심층분석

주요국 사이버보안 인력양성 정책 분석

최근 세계 각지에서 대규모 데이터 유출 사고 등 사이버공격이 잇따라 발발하면서, 관련 업계의 사이버보안 전문인력 수요가 급증하는 추세다. 이에 따라 각국 정부 역시 사이버보안 인력양성을 통한 수요 안정화를 위해 다양한 정책적 시도에 나서고 있는 분위기다.

목차

1. 사이버보안 인력양성의 필요성
2. 국내 사이버보안 인력양성 현황
3. 주요국 사이버보안 인력양성 현황
4. 결론 및 시사점

주요국 사이버보안 인력 양성 정책 분석

1. 사이버보안 인력양성의 필요성

■ 최근 전 세계적으로 사이버보안에 대한 각계각층의 관심이 크게 증가하고 있으나, 사이버보안 업무를 효과적으로 수행할 전문인력이 부족한 실정

- 글로벌 IT 벤더 시스코(Cisco)의 2014년 연례 보안 리포트(Annual Security Report)에 따르면, 최근 수 년 간 모바일과 클라우드 기술이 급격히 성장했음에도 불구하고, 그에 상응하는 전문 보안 시스템이 부족해 사이버범죄 피해가 급증한 것으로 파악
- 시스코는 특히 사이버보안 전문인력이 전 세계적으로 100만 명 이상 부족하다며, 이로 인해 단순 피싱 공격에서부터 특정 대상을 직접 겨냥한 대규모 사이버공격에 이르기까지 다양한 위협에 노출될 것이라고 경고

■ 보안 업계에서는 더욱 고도화된 사이버 위협에 대응하기 위해 단편적인 보안 기술 및 솔루션보다는 사람에 투자해야 할 시기라는 의견이 확산

- 2014년 2월 개최된 글로벌 보안 컨퍼런스 'RSA Conference 2014'에서는 갈수록 지능화되는 사이버공격에 대해 보안 솔루션 제품 개발을 통한 1:1식 대응만으로는 한계가 있다는 주장 제기
- HP의 기업 보안 제품 담당자 아트 길리랜드(Art Gilliland) 부사장은 모든 위협으로부터 기업을 방어할 보안 솔루션은 존재하지 않으며, 기업들이 보다 효과적인 보안 대책을 마련하기 위해서는 포괄적인 보안 프로그램을 구성할 인력과 관련 보안 프로세스에 더 많은 투자를 기울여야 한다고 조언
- 이를 위해서는 보안 관련 업무를 전담할 인력양성 및 교육에 투자하는 것이 보다 효과적이라는 지적

■ 이처럼 업계 내의 사이버보안 인력난이 심화됨에 따라, 국가 차원의 사이버보안 인력 확충을 위한 정책적 필요성이 대두되는 상황

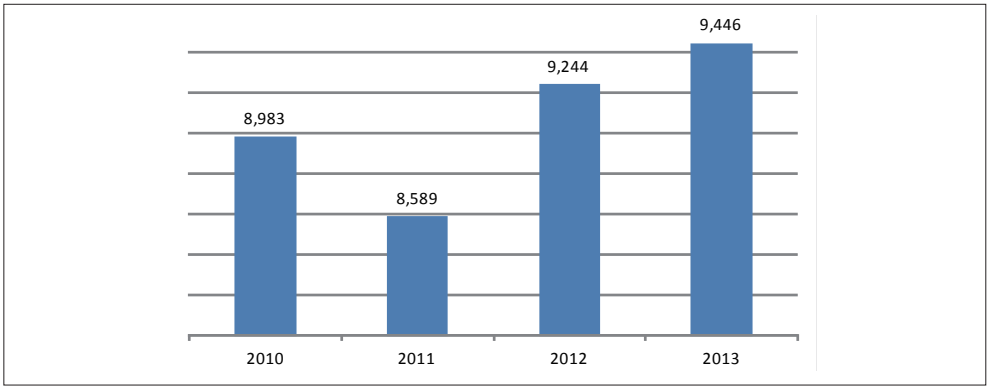
- 각국 정부는 사이버보안 강화 정책 수립에 있어 사이버보안에 대한 업계의 경각심을 높이고 실질적인 보안 업무를 책임질 수 있는 전문인력의 중요성을 인식하고 있는 것으로 파악

- 일례로 미국에서는 오바마(Barack Obama) 대통령의 사이버보안 강화 행정명령의 일환으로 마련된 주요 기반시설의 사이버보안 프레임워크 표준안이 인력양성 측면에서는 구체적인 방안을 제시하지 못하고 있다는 비판에 직면
- 사이버보안 인력양성 관련 정부의 정책 방향은 사이버보안 교육 전담기관 설립, 무상 교육 프로그램 제공 및 사이버보안 세미나 등 학술행사 개최, 사이버보안 직업군의 체계화를 통한 업계의 효과적인 인력 수급 환경 지원 등으로 구분

■ **한편, 지식정보보안산업협회[1] 의 2013년 국내 지식정보보호산업 실태조사에 따르면, 2013년 정보보안 업체의 신규 채용 계획은 1,598명으로 나타났으며, 이는 2012년 실태조사 당시 추정치인 1,074명을 상회해 최근 업계의 인력 수요가 증가하고 있음을 나타냄**

- 정보보안(사이버보안)과 물리보안을 포함한 국내 정보보호산업 인력 수는 2013년 기준 34,707명이며, 이 중 정보보안 인력은 27.2%인 9,446명 수준
- 정보보안 인력은 2010년 8,983명에서 2011년 8,589명으로 년 다소 감소했다가 2012년부터 다시 증가세로 돌아섰으며, 보안 전문인력에 대한 높은 수요를 감안할 때 향후 지속적으로 증가할 전망

● **국내 정보보안(사이버보안) 인력 현황 (2010~2013)**



출처 : 지식정보보안산업협회

- 그러나 2013년 기준 정보보안 인력 수준별 분포는 특급 인력의 비중이 가장 낮고 초급이 가장 높아 전문성 있는 인재 부족 문제를 유발하는 실정

1) Korea Information Security Industry Association

2. 국내 사이버보안 인력양성 현황

■ **최근 국내에서는 금융기관 등 민간기업을 겨냥한 개인정보 해킹, 정부기관 사이트를 목표로 한 DDoS 공격 등 공공 및 민간 영역에서 잇따라 사이버 공격 사고가 발생함에 따라 사이버보안에 대한 경각심이 급증**

- 공공 부문에서는 정부기관 사이트를 겨냥한 2009년 7월 7일 DDoS 공격, 정전 60주년에 국가 주요시설 및 언론사 홈페이지를 마비시킨 2013년 6월 25일 해킹 테러 등이 대표적
- 민간 기업을 대상으로는 주로 금융기관과 인터넷 사업자를 겨냥해 개인정보 등 민감한 데이터를 유출하려는 해킹 피해가 잇따르고 있으며, 특히 금융기관에 대한 사이버 공격은 실제 개인에게 경제적 피해로 이어지며 사회적 문제로 대두

■ **한국 정부는 미래 창조경제산업에서 정보보호산업이 지닌 중요성에 주목하고, 정보보호산업 발전 종합대책 수립을 통해 시장 확대, 기술력 강화, 전문인력양성 등 전략 방향을 제시('13.7)**

- 정보보호 전문인력양성 측면에서는 업계의 높은 인력 수요를 충족시키고 새로운 창조시장을 선도할 인재를 만들기 위한 체계적인 인력양성 계획을 제시하고, 2017년까지 최정예 정보보호 전문인력을 5,000명 양성할 목표를 설정
- 초 · 중 · 고 정보보호 영재 발굴, 정보보호 관련 학과 및 대학원 연구 지원 및 전문교육과정 지원 확대를 통해 석 · 박사급 인력을 확보하고, 우수 인재를 위한 특별 교육 프로그램, 기업 대상의 정보보호 최고위과정 및 분야별 보안담당자 교육 등 실제 업계 수요를 반영한 전문인력양성책을 도모
- 정보보호 인력의 체계적인 관리를 위한 정보보호 인력 통합관리 지원 시스템 구축 및 인력의 전문성 확보를 위한 국가기술 자격제도 확대 등 체계적인 인력 공급체계도 구축할 계획

■ **정부는 또한 최근 급증한 사이버 공격에 적극적으로 대응하기 위해 산업 지원책과는 별도로 범국가 차원의 사이버위협 대응을 위한 국가 사이버안보 종합대책을 발표('13.7)**

- 청와대 중심의 사이버안보 컨트롤타워 구축, 기관간 스마트 협력체계 구축을 통한 정보공유 활성화, 사이버 보호의 견고성 보강을 위한 정보통신 기반시설 확대 및 운영 체계 개선, 사이버안보 창조적 기반 조성을 위한 최정예 정보보호 전문가 양성 프로그램 확대 등의 4대 전략을 수립

- 정보보호 전문가 양성 계획은 앞서 언급된 정보보호산업 발전 종합대책과 연계해 전문가 양성사업 확대, 영재교육원 설립, 정보보호 핵심기술 분야 선정[2] 및 연구개발 지원 등의 프로그램을 추진할 계획

■ **이에 따라 공공 및 민간 영역을 막론하고 전문 기술을 갖춘 사이버보안 인력 수요가 크게 증가하면서, 정부기관 및 학교, 민간 부문에 걸쳐 사이버보안 전문가 양성에 역량을 집중하는 추세**

- 공공 부문에서는 공무원들의 사이버보안 의식을 고취시키고 전담조직 및 인력 전문성 강화를 위한 교육 프로그램을 제공
- 대학 등 상위 교육기관에서는 사이버보안 관련 학과를 개설하고 젊은 인재들이 사이버보안 전문가로 성장할 수 있는 학문적 발판을 마련
- 민간 부문은 산업계의 사이버보안 관련 수요를 고려한 실무 중심의 인력양성이 활성화되고 있으며, 정부기관의 사이버보안 전문가 양성 프로그램을 비롯해 민간 교육기관의 사이버보안 교육 서비스 등이 확산 중

■ **공공 부문의 사이버보안 인력양성은 안전행정부를 중심으로 공무원 대상의 체계적이고 지속적인 사이버보안 교육 프로세스 구축을 도모**

- 안전행정부가 운영하는 중앙공무원교육원은 정보보호 관련 기본 실무를 포함해 보안관제 실무, 해킹 대응, 사례 중심의 대응 방안 교육, 사이버 대응체제 구축, 사고 분석 및 대응 등의 교육과정을 포함
- 또한, 국가보안기술연구소는 2011년 8월 정부가 발표한 '국가 사이버안보 마스터플랜'의 일환으로 2012년 7월 국가정보보안교육원을 설립하고, 사이버안보 정책 과정, 보안담당자 실무 과정, 각 부처별 보안 현안 문제 해결을 위한 사이버 전문가 교육과정 등을 운영 중

■ **민간 분야에서는 한국인터넷진흥원이 사이버보안 분야의 고급인력양성을 위한 정책 전개**

- 특히 일반인의 정보보호 인식 제고 및 수강자의 분야와 수준에 맞는 다양한 교육 프로그램 제공을 목적으로 KISA 아카데미를 운영 중이며, 온라인 웹사이트에 통합교육관리시스템을 구축하고 연간 교육 커리큘럼을 개설해 신청자를 모집하는 방식으로 교육 서비스를 제공
- KISA 아카데미는 2014년 기준으로 디지털 포렌식, 보안 컨설턴트, 보안관제, 금융보안, 시큐어 코딩 등의 교육 프로그램을 제공

2) 정부는 10대 정보보호 핵심기술 개발 분야로 암호·인증·인식·감시·탐지 등 5대 정보보호 기반 분야 및 스마트폰·사물인터넷·클라우드·지능형교통시스템·사회기반 등 5대 신성장 분야를 제시

- KISA 아카데미의 대표적인 인력양성 프로그램으로는 최정예 사이버보안 인력(K-Shield) 인증 교육이 있으며, 고급 사이버보안 교육과정을 이수한 인재들은 최정예 사이버보안 인력 인증을 받아 공인 사이버보안 전문가로서 업무 수행이 가능
- 이 외에 한국인터넷진흥원은 지식정보보안 재직자 교육, 대학정보보호동아리 지원, 고용계약형 석사과정, 정보보호관리체계[3] 교육, 정보보호기술 온라인 학습장 운영 등을 추진 중

■ **민간 기업에서는 사이버보안 전문인력에 대한 높은 수요에 힘입어 다양한 형태의 교육 사업이 전개되고 있으며, 대부분 취업 등을 대비한 실무 중심의 교육이 이뤄지는 양상**

- 민간 사이버보안 전문기업 및 IT 교육기관에서 잇따라 정보보호 관련 교육 서비스를 제공하고 있으며, 주로 각종 정보보호 전문 자격증 관련 교육이 활성화된 상태[4]
- 지식경제부, 한국인터넷진흥원, 한국정보통신자격협회, 한국해킹보안협회 등에서 운영 중인 다양한 자격증 제도는 민간 영역에서 개인의 사이버보안 역량을 판단할 수 있는 기준으로 자리매김

■ **대학교의 정보보호 관련 학과는 구 정보통신부의 IT 인력양성 사업 지원으로 2002년부터 개설되기 시작했으며, 2012년 현재 정보보호학과, 융합보안학과, 컴퓨터정보전학과, 사이버보안학과, 사이버경찰학과 등 27개 학과가 분포**

- 국방부와 고려대학교는 졸업 후 장교로 임관해 일정 기간 동안 사이버사령부 등에서 사이버국방을 위해 일하는 채용조건형 계약학과인 사이버국방학과를 신설
- 한편, 한국인터넷진흥원은 사이버보안에 관심을 갖는 대학생들에게 올바른 정보보호 윤리관과 보안 관련 실무 경험을 제공하기 위해 대학 정보보호 동아리 지원 사업을 시행 중이며, 2012년 기준 총 37개 대학교의 40개 동아리를 선정해 연구활동, 정보보호 세미나, 실습교육 등을 지원

■ **이 외에 방송통신위원회와 한국인터넷진흥원은 초 · 중 · 고 및 일반인을 대상으로 사이버보안 윤리 의식 개선을 위한 교육 프로그램을 전개하고 있으며, 교육과학기술부는 사이버 침해 대응과 개인정보보호 교육을 목표로 정보보호교육 지역센터를 지정해 운영 중**

3) Information Security Management System(ISMS), ISO27001 표준에 따라 정보통신 네트워크의 안전성을 위해 운영되는 기술적 · 물리적 보호조치 등 종합적인 관리체계에 대한 인증 제도

4) 국내에는 지식경제부의 정보보안기사, 한국인터넷진흥원의 정보보호전문가, 한국정보통신자격협회의 인터넷보안전문가, 한국해킹보안협회의 해킹보안전문가 등의 자격증 제도가 운영되고 있으며, 해외에서도 인정을 받는 국제 자격증으로는 정보시스템전문가(Certified Information Systems Security Professional, CISSP), 정보보호관리자(Certified Information Security Manager, CISM) 등이 존재

3. 주요국 사이버보안 인력양성 현황

3.1. 미국 : 사이버보안 인력 프레임워크

■ 미국 정부는 2010년 4월 국가 사이버보안 교육 이니셔티브(National Initiative for Cybersecurity Education, NICE)를 발족하며 본격적으로 국가 차원의 사이버보안 인력양성을 도모

- NICE는 기존 사이버보안 강화 정책인 포괄적 국가 사이버보안 이니셔티브(Comprehensive National Cybersecurity Initiative) 중 인력양성 부분을 분리시켜 역량을 더욱 집중하기 위한 것
- 오바마(Barack Obama) 대통령의 사이버 중점 정책 추진 방침과 더불어 백악관 국가안보위[5] 의 사이버보안 이사회[6] , 국가정보장실[7] 의 합동유관기관 사이버 태스크포스[8] 의 결정에 따라 국립표준기술연구소[9] 가 NICE의 전반적인 정책 관리 역할을 수행
- NICE는 4가지 정책 방향으로 ▲국가 사이버보안 인식 제고[10] ▲교육기관의 사이버보안 교육 도입[11] ▲연방 사이버보안 인력 구조 구축[12] ▲사이버보안 인력 훈련 및 전문화[13] 등을 제시

■ NICE의 정책 방향 중 연방 사이버보안 인력 구조 구축은 2011년 국립표준기술연구소가 발표한 사이버보안 인력 프레임워크 (Cybersecurity Workforce Framework)로 더욱 체계화

- 사이버보안과 관련된 업무 및 전문기술을 카테고리별로 분류하고 특정 업무마다 개인에게 요구되는 역량을 세밀히 분석함으로써, 적재적소에 필요한 인재를 체계적으로 양성하는 것이 목적
- 보안 역량에만 초점을 맞추기보다 시스템 관리 및 운영, 데이터 분석 등 사이버 영역 전반을 포괄하는 범위에서 사이버보안 인력양성을 다루려기 위함

5) National Security Council
6) Cybersecurity Diretorate
7) Office of the Derector of National Intelligence
8) Joint Interagency Cyber Task Force
9) National Institute of Standards and Technologies
10) 국토안보부(Department of Homeland Security)가 담당
11) 교육부(Department of Education)과 과학기술국(Office of Science and Techlology)이 담당
12) 인사국(Office of Personnel Management)이 담당
13) 국방부(Department of Defense), 국가정보장실, 국토안보부가 담당하며 세부 정책 추진과 관련해 각 연방 CIO 위원회 및 법무부(Department of Justice), 국가정보원(National Security Agency)의 역할도 강조

■ **사이버보안 인력 프레임워크는 실제 보안 시스템의 구축과 운영, 관리 및 유지보수 차원에서 사이버보안 업무를 크게 7가지로 분류하고, 업무별 세부 직종을 두어 구체적인 전문기술 요구사항을 제시**

- 7가지 업무는 안전한 기술 보급(Securely Provision), 운영 및 관리(Operate and Maintain), 보호 및 방어(Protect and Defend), 조사(Investigate), 운영 및 수집(Operate and Collect), 분석(Analyze), 지원(Support) 등으로 분류
- 가령 사이버보안 인력 프레임워크의 '안전한 기술 보급' 부문에는 IT 시스템 및 솔루션을 실제로 조직에서 수용할 때 관여하는 업무와 직종들이 해당되며, 여기에는 시스템 인증, 품질 보증을 위한 테스팅, 보안 기준 등 요구사항을 반영하기 위한 계획 수립, 실질적인 시스템 개발 업무 등이 포함

● **주요 기반시설 사이버보안 강화를 위한 행정명령의 주요 지시사항**

분류	설명
안전한 기술 보급 (Securely Provision)	• 시스템 개발 영역 • 안전한 IT 시스템의 기획, 디자인, 실질적인 구축 업무 • 정보 신뢰성 보장, SW 엔지니어링, 기업 아키텍처, 기술 시연, 시스템 요구사항 계획, 테스트 및 평가, 시스템 개발 등
운영 및 관리 (Operate and Maintain)	• 시스템 운영 영역 • 시스템 운영과 행정, 관리, 유지보수 업무 • 데이터 행정, IT 시스템 보안 관리, 정보 관리, 고객 서비스, 네트워크 서비스, 시스템 행정, 시스템 보안 분석 등
보호 및 방어 (Protect and Defend)	• 보안 강화 영역 • 시스템 안정성 강화, 위협요인 최소화, 외부 공격 대응 업무 • 컴퓨터 네트워크 보안, 사고 대응, 컴퓨터 보안 인프라 지원, 보안 프로그램 관리, 취약성 조사 및 관리 등
조사 (Investigate)	• 사후 대응 영역 • 사고 및 외부 공격 원인 분석, 증거 확보 업무 • 디지털 포렌식, 사고 조사 등
운영 및 수집 (Operate and Collect)	• 정보 수집 영역 • 사이버보안 강화를 위한 정보수집 업무 • 정보 수집 운영, 사이버 운영 계획 및 수행 등
분석 (Analyze)	• 정보 분석 영역 • 통계 분석, 사이버보안 계획 수립 지원 업무 • 사이버 위협 분석, 전방위 정보활동, 취약성 분석, 타깃 분석 등
지원 (Support)	• 외부 지원 영역 • 법률적 지원, 인력양성, 정책적 기반 마련 업무 • 법률 자문, 교육 및 훈련, 전략적 정책 계획 및 개발 등

출처 : 미국 국립표준기술연구소(2013.7)

- 프레임워크는 각 업무 분류별 세부 직종마다 주요 업무 내용과 필요한 지식 등을 구체적으로 정리해 두고 있어, 기업 및 단체가 현재 필요한 인재를 파악해 추가 인력 확보 및 사이버보안 교육 프로그램 계획 등에 폭넓게 활용 가능

- 기술 훈련이 필요한 개인 역시 프레임워크를 통해 현재 시장에서 요구되는 전문기술이 무엇인지, 어떤 직종에서 어떤 업무를 담당하게 될 지 쉽게 이해할 수 있어 커리어 구축에 유용

■ **사이버보안 인력 프레임워크는 2013년 7월 최종 버전이 공개된 이후 점진적인 보급 및 업데이트가 이뤄지고 있는 것으로 파악**

- 국토안보부는 프레임워크의 보급 독려를 위해 사이버보안 커리어 및 연구 지원 웹사이트[14]에서 이를 대대적으로 홍보하고 있으며, 이 외에도 지속적인 세미나 개최, 사이버보안 교육 커리큘럼 제공 등 사이버보안 전문인력양성을 위한 활동을 추진 중
- 이 외에 사이버보안 인력 프레임워크를 연방 및 지방정부, 민간 영역에 확대 보급하기 위한 사이버 인력 인벤토리 프로그램(Cyber Workforce Inventory Program)도 추진

3.2. 영국: 사이버보안 전문가 인증 제도

■ **영국 정보안보국 정부통신본부[15] 산하의 정보보호 전문기관인 전자통신보안그룹[16]은 사이버보안 전문인력에 대한 수요를 충족하기 위해 사이버보안 전문가 인증 제도(Certified Professionals)를 시행 중**

- 영국 정부의 사이버보안 전략의 일환으로 발족한 인증 제도는 전자통신보안그룹이 2011년 3월 최초로 사이버보안 전문직종을 정의한 1차 보고서를 발간하며 정식 발족, 2014년 3월 현재 4차 보고서까지 공개된 상태
- 사이버보안 전문가 업종을 국가 차원에서 정의하고 각 업종별로 갖춰야 할 역량을 수치화함으로써, 정부기관 및 기업을 위한 체계적인 인력양성 및 인재 수급 환경을 창출하는 것이 목적

■ **사이버보안 전문가 인증 제도는 사이버보안 및 정보보호와 관련된 직업들을 공식적으로 정의하고, 각 직업별 기술 수준을 수치화해 특정 인재의 역량을 직관적으로 판단할 수 있도록 한 점이 특징**

- 각 직업별로 요구되는 기술 역량을 프레임워크 형태로 통일시켜 수치로 표시하고 있어, 특정 업무에 필요한 인재를 찾거나 새로 인재를 훈련시킬 때 직관적인 기준을 제시한 것도 주목할 만한 부분

14) niccs.us-cert.gov
15) Government Communications Headquarter, CGHQ
16) Communications-Electronics Security Group, CESG

- 특정 업무에 요구되는 각 기술 역량은 영국 정보보호 전문학원[17] 이 정의한 것을 기준으로 삼아 산업표준으로서의 역할도 고려되며,
- 또, 각 직종별로 기술 역량의 수준에 따라 인증 레벨을 구분해 실력이 뛰어난 인재를 선별하도록 유도

■ 전자통신보안그룹은 인증 제도를 통해 사이버보안 전문가 직종을 7가지로 분류

- 신임자(accreditor)는 IT 시스템이 산업 기준에 부합하는지 여부를 판단해 사용 승인을 내리는 결정권자 역할을 담당하며, 특히 리스크 평가 및 관리 역량, 법제도에 대한 지식, 정보보호 관련 방법론에 대한 역량이 중요
- 정보보증[18] 감사(IA Auditor)는 기업 및 기관의 보안 시스템이 기준에 부합한지 평가하고 개선 방안을 제시하는 역할을 수행하며, 업무 총괄, 제도 및 표준 관련 지식, 규제 환경에 대한 이해력, 조사 및 평가 능력이 중시되는 직종
- 정보보증 아키텍트(IA Architect)는 기업의 요구에 부합하는 보안 시스템을 기획 및 구축하고 리스크를 최소화하는 업무를 맡으며, 사업 혁신성 개선, 보안 아키텍처 및 개발 역량이 중요시됨
- 정보보안 리스크 자문(Security and Information Risk Advisor)은 보안 리스크를 식별하고 해결방안을 제시하는 조언자로서의 역할을 담당하며, 정보보안과 관련된 제도적, 산업적 지식이 풍부해야 하고 리스크 평가 및 관리 역량, 조사 능력, 사후 대처 능력 등이 필요한 직업
- IT 보안 책임자 직업군(IT Security Officer Family)은 사이버보안과 관련된 각종 업무를 책임지는 최고결정권자들을 의미하며, 전반적인 IT 시스템 관련 의사결정, 관리 업무를 총괄하기 위한 규제 관련 지식과 시스템 운영 및 관리 능력, 사후 대처 능력 들이 요구
- 통신 보안 직업군(Communications Security Family)은 IT 보안 책임자 직업군과 유사하나 통신 네트워크 분야에서 주로 다뤄지는 암호화 관련 보안 업무를 책임진다는 점이 차이
- 도입 테스터(Penetration Tester)는 실제 시스템 및 솔루션 도입 전에 테스트를 수행하는 데 있어 주도적인 역할을 수행하는 직종으로, 제도 및 표준 관련 지식, 보안 테스팅 및 취약성 평가 능력, 실무 연구 능력 등이 고려

17) Institute of Information Security Professionals
18) Information Assurance(IA)로, 영국에서는 사이버보안과 거의 같은 의미로 통용

● 영국 사이버보안 전문가 인증 제도의 7가지 전문가 직종

전문가 직종	역할	주요 기술 역량
신임자(Accreditor)	IT 시스템이 산업 기준에 부합하는지 여부를 판단하는 결정권자	리스크 평가 및 관리, 법제도 지식 등
정보보증 감사(IA Auditor)	보안 시스템의 기준 부합 여부를 평가하는 감사자	규제환경 이해, 조사 및 평가 능력 등
정보보증 아키텍트(IA Architect)	보안 시스템의 기획, 구축을 담당하고 리스크를 최소화하는 현장 실무자	보안 아키텍처, 개발 능력 등
정보보안 리스크 자문(Security and Information Risk Advisor)	보안 리스크를 식별하고 해결방안을 제시하는 조언자	리스크 평가 및 관리, 사후 대청 능력 등
IT 보안 책임자 직업군(IT Security Officer Family)	사이버보안 관련 각종 업무를 총괄하는 책임자	의사결정, 규제환경 이해, 시스템 운영 · 관리 능력 등
통신 보안 직업군(Communications Security Family)	특히 통신 네트워크 분야의 전문 영역인 암호화 관련 보안 업무 책임자	의사결정, 규제환경 이해, 시스템 운영 · 관리 능력 등
도입 테스터(Penetration Tester)	실제 시스템 도입 전 적합성 여부를 판단하는 테스터	테스팅 및 취약성 평가, 실무 연구 능력 등

출처 : 영국 CESG(2013.7)

■ 각 직업별 인증 기준을 통과하기 위한 기술 역량은 크게 9가지 카테고리로 구분하고, 각 역량들을 카테고리별로 A부터 F까지의 코드로 분류

- 정보보호 관리(Information Security Management, 코드 A) 부문은 전반적인 정보보호 시스템의 관리, 구축, 계획을 위한 능력들을 의미하며, 업무 총괄 능력, 제도 및 표준, 규제 환경에 대한 지식, 정보보호 전략 수립 능력, 외부 자원 관리 역량 등이 포함
- 정보 리스크 관리(Information Risk Management, 코드 B) 부문은 내부 시스템의 취약성 등 리스크를 파악하고 이를 최소화하는 능력으로, 리스크 평가 및 관리 역량이 이에 해당
- 보안 시스템 도입(Implementing Secure Systems, 코드 C) 부문은 실질적인 보안 시스템을 조직에 도입하기 위한 보안 아키텍처 기획 및 개발 역량을 의미
- 정보보증 방법론 및 테스팅(IA Methodologies and Testing, 코드 D)은 보안 시스템 도입에 있어 이론적인 기반을 제시하는 능력으로, 보안 방법론에 대한 지식, 테스팅 기술 등이 포함
- 보안 실무(Security Discipline, 코드 E~I) 역량은 크게 운영 관리(Operational Security Management, 코드 E), 사고 관리(Incident Management, 코드 F), 감사 평가(Audit,

Assurance and Review, 코드 G), 사업 지속성 관리(Business Continuity Management, 코드 H), 정보 시스템 연구(Information System Research, 코드 I)의 세부 분류로 구분되며 실무 현장에서의 업무 능력들이 포함

- 일례로 IT 보안 책임자 직업군의 경우 보안 시스템에 대한 총괄 업무 담당을 위해 법제도와 규제에 대한 전반적인 지식이 요구되며, 실무 영역에서 보안 운영 관리, 서비스 제공, 취약성 평가 역량, 사고 대응 차원에서 사고 관리 역량이 필요한데, 이는 코드상으로 각각 A6, E1, E2, E3, F1에 해당

● **영국 사이버보안 전문가 인증 제도의 직업 역량 수치표 예시 (IT 보안 책임자 직업군)**

핵심 역량: A6, E1, E2, E3, F1	인증 레벨별 요구 역량 수준*		
기술 역량 분류	정보보호 보안실무자	정보시스템 보안관리자	IT 보안 책임자
A1–업무 총괄(Governance)	2	2	3
A2–제도 및 표준(Policy 7 Standards)	2	2	3
A3–정보보호 전략(Information Security Strategy)	1	2	3
A4–혁신 사업 개선(Innovation & Business Improvement)	2	2	3
A5–정보보호 인식 및 훈련(IS Awareness & Training)	1	2	2
A6–법률 및 규제 환경(Legal & Regulatory Environment)	2	2	3
A7–외부 자원 관리(Third Party Management)	1	2	2
B1–리스크 평가(Risk Assessment)	1	2	2
B2–리스크 관리(Risk Managment)	1	2	3
C1–보안 아키텍처(Security Architecture)	1	2	2
C2–보안 개발(Security Development)	1	1	2
D1–정보보증 방법론(IA Methodologies)	1	2	2
D2–보안 테스팅(Security Testing)	1	2	2
E1–보안 운영 관리(Secure Operations Managements)	1	2	3
E2–보안 서비스 제공(Secure Ops & Service Delivery)	2	3	3
E3–취약성 평가(Vulnerability Assessment)	1	2	3
F1–사고 관리(Incident Management)	1	2	2
F2–조사(Investigation)	1	2	2
F3–범죄수사학(Forensics)	1	2	2
G1–감사 및 검사(Audit and Review)	1	2	2
H1–사업 지속성 계획(Business Continuity Planning)	1	2	2
H2–사업 지속성 관리(Business Continuity Management)	1	2	2
I1–연구(Research)	–	–	1
I2–학술적 연구(Academic Research)	–	–	1
I3–실무 연구(Applied Research)	–	–	1

* 해당 항목의 수치가 높을수록 업무 수행을 위해 높은 기술 역량이 요구됨을 의미

출처 : 영국 CESG(2013.7)

3.3. 일본: 정보처리추진기구의 사이버보안 역량 강화 사업

■ 일본 내 IT 관련 정책추진에 중심적인 역할을 맡고 있는 정보처리추진기구[19]는 일본 정부의 IT 인재 육성 정책의 일환으로 사이버보안 역량 강화 사업을 추진 중

- 정보처리추진기구의 사업 추진은 ▲정보보호(사이버보안) 직종 및 역량 분류 작업 ▲IT 인재에 대한 정보보호 교육 수요조사 ▲IT 인재에 대한 정보보호 교육 사업 성과 검토 등으로 구분
- 이 중 정보보호 직종 및 역량 분류 작업은 지난 2012년 경제산업성이 정보보호 직종과 역량 관련 표준안이 마련되어 이를 활용한 표준 직업군과 관련 역량들을 체계화
- 정보보호 육성 수요조사와 관련해서는 매년 수요조사 보고서를 발간하고 있으며, 최신 보고서인 2013년판은 지난 2014년 3월 발간

■ 정보처리추진기구는 정보보호 역량 분류 결과물을 토대로 정보보호 강화에 대응하는 공통 직업 역량 프레임워크(Common Career Skill Framework, CCSF)을 마련

- CCSF는 전반적인 IT 인재 육성에 있어 각각의 직업군을 체계화하고 특정 업무를 수행할 인재 육성에 요구되는 기술 역량의 기준을 제시하기 위한 일종의 산업 표준 역할을 수행
- 그 중에서도 사이버보안과 관련해서는 경제산업성의 정보보호 인재 육성지표 등 책정 사업의 일환으로 작성된 '정보보호 인재의 모델 직업군(情報セキュリティ人材のモデルキャリア)' 보고서 내용을 기준으로 활용
- 경제산업성의 보고서는 CCSF의 기술 표준에 해당하는 'IT 시스템 기술 표준(ITSS)'[20], 'IT 시스템 유저 기술 표준(UISS)'[21], '조직 기술 표준(ETSS)'[22]을 기준으로 각 사이버보안 직업군을 정의하고 직업별 요구되는 기술 역량을 수치화하여 제시
- 또한, 각 직업별로 기술 역량의 수준에 따라 레벨 차등을 두어 높은 레벨일수록 책임이 따르는 중요 업무를 맡을 수 있다고 명시하고 있으며, 새로운 인력양성이나 기존 인재의 역량 강화를 위한 육성 방침에 대한 조언도 포함

19) Information-technology Promotion Agency, IPA
20) IT Skill Standard, IT 시스템 및 SW의 개발 및 서비스 제공을 담당하는, IT 제공자 측면에서의 인재를 위한 기술 표준
21) User IT Skill Standard, IT 시스템을 실제 도입 및 활용하는, 고객 기업 측면에서의 인재를 위한 기술 표준
22) Embedded Technology Skill Standard, 임베디드 솔루션 및 SW 개발에 특화된, IT 제공자 측면에서의 인재를 위한 기술 표준

■ **정보보호 인재 육성 관련 수요 및 과제 조사 보고서는 현재 일본 산업계의 사이버보안 관련 위협요인을 정리하고, 이에 대응하기 위한 보안 인재 육성의 과제와 해결책을 제시하는 데 초점**

- 정보처리추진기구가 정기적으로 발간하는 연례 보고서인 '10대 보안위협', 'IT 인재백서' 등을 토대로 사이버보안 산업 현황을 파악함으로써, 현재 업계의 주요 보안 이슈에 신속히 대응하는 인재 육성 정책을 펼치는 데 필요한 기초자료로 활용
- 2014년 3월 최신 보고서[23]에 따르면, 현재 일본 내 주요 사이버보안 위협을 6가지[24]로 규정하고, 각 위협에 대한 대처 방안과 요구되는 IT 인재의 역량 등을 상세히 소개

● **일본 내 주요 정보보호(사이버보안) 위협별 대응을 위해 요구되는 IT 인재 역량**

정보보호 위협	위협에 대응하기 위해 요구되는 IT 인재 역량				
	시스템 라이프사이클			관리	사업전략
	IT 시스템 기획	시스템 개발·구축	시스템 운영	정보보호 관리	정보보호 전략
타깃 공격(멀웨어, 바이러스 등)			○		
불법 침입(해킹 등)		○	○		
시스템 악용		○			
클라우드 관련 데이터 사고 (데이터 유실, 도난 등)	○		○		
스마트 단말 데이터 유출					○
내부 직원의 부정 및 실수				○	

출처 : 일본 정보처리추진기구(2014.3)

- 또한, 실제 기업이 정보보호 전문인력을 확보하기 위해 해결되어야 할 과제들을 4가지[25]로 정리하고 해결책을 제시

■ **마지막으로 정보처리추진기구는 2014년 중으로 지금까지의 정보보호 인재 육성과 관련해 추진했던 사업들을 종합적으로 검토하는 성과분석 사업을 시행할 예정이며, 아직까지 구체적인 계획은 공개되지 않은 상태**

23) 일본 정보처리추진기구, "情報セキュリティ上の脅威から企業を護るための人材育成ガイド", 2014.3.
24) 타깃 공격, 불법 침입, 시스템 악용, 클라우드 관련 데이터 사고, 스마트 단말 데이터 유출, 내부 직원의 부정 및 실수 등
25) 기업 내부적으로는 ▲인재의 필요성에 대한 이해 부족 ▲인재 육성의 어려움 ▲인재의 기업 내 처우 부실 등이 지목됐으며, 기업 외적으로는 ▲우수한 인재 확보 및 이직 등 높은 인재 유동성 등 외부요인이 지목

3.4. 이스라엘: 선진기술원을 통한 산업 중심적 사이버보안 인력양성 전략

■ 이스라엘 정부는 별도의 정책을 추진하기보다, 이스라엘의 IT 산업 성장세의 힘을 빌어 사이버보안 산업 육성 및 인력양성을 도모하는 전략을 수립

- 현재 시스코(Cisco), 마이크로소프트(Microsoft), 구글(Google), 애플(Apple), IBM, 오라클(Oracle), SAP, EMC, HP 등 수많은 메이저 기업들이 이스라엘 내에 기술 연구소를 설립하고 운영 중인 상태
- 이들 대형 IT 사업자들은 이스라엘 출신의 신생업체를 대거 인수하면서 기술력 강화에 힘쓰고 있으며, 이 때문에 이스라엘은 '스타트업 국가(The Startup Nation)'라는 별칭으로 불리는 상황 [26]
- 특히 IBM, 시스코, GE(General Electric) 등은 2013년에만 이스라엘의 사이버보안 관련 업체에 대한 대규모 M&A 및 투자에 나서는 등 이스라엘 내 사이버보안 산업이 본격적으로 성장하는 계기로 작용
- 이처럼 글로벌 대기업들이 이스라엘을 중심으로 IT 기술 혁신을 도모하는 상황을 이용하려는 것이 이스라엘 정부의 주된 사이버보안 강화 정책의 골자

■ 이스라엘 업계는 지난 2013년 9월 벤 구리온 대학(Ben Gurion University) 캠퍼스에 설립된 선진기술원 (Advanced Technology Park)이 사이버보안 산업 진흥에 있어 중대한 계기가 된 것으로 평가

- 이스라엘의 베냐민 네타냐후 수상이 설립을 주도한 선진기술원은 산업계와 학계의 연계를 통한 사이버네틱스 및 사이버보안 기술의 글로벌 중심을 표방
- 선진기술원이 들어선 벤 구리온 대학은 오랫동안 이스라엘의 사이버보안 기술 연구의 메카로 자리했던 장소로, 도이치 텔레콤(Deutche Telekom) 등 외국 기업들과 사이버보안 관련 제휴도 다수 추진

■ 무엇보다 선진기술원은 이스라엘 국방부와도 연계되어 특히 사이버보안 측면에서 이스라엘 정부의 대규모 지원이 예상되는 상황

- 이스라엘은 주변국과의 긴장 상태로 인해 특히 국방 및 보안에 대한 경각심이 높은 국가로, 이스라엘 국방부는 사이버전쟁을 상정한 전문 해커 중심의 사이버군대를 보유한 것으로도 유명

26) 실제로 이스라엘의 인구대비 신생업체 수는 1,844명 당 1개로 미국의 2.5배 수준

- 이 같은 이스라엘의 국가 성향은 사이버보안에 대한 높은 관심으로 이어지고 있으며, 일반 시민들 역시 사이버보안 관련 직업과 학문 연구에 큰 관심을 보이는 분위기
- 결국 이스라엘 정부 주도의 선진기술원 설립 사업은 국가의 비전과 국민의 의지, 산업 내 수요가 절묘하게 결합하면서 자연스럽게 사이버보안 기술 발전 및 인력 확대로 이어지는 결과를 달성할 것으로 기대

■ **한편, 이스라엘 정부의 사이버보안 관련 정책을 총괄하는 총리실 소속 사이버국에서는 이스라엘 대학의 사이버보안 교육 지원, 사이버국방 프로그램 정책 등을 추진 중**

- 과학기술부[27]와의 협력을 통해 대학 연구기관의 사이버보안 지원 펀드로 2012~2014년 동안 3,200만 세켈(약 94억 7,000만 원)을 투자했으며, 사이버 분야에서 대학원 이상의 학위 취득을 준비 중인 학생을 지원하고자 2012~2014년 동안 1,600만 NIS(약 47억 3,000만 원)도 추가 확보
- 사이버 정보전이 격화되면서 주변국의 해킹 공격 우려가 증대됨에 따라, 전문적인 사이버 국방 인력양성을 위한 특별 프로그램 '마그시밈 류미트(Magshimim Leumit)'를 출범하고, 16~18세의 젊은 이스라엘 청소년을 대상으로 전문적인 사이버 및 컴퓨팅 관련 교육 프로그램을 제공
- 특히 '마그시밈 류미트' 프로그램은 이스라엘 정보국 모사드[28], 이스라엘 안보국[29] 등 주요 사이버보안 관련 정부기관과의 연계를 통해 교육 수료 후 정부기관 취직 기회 등을 제공하며 공공 분야의 인력 수요를 창출

4. 결론 및 시사점

■ **본 고에서 소개한 주요국의 사이버보안 인력양성 정책은 대체로 사이버보안 및 관련 직종을 정의하고, 사이버보안 인재로서 요구되는 기술 역량을 체계화하는 데 많은 노력을 기울이는 것으로 파악**

- 미국의 사이버보안 인력 프레임워크는 사이버보안뿐만 아니라 관련 IT 산업 전반에 걸쳐 연관성이 있는 직업들을 체계적으로 분류
- 영국의 사이버보안 전문가 인증 제도는 실제 보안 관련 직업을 보유한 인재들을 효율적으로 관리하고 육성하기 위한 수치화된 기준을 제시했다는 점에서 높게 평가

27) Ministry of Science and Technology
28) Mossad
29) Israel Security Agency

- 일본은 과거부터 IT 인력양성이라는 측면에서 체계화된 직업군 분류 표준을 마련해 두고 있는데, 최근 사이버보안에 대한 사회적 관심이 높아지면서 IT 인재의 직업군 분류에서 사이버보안 관련 내용이 대거 반영되는 분위기
- 이스라엘은 정부 차원에서 사이버보안 관련 직업군의 기준이 아직 구체화되지 않은 것으로 파악되나, 산업계 및 학계와의 연계를 통해 사이버보안 인력양성을 도모하고 있다는 점에서 이들의 자율적인 체계화 작업에 기대는 것으로 관측

■ **이 같은 직업군 분류 및 기술 역량 체계화는 실제로 산업계에서 요구하는 인재상을 찾아내어 신속히 수요를 충족하기 위한 가장 기초가 되는 작업**

- 이는 단순히 정부 주도의 사이버보안 교육 프로그램 추진을 위한 것이 아니라, 산업계가 스스로 사이버보안 인재를 확보하고 필요하다면 직접 교육시키도록 유도하기 위한 것
- 실제로 미국, 영국, 일본의 각 사이버보안 직업군 분류 체계들은 각 기업들이 해당 분류 체계를 왜 활용해야 하는지 실제 사례를 바탕으로 설명하는 데 공을 들이고 있는 것으로 파악

■ **향후 사이버보안 인력양성을 더욱 가속화하기 위해서는 직업 분류 체계화 작업과 함께 이를 실제 기업들이 도입해 인력양성에 직접 나설 수 있도록 정책적 지원이 뒷받침되어야 할 전망**

- 대부분의 사이버보안 인재 수요는 기업 등 시장 측면에서 창출되고 있으므로, 기업이 이 같은 수요를 스스로 해소할 수 있도록 독려하는 것이 정부의 역할
- 이 같은 측면에서 이스라엘 정부와 같이 직접적인 사이버보안 인력양성 정책은 뚜렷하게 제시하지 않으면서도 산업계와 학계가 스스로 협력하며 발전할 수 있는 생태계를 구축하는 것도 유효한 정책적 방향

■ **그러나 국가 차원에서 산업계 전반에 걸친 사이버보안 인력 수요를 해소하는 것은 현실적으로 쉽지 않은 실정**

- 각 산업별로 구축되어 있는 IT 시스템 및 사이버 생태계, 보안 우선순위, 대표적인 위협 요인 등이 차이를 보이는 데다, 특정 산업에 대한 이해가 수반되어야 실질적인 보안 업무 수행이 가능하기 때문
- 따라서 일원화된 교육 프로그램이나 특정 역량만을 부양하는 인력양성 정책보다는 포괄적인 관점에서 사이버보안 인재를 키울 수 있는 생태계를 구축하는 것이 정부의 정책 추진에 있어 핵심 과제로 지목

■ 사이버보안 인력양성 생태계 구축의 첫걸음은 사이버보안 관련 직무를 명확히 이해하는 것

- 사이버보안은 일반인에게는 여전히 막연하고 생소한 개념이며, 구체적으로 어떤 분야에서 어떤 목적으로 업무를 수행하는 것이 '사이버보안'에 해당하는지 정의하는 것이 최우선
- 사이버보안은 지켜야 할 대상이나 위협요인에 따라 수많은 변수가 발생하므로 각각의 보안 업무에 따라 요구되는 기술 역량도 달라지며, 사이버보안을 정의할 때에도 이 점을 최대한 고려
- 사이버보안은 다른 IT 계열의 업무와 직간접적으로 관계를 맺으므로, 이들 업무와의 연계성을 감안해 별도의 사이버보안 업무를 지정하거나 기존 IT 업무를 사이버보안과 통합하는 작업도 필요
- 모든 업무에서 공통적으로 요구되는 역량을 파악하는 것도 중요하며, 이를 전문인력이 아닌 일반인 대상의 기초적인 사이버보안 교육에 활용함으로써 전반적인 사이버보안 환경의 개선을 도모
- 국내의 경우 교육 프로그램 인증제도 마련, 정보보호교육 총괄기관 설립 등을 통해 사이버보안 관련 직업군의 체계적인 관리와 각 업무 영역별로 요구되는 능력에 대한 구체적인 기준 제시를 할 수 있다면 보다 효율적인 인력양성 시스템을 갖출 수 있을 전망

■ 전문적인 지식이 요구되는 사이버보안 인력양성에 있어 전문 기술과 노하우를 보유한 기업체 또는 교육기관의 도움이 국가의 정책 추진에 있어 필수적인 요소

- 현재 업계의 사이버보안 인력 수요를 누구보다 빨리 파악할 수 있는 기업들은 사이버보안 인력난에 신속히 대응할 수 있으며, 실무 측면에서 요구되는 기술 역량을 함양하는 데 적합한 교육과정 개발이 가능
- 교육기관은 기업과의 연계를 통해 이들의 기술력과 노하우를 교육 커리큘럼으로 체계화하는 데 특화되어 있으며, 사이버보안에 관심이 있는 이들을 모으고 기회를 제공하는 포털로서의 역할도 수행 가능
- 정부는 이 같은 산 · 학 연계를 촉진하기 위한 수단으로 파트너십 지원 프로그램, 연구단지 구축, 기술 상용화 촉진 정책 등을 고려 가능
- 또한, 교육기관에 대한 사이버보안 전문 교원 확보, 사이버보안 관련 학과 신설, 수료생에 대한 혜택 확대 등으로 민간 영역에서의 사이버보안 인력양성의 활성화를 도모 가능

참고문헌

1. 미국 NICE, “CYBERSECURITY workforce framework”, 2013.7.
2. 영국 CESG, “CESG Certification for IA Professionals”, 2014.3.
3. 영국 CESG, “Guidance to CESG Certification for IA Professionals”, 2014.3.
4. 일본 경제산업성, “情報セキュリティ人材の育成指標等の策定事業 – 情報セキュリティ人材のモデルキャリア”, 2013.3.
5. 일본 정보처리추진기구, “平成25年度 ＩＴ人材における情報セキュリティの育成ニーズ・課題調査”, 2014.3.
6. 일본 정보처리추진기구, “情報セキュリティ上の脅威から企業を護るための人材育成ガイド”, 2014.3.
7. NextGov, “OBAMA’S NEW CYBERSECURITY GUIDELINES LACK A WORKFORCE PLAN”, 2014.2.14
8. Tech Republic, “How Israel is rewriting the future of cybersecurity and creating the next Silicon Valley”, 2013.10.1
9. 보안뉴스, “최정예 사이버보안 인력(K–Shield) 되고 싶다면?”, 2014.5.8
10. 미래창조과학부, “국가 사이버안보 종합대책 발표”, 2013.7.4
11. 미래창조과학부, “미래부, 정보보호산업 발전 종합대책 발표”, 2013.7.4
12. 지식정보보안산업협회, “2013 국내 정보보호산업 실태조사”, 2013.12
13. 한국인터넷진흥원, “2014년 K–Shield 인증 교육과정 교육생 모집”, 2014.4.28
14. 한국인터넷진흥원, “2013 한국인터넷백서”, 2013.9.23
15. 한국인터넷진흥원, “국내 정보보호 교육체계 연구”, 2013.6.