ability of the Elderly after Retirement - Focusing on Senior Job Creation Projects in Korea and Japan, Silver Talent Center”, Korean Society of Japanese Language and Literature, pp. 297-300, [Co-hosted by 4 Academic Societies], Apr. 2021.

[13] Kwon-hee Kwon, “Study on the Determinants of Re-employment and Job Satisfaction after Retirement among Middle-aged People”, Korea University of Technology and Education Techno Human Resources Development Graduate School, Korean Summary, 2022. UCI: I804:44013-200000607775

[14] Myung-Ho Seo, “Study on the Influencing Factors of Re-employment of the Elderly: Focusing on Elderly Re-employment in the Jeollanam-do Region”, pp. 130-132, 2019.

[15] Hyun-seok Oh, Sang-hoon Pyeon, “Study on the influencing factors of re-employment of the elderly”, Social Convergence Research, Vol. 5, No. 3, pp. 13-28, Daegu Science University

Defense and Security Research Institute, 2021. DOI : 10.37181/JSCS.2021.5.3.013

[16] Jin-Tae Choi, Hyo-Jin Kim, Myeong-Jun Kim, “Direction of Senior Citizen income Security Policy in an Aging Society,” Korean Society for Local Autonomy, Vol. 23, No. 4, pp. 97-113, 2022.

[17] Soo-hyung Kim, Hyeong-Soo Kim, “Trend analysis on the Senior Industry: Focusing on Analysis of Newspaper Articles”, Korean Association of Senior-Friendly Industries, 13th No. 1, pp. 13-27, 2021. DOI : 10.34264 /jkafa.2021.13.1.13

[18] Su-Rin Kim, “Study on Plans to Revamp the Elderly Job Project for the New Elderly Generation”, pp. 159-165, Korea Labor Force Development Institute for the Aged, 2020.

[19] Jonathan Tan, Embracing "The Silver TSUNAMI"-Future of Mature of Mature Working Adults”, Singapore Management University, Jun. 2016.

[20] Lisa Greenwald, Craig Copeland, Jack VanDerhei, “The 2017 Retirement Confidence Survey: Many Workers Lack Retirement Confidence and Feel Stressed About Retirement Preparations”, EBRI issue brief. pp. 1-29, 2017. PMID: 29215235

[21] Information Security Industry Promotion Portal - Security control company, *https://www.ksecurity.or.kr/kisis/subIndex/470.do*

[22] SW Technician Career Confirmation Status Standard (2020), Korea Software Industry Association, *https://www.sw.or.kr/site/sw/17/1170602000000202020072202.jsp*

[23] Korea Internet & Security Agency, “Cyber Threat Trend Report for the Second Half of 2023”, Jan. 2024.

Authors

Seung Han Yoon obtained a bachelor's degree in Information Security through the Korean Academic Credit Bank System in 2022. His major experiences include serving as the head of the integrated security control team at the Gyeongsangnam-do Office of Education (from 2012 to 2016), Director of the Cyber Safety Center at Korea Midland Power and Korea Land & Housing Corporation (from 2016 to 2019), Information Security Team Leader at the Korea Forest Welfare Agency (from 2019 to 2020), and Director of the Cyber Security Talent Center at the Korea Internet & Security Agency (from 2021 to 2022). Currently, he works as the head of the technology infringement analysis team at the Defense Agency for Technology and Quality.

Ah Reum Kang received the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2012 and 2016. She is a professor in the Department of Information Security at Pai Chai University in Daejeon, South Korea. Her current research interests include security, artificial intelligence, malware, medical data analysis, and online game security.