글로벌 정보보호인력양성 사례분석 연구

Case analysis study on global information security human resources training

고용노동부
HRDK 한국산업인력공단 Human Resources Development Service of Korea
ISC 정보보호 인적자원개발위원회 Information Security Industrial Skills Council

글로벌 정보보호인력양성 사례분석 연구

Case analysis study on global information security human resources training

수탁기관 : 한국정보통신보안윤리학회

연구책임자: 교 수 유 진 호 (상명대학교)
참여연구원: 교 수 조 일 형 (상명대학교)
교 수 김 민 정 (상명대학교)
연 구 원 김 진 성 (상명대학교)
책 임 최 수 민 (한국정보통신보안윤리학회)

Content

표 목차

Content

그림 목차

P·A·R·T 01

서론

1. 연구 목적

□ 글로벌 정보보호 전문인력 양성방안을 조사하여, 해외 우수사례를 발굴하고 국내 현황과의 비교·분석을 통해 향후 국내 정보보호 전문인력 양성 방안 개선과 고도화에 활용

2. 연구 범위

□ 정보보호 전문인력 자격제도 조사

- 국가별로 주요 자격제도의 운영방식 및 사후관리 관련 사항 제시
  예) 검정내용, 시험시간, 합격기준, 응시료, 시험방식, 응시언어, 자격 유효기간 등

□ 국내 자격제도와의 비교

- 과정평가형 자격 등 국내 자격제도의 주요 현황 및 특징과 조사한 해외 사례와의 공통점·차이점 등 분석

□ 정보보호 전문인력 양성을 위한 교육 프로그램 조사

- 국가별 주요 교육기관 및 교육프로그램의 운영 현황에 대한 사항 제시
  예) 교육기관 운영형태 및 주요 설비, 교육 커리큘럼 및 특징, 교육대상 등

□ 국내 정보보호 전문인력 양성 교육과의 비교

- 국내 정보보호 전문인력 양성 프로그램의 주요 현황 및 특징과 조사한 해외사례와의 공통점·차이점 등 분석

□ 정보보호 전문인력 양성 교육 프로그램 우수 사례 발굴

- 조사 내용을 바탕으로 국내 정보보호 전문인력 양성에 적용 가능한 우수 사례 공유 및 국내 적용방안 등 시사점 제시

P·A·R·T 02

정보보호분야 자격제도

제1절 국가별 자격제도 운영현황

1. 미국

□ 민간 중심으로 운영되며, 정부 기관이 자격제도의 공신력을 인정

- **민간 인증기관 중심이며, IT 기업도 자사의 서비스를 위한 교육 및 자격제도를 시행**
  - 국제 정보시스템 보안인증 컨소시엄(**ISC2**, International Information System Security Certification Consortium), 정보시스템 감사 및 통제 협회(**ISACA**, Information Systems Audit and Control Association), 국제 전자상거래 컨설턴트 협의회(**EC-Council**, International Council of E-Commerce Consultants) 등 민간 인증기관이 주도
  - 아마존(AWS), MS(Azure), 구글(GCP) 등은 자사의 클라우드 서비스를 위한 자격제도 및 교육을 운영

- **미국 국가표준협회(ANSI, American National Standards Institute)와 국방부 등 관련 정부 기관에서 민간 개인 자격제도의 공신력을 인정**
  - ANSI의 국가인증위원회(ANAB, ANSI National Accreditation Board)는 개인의 자격을 인증하는 기관(certification body for persons)의 인증체계 개발 및 유지관리에 대한 요구사항을 평가하여 국제 표준인 **ISO/IEC 17024**[1] 인증을 부여
  - 미 국방부(DoD, Department of Defense) 인력혁신국의 **DoD 매뉴얼(DoDM) 8140.03**은 사이버공간 인력 자격 및 관리 프로그램으로, 민간 자격제도를 포함하여 사이버보안에 대한 역량을 구분하여 인증

□ **ISC2**의 주요 정보보호 자격제도

- **ISC2는 정보보호 전문가를 중심으로 1989년 설립된 비영리기관으로, 다양한 정보보호 자격제도와 교육을 시행 중**

1) 국제표준화기구(ISO, International Organization for Standardization)에서 발행하는 개인 인증을 운영하는 기관에 대한 적합성 평가 항목이며, 법률, 금융 등 일반요구사항, 경영 및 조직구조, 인력운영, 기록 및 정보관리, 인증제도, 인증 프로세스, 관리시스템 등 인증기관의 공정한 운영을 위한 항목으로 구성

- 정보시스템 보안전문가 인증(CISSP, Certified Information Systems Security Professional)
  - **(목적)** 조직의 정보보호 프로그램을 이끌 수 있는 지식, 기술, 능력을 갖춘 사이버보안 전문가(professional) 양성이 목적
  - **(검정내용)** 보안 및 위험 관리, 자산 보안, 보안 아키텍처 및 엔지니어링, 통신 및 네트워크 보안, ID 및 액세스 관리, 보안 평가 및 테스트, 보안 운영, 소프트웨어 개발 보안 등 8개 부문

[표 2-1] CISSP 검정내용

부문 (가중치, %)	세부항목
보안 및 위험관리 (16%)	• 보안 개념 이해 및 적용(정보보호 5요소) • 보안 거버넌스 원칙의 평가 및 적용 • 보안 관련 법률, 규제 및 규정 • 조사 유형(예 : 행정, 형사, 민사, 규제, 산업 표준)에 대한 이해 • 보안정책, 표준, 절차 및 가이드라인 개발, 문서화 및 구현 • 비즈니스 연속성 요구사항 식별, 분석, 평가, 우선순위 지정 및 구현 • 인사 보안 정책 및 절차에 기여하고 이를 시행 • 위험관리 개념 이해 및 적용 • 위협 모델링 개념 및 방법론 • 공급망 위험관리 개념 적용 • 보안교육 및 훈련 프로그램 구축 및 유지
자산보안 (10%)	• 정보 및 자산 식별 및 분류 • 정보 및 자산 처리 요구 사항 설정 • 정보 및 자산을 안전하게 제공 • 데이터 수명 주기 관리 • 적절한 자산 유지(예 : 수명 종료, 지원 종료) 보장 • 데이터 보안 제어 및 규정준수 요구사항 결정
보안 아키텍처 및 엔지니어링 (13%)	• 보안 설계 원칙을 사용하여 엔지니어링 프로세스를 연구, 구현 및 관리 • 보안 모델의 기본 개념 이해(예 : Biba, Star Model, Bell-LaPadula) • 시스템 보안 요구 사항에 따라 제어 선택 • 정보 시스템의 보안 기능 이해 • 보안 아키텍처, 설계 및 솔루션 요소의 취약성을 평가하고 완화 • 암호화 솔루션 선택 및 결정 • 암호 분석 공격 방법 이해 • 사이트 및 시설 설계에 보안 원칙 적용 • 설계 사이트 및 시설 보안 제어 • 정보 시스템 수명 주기 관리
통신 및 네트워크 보안 (13%)	• 네트워크 아키텍처에 보안 설계 원칙 적용 • 보안 네트워크 구성 요소 • 설계에 따라 보안 통신 채널을 구현

부문 (가중치, %)	세부항목
ID 및 액세스 관리 (13%)	• 자산에 대한 물리적 및 논리적 액세스 제어 • 설계 식별 및 인증 전략(예 : 사람, 장치 및 서비스) • 제3자 서비스와의 연합 ID • 권한 부여 메커니즘 구현 및 관리 • ID 및 액세스 프로비저닝 수명 주기 관리 • 인증 시스템 구현
보안 평가 및 테스트 (12%)	• 평가, 테스트 및 감사 전략 설계 및 검증 • 보안 제어 테스트 수행 • 보안 프로세스 데이터 수집(예 : 기술 및 관리) • 테스트 출력 분석 및 보고서 생성 • 보안 감사 수행 또는 촉진
보안 운영 (13%)	• 조사 이해 및 준수 • 로깅 및 모니터링 활동 수행 • 구성 관리 수행(예 : 프로비저닝, 베이스라이닝, 자동화) • 기본 보안 운영 개념 적용 • 리소스 보호 적용 • 사고 관리 수행 • 탐지 및 예방 조치 운영 및 유지 • 패치 및 취약성 관리 구현 및 지원 • 변경 관리 프로세스를 이해하고 참여 • 복구 전략 구현 • 재해 복구 프로세스 구현 • 재해 복구 계획 테스트 • 사업 연속성 계획 및 연습 참여 • 물리적 보안 구현 및 관리 • 인사 안전 및 보안 문제 해결
소프트웨어 개발 보안 (10%)	• 소프트웨어 개발 수명 주기에서 보안을 이해하고 통합 • 소프트웨어 개발 생태계에서 보안 제어를 식별하고 적용 • 소프트웨어 보안의 효과성 평가 • 취득한 소프트웨어의 보안 영향 평가 • 보안 코딩 가이드라인 및 표준 정의 및 적용

[출처] https://www.isc2.org/

- **(응시자격)** 검정내용의 8개 부문 중 2개 이상에서 최소 5년 경력 필요[2)]
- **(시험시간)** 최대 3시간
- **(합격기준)** 1,000점 만점에 700점 이상(약 100 ~ 150 문항[3)])
- **(응시료)** $749

2) 컴퓨터, 정보기술 분야의 학위 또는 ISC2의 자격증으로 최대 1년의 경력을 추가할 수 있으며, 경력이 전혀 없어도 CISSP 시험에 합격하여 ISC2 준회원이 된 후 6년 이내에 경력을 쌓으면 자격인정
3) CAT 시험방식으로 개인별로 문항 수와 난이도에 차이

- **(시험방식)** 컴퓨터 적응형 시험(CAT, Computerized Adaptive Testing)으로, 응시자의 능력 수준에 맞춰 조정
- **(응시언어[4])** 중국어, 영어, 독일어, 일본어, 스페인어
- **(자격유효기간)** 자격 취득 후 매년 135달러의 연간유지관리수수료(AMF, Annual Maintenance Fees)를 지불하고, 자격증을 유지하기 위해서는 지속적인 전문 교육(CPE, Continuing Professional Education)[5]의 학점 취득이 필요[6]

○ 시스템 보안실무자 인증(SSCP, Systems Security Certified Practitioner)

- **(목적)** 전문가가 사이버보안 모범 사례를 통해 IT 인프라를 구현, 모니터링 및 관리할 수 있는 지식과 기술을 갖추고 있음을 입증
- **(검정내용)** 보안 개념 및 관행, 액세스 제어, 위험 식별, 모니터링 및 분석, 사고 대응 및 복구, 암호화, 네트워크 및 통신 보안, 시스템 및 애플리케이션 보안 등 7개 부문에 대한 세부 항목으로 구성

[표 2-2] SSCP 검정내용

부문 (가중치, %)	세부항목
보안개념 및 관행 (16%)	• 윤리강령 준수 • 보안 개념 이해 • 보안 제어 식별 및 구현 • 기능적 보안 제어 문서화 및 유지 관리 • 자산관리 라이프사이클(예 : 하드웨어, 소프트웨어 및 데이터) 지원 및 구현 • 변경관리 라이프사이클 지원 및 구현 • 보안인식, 교육지원 및 구현(예 : 소셜 엔지니어링/피싱/인식 커뮤니케이션) • 물리적 보안(예 : 데이터 센터, 방문자 관리, 개인장치 제한)
액세스 제어 (15%)	• 인증 방법 구현 및 유지 관리 • 인터네트워크 신뢰 아키텍처 이해 및 지원 • ID 관리 라이프사이클 지원 및 구현 • 액세스 제어 이해 및 관리
위험 식별, 모니터링 및 분석 (15%)	• 위험 관리 이해 • 법률 및 규제 문제(예 : 관할권, 제한, 개인정보 보호) 이해 • 보안 평가 및 취약성 관리 활동 수행 • 보안 플랫폼 운영 및 모니터링 • 모니터링 결과 분석
사고대응 및 복구 (14%)	• 사고 대응 수명 주기를 이해하고 지원 • 법의학적 조사를 이해하고 지원 • 사업 연속성 계획 및 재해 복구 계획을 이해하고 지원

4) 한국어 시험은 2024년 4월 철수
5) https://www.isc2.org/members/cpe-opportunities
6) ISC2의 자격증을 2개 이상 받아도 1회만 납부하면 모든 자격의 유지가 가능

부문 (가중치, %)	세부항목
암호화 (9%)	• 암호화의 이유와 요구사항 이해 • 암호화 개념 적용 • 보안 프로토콜을 이해하고 구현 • 공개 키 인프라 이해
네트워크 및 통신 보안 (16%)	• 네트워크 공격(예 : DDoS, 중간자 공격(MitM), DNS 캐시 포이즈닝) 이해 • 네트워크 액세스 제어 관리 • 네트워크 보안 관리 • 네트워크 기반 보안 어플라이언스 및 서비스 작동 및 구성 • 보안 무선 통신 • 사물인터넷 보안 및 모니터링(예 : 네트워크 격리, EOL(End of Life) 관리)
시스템 및 애플리케이션 보안 (15%)	• 악성 코드 및 활동 식별 및 분석 • 엔드포인트 장치 보안 구현 및 운영 • 모바일 장치 관리 및 관리 • 클라우드 보안 이해 및 구성 • 보안 가상 환경 운영 및 유지 관리

[출처] https://www.isc2.org/

- **(응시자격)** 검정자격의 7개 부문 중 하나 이상의 부문에서 최소 1년의 경력이 필요[7)]
- **(시험시간)** 3시간
- **(합격기준)** 1,000점 만점에 700점 이상(총 125문항)
- **(응시료)** $249
- **(시험방식)** 피어슨뷰(Pearson VUE)[8)] 시험센터를 이용한 온라인 테스트
- **(응시언어)** 영어, 일본어, 스페인어
- **(자격유효기간)** 자격 취득 후 매년 135달러의 AMF를 지불하고, 자격증을 유지하기 위해서는 CPE 학점 취득이 필요

○ 클라우드 보안전문가 인증(CCSP, Certified Cloud Security Professional)

- **(목적)** 전문가가 클라우드에서 데이터, 애플리케이션, 인프라를 설계, 관리하고 보호하는 데 필요한 고급기술과 지식을 보유하고 있음을 입증
- **(검정내용)** 클라우드 개념과 아키텍처 및 디자인, 클라우드 데이터 보안, 클라우드 플랫폼 및 인프라 보안, 클라우드 애플리케이션 보안, 클라우드 보안 운영, 법률과 위험 및 규정 준수 등 6개 부문의 세부항목으로 구성

7) 컴퓨터, 정보기술(IT) 분야의 학위 또는 ISC2의 자격증으로 최대 1년의 경력을 추가할 수 있으며, 경력이 전혀 없는 경우에도 SSCP에 합격 후 ISC2 준회원이 되고 2년 이내에 경력을 쌓으면 자격인정

8) 영국에서 시작된 다국적 교육기업으로, 180개 이상의 국가 및 지역에 있는 5,500개의 Pearson VUE 시험 센터에서 다양한 국제 시험을 대행(https://www.pearsonvue.com/us/en/about.html)

[표 2-3] CCSP 검정내용

부문 (가중치, %)	세부항목
클라우드 개념, 아키텍처 및 디자인 (17%)	• 클라우드 컴퓨팅 개념 이해 • 클라우드 참조 아키텍처 설명 • 클라우드 컴퓨팅과 관련된 보안 개념 이해 • 보안 클라우드 컴퓨팅의 설계 원칙 이해 • 클라우드 서비스 제공자 평가
클라우드 데이터 보안 (20%)	• 클라우드 데이터 개념 설명 • 클라우드 데이터 저장 아키텍처 설계 및 구현 • 데이터 보안 기술 및 전략 설계 및 적용 • 데이터 검색 및 분류 구현 • 정보 권한 관리 설계 및 구현 • 데이터 보존, 삭제 및 보관 정책 계획 및 구현 • 데이터 이벤트의 감사성, 추적성 및 책임성을 설계하고 구현
클라우드 플랫폼 및 인프라 보안 (17%)	• 클라우드 인프라 구성요소 이해 • 보안 데이터 센터 설계 • 클라우드 인프라와 관련된 위험 분석 • 보안 제어 설계 및 계획 • 재해 복구 및 비즈니스 연속성 계획
클라우드 애플리케이션 보안 (17%)	• 애플리케이션 보안에 대한 교육 및 인식 제고 • 보안 소프트웨어 개발 수명 주기 프로세스 설명 및 적용 • 클라우드 소프트웨어 보증 및 검증 적용 • 검증된 보안 소프트웨어 사용 • 클라우드 애플리케이션 아키텍처의 세부 사항 이해 • 적절한 ID 및 액세스 관리 솔루션 설계
클라우드 보안 운영 (16%)	• 클라우드 환경을 위한 물리적, 논리적 인프라 구현 및 유지관리 • 운영 통제 및 표준 구현(예 : ITIL, ISO/IEC 20000-1) • 디지털 포렌식 지원 • 이해당사자와의 커뮤니케이션 관리 • 보안 작업 관리
법률, 위험 및 규정 준수 (13%)	• 클라우드 환경 내의 법적 요구 사항 및 고유한 위험 설명 • 개인정보 문제 이해 • 클라우드 환경에 필요한 감사 프로세스, 방법론 및 적응 이해 • 클라우드가 기업 위험 관리에 미치는 영향 이해 • 아웃소싱 및 클라우드 계약 설계 이해

[출처] https://www.isc2.org/

- **(응시자격)** 정보기술 분야에서 최소 5년 이상의 업무 경험이 있어야하며, 그 중 3년은 정보보호 분야에서 근무한 경력이고, 1년은 CCSP 6개 부문 중 하나 이상의 부문에서 근무한 경력이 필요[9)]
- **(시험시간)** 3시간
- **(합격기준)** 1,000점 만점에 700점 이상(총 125문항)
- **(응시료)** $599
- **(시험방식)** 피어슨뷰(Pearson VUE) 시험센터를 이용한 온라인 테스트
- **(응시언어)** 영어, 중국어, 일본어, 독일어
- **(자격유효기간)** 자격 취득 후 매년 135달러의 AMF를 지불하고, 자격증을 유지하기 위해서는 CPE 학점 취득이 필요

□ ISACA의 주요 정보보호 자격제도

- ISACA는 2020년에 설립된 독립적이고 비영리적인 글로벌 협회로, IT감사, 통제, 보안 및 거버넌스 분야의 전문가 양성을 위한 CISA, CISM, CGEIT, CRISC 등의 자격제도를 운영

- 정보시스템 감사 인증(CISA, Certified Information Systems Auditor)
  - **(목적)** 전문가가 클라우드에서 데이터, 애플리케이션, 인프라를 설계, 관리하고 보호하는 데 필요한 고급기술과 지식을 보유하고 있음을 입증
  - **(검정내용)** 정보시스템 감사 프로세스, IT 거버넌스 및 관리, 정보시스템 개발 및 구현, 정보시스템 운영 및 비즈니스 회복력, 정보 자산 보호, 5개 직무 부문의 실무를 포괄하는 문제로 구성

[표 2-4] CISA 검정내용

부문	가중치	내용
정보시스템 감사 프로세스	18%	조직이 정보시스템을 보호하고 통제하는 데 필요한 IT 감사 표준에 따라 조직의 정보보호, 위험 및 통제 솔루션의 상태에 대한 신뢰성을 확인
IT 거버넌스 및 관리	18%	이해관계자들에게 중요한 문제를 식별하고 정보 및 관련 기술의 거버넌스를 보호하기 위한 조직의 전략을 지원
정보시스템 개발 및 구현	12%	IT 통제에 대한 역량을 증명하고, IT와 비즈니스의 관계에 대해 이해
정보시스템 운영 및 비즈니스 회복력	26%	
정보 자산 보호	26%	사이버보안의 원칙, 모범 사례 및 함정을 이해

[출처] https://www.isaca.org/

9) 컴퓨터, 정보기술(IT) 분야 학위 또는 ISC2의 자격증으로 최대 1년의 경력을 추가할 수 있으며, 경력이 전혀없는 경우에도 CCSP 시험에 합격하여 ISC2 준회원이 된 후 2년 이내에 경력을 쌓으면 자격인정

- **(응시자격)** 최소 5년 이상의 IS/IT 감사, 통제, 보증 또는 보안 경력이 필요하며, 최대 3년의 경력은 학위나 다른 인증(CISSP, CISM 등)으로 대체 가능
- **(시험시간)** 4시간(240분)
- **(합격기준)** 800점 만점에 450점 이상(총 150문항)
- **(응시료)** $575(ISACA 회원), $760(ISACA 비회원)
- **(시험방식)** 컴퓨터 기반 테스트(CBT, Compulsory basic training)이며, 전세계 공인 PSI 시험센터[10] 또는 원격감독시험으로 실시
- **(응시언어)** 한국어, 영어, 스페인어, 프랑스어, 독일어, 일본어, 중국어
- **(자격유효기간)** CISA 자격을 유지하려면 연간 유지관리 수수료 45달러(비회원은 85달러)를 지불하고, 매년 최소 20개의 CPE를 취득하고 3년 동안 총 120개의 CPE 취득이 필요[11]

○ 정보보호 관리자 인증(CISM, Certified Information Security Manager)

- **(목적)** 위험을 평가하고, 효과적인 거버넌스를 구현하고, 사고에 적극적으로 대응하는 능력을 확인
- **(검정내용)** 정보 보안 거버넌스, 정보 보안 위험 관리, 정보 보안 프로그램, 사고 관리 등 4개 직무 부문의 실무를 포괄하는 문제로 구성

[표 2-5] CISM 검정내용

부문	가중치	내용
정보보호 거버넌스	17%	기업 거버넌스 문화, 규정 및 구조에 대한 통찰력을 제공하고 정보보호 전략을 분석, 계획 및 개발하여, 이해관계자에게 신뢰성을 제공
정보보호 위험관리	20%	잠재적인 정보보호 위험, 위협 및 취약성을 분석하고 식별할 수 있는 역량을 제공
정보보호 프로그램	33%	보안 제어, 테스트, 커뮤니케이션, 보고 및 구현을 포함하여 정보 보안 프로그램을 관리할 수 있는 역량을 제공
사고관리	30%	비즈니스가 사고에 대응하고 복구를 안내할 수 있도록 준비하는 방법을 포함하여 위험 관리 및 준비에 대한 심층적인 교육을 제공

[출처] https://www.isaca.org/

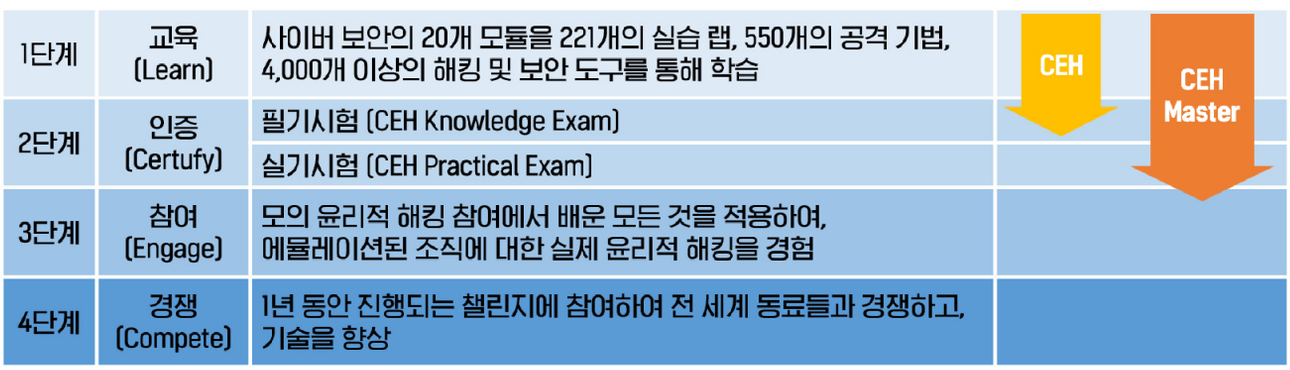
10) 글로벌 교육 솔루션 기관으로, CISA를 포함하여 토익, 토플, 등 다양한 온라인 테스트를 지원
11) 컨퍼런스, 학습, 자원봉사 등 다양한 방안을 제공(https://www.isaca.org/credentialing/cisa/maintain-cisa-certification)

- **(응시자격)** 최소 3년 이상의 IT 위험 관리 및 IS 통제 경력이 필요하며, 경력 면제 또는 대체는 불가능
- **(시험시간)** 4시간(240분)
- **(합격기준)** 800점 만점에 450점 이상(총 150문항)
- **(응시료)** $575(ISACA 회원), $760(ISACA 비회원)
- **(시험방식)** CBT 방식이며, 전세계 공인 PSI 시험센터 또는 원격감독시험으로 실시
- **(응시언어)** 한국어, 영어, 스페인어, 중국어
- **(자격유효기간)** CISM 자격을 유지하려면 연간 유지관리 수수료 45달러(비회원은 85달러)를 지불하고, 매년 최소 20개의 CPE를 취득하고 3년 동안 총 120개의 CPE 취득이 필요

□ EC-Council[12]의 주요 정보보호 자격제도

- EC-Council은 미국의 911테러 이후, 같은 공격이 사이버 상에서 가해진다면 위협적이라는 판단 하에 설립된 민간기관으로, CEH, ENSA, CHFI, EDRP, ECSA 등 다양한 정보보호 자격제도를 시행
- 윤리적 해커 인증(CEH, Certified Ethical Hacker)
  - **(목적)** 사이버 범죄자가 사용하는 다중플랫폼 전략과 전술을 학습하고 업계에서 즉시 활용할 수 있는 기술을 습득하여 범죄자가 시스템 취약점을 파악하기 전에 취약점을 파악
  - **(검정내용)** 사이버 보안을 20개 모듈로 구분하여, 교육부터 이어지는 4단계 프레임워크에 따라 실제 시나리오를 활용한 교육과 실습

[그림 2-1] CEH 교육 프레임워크



[출처] https://iclass.eccouncil.org/

12) 국제 전자상거래 컨설턴트 협의회(EC-Council, International Council of E-Commerce Consultants)

[표 2-6] CEH 검정내용(20개 모듈)

모듈	내용
윤리적 해킹 소개	윤리적 해킹의 기본, 정보보안 통제, 관련법률, 표준절차 등
풋프린팅과 정찰	윤리적 해킹의 중요한 사전공격 단계인 풋프린트 추적 및 정찰을 수행
네트워크 스캐닝	다양한 네트워크 스캐닝 기술과 대책
목록 (enumeration)	경계 경로 프로토콜(BGP, Border Gateway Protocol), 네트워크 파일공유(NFS, Network File Sharing) 등의 악용사례와 관련 대책
취약성분석	대상 조직의 네트워크, 통신인프라, 앤드시스템에서 보안허점을 식별
시스템해킹	스테가노그래피(Steganography), 스테가노 분석 공격, 흔적 지우는 방법 등 시스템 및 네트워크 취약성을 발견하는데 사용되는 다양한 해킹 방법론
멀웨어 위협	트로이 목마, 바이러스. 웜 등 다양한 유형의 멀웨어, APT 및 파일리스 멀웨어, 멀웨어 분석 절차, 멀웨어 대책 등
스니핑	패킷 스니핑 기술과 이를 활용한 네트워크 취약점 발견 방법, 스니핑공격에 대한 방어책
사회공학	도난시도 식별, 인적 수준의 취약성 검사, 사회공학 대책 등
서비스거부	서비스 거부(DoS, Denial-of-Service) 및 분산 서비스 거부(DDoS, Distributed Denial of Service) 공격기법
세션 하이재킹	네트워크 수준의 세션관리, 인증, 권한부여, 암호화 취약점과 관련 대책을 발견하는데 사용되는 다양한 세션 하이재킹 기술
IDS, 방화벽 및 허니팟 회피	방화벽, 침입탐지시스템(IDS, Intrusion Detect System), 허니팟 회피기술, 네트워크 경계의 취약점을 감사하는데 사용되는 도구 및 대책
웹서버 해킹	웹 서버 인프라의 취약성을 감사하고 대응책을 마련하는데 사용되는 포괄적인 공격방법론
웹 애플리케이션 해킹	웹 애플리케이션의 취약성과 대응책을 감사하는데 사용되는 포괄적인 웹 애플리케이션 해킹방법론
SQL 인젝션	SQL 인젝션 공격기술, 회피기술 및 SQL 인젝션 대책
무선 네트워크 해킹	무선 네트워크에 대한 다양한 유형의 암호화, 위협, 해킹방법론, 해킹도구, 모안도구 및 대책
모바일 플랫폼 해킹	모바일 플랫폼 공격 벡터, 안드로이드 및 IOS 해킹, 모바일 기기 관리, 모바일 보안지침 및 보안도구
IoT 및 OT 해킹	다양한 유형의 사물인터넷(IoT, Internet of Things)과 운영기술(OT, Operation Technology) 공격, 해킹방법론, 해킹도구와 대책
클라우드 컴퓨팅	컨테이너 기술, 서버리스 컴퓨팅 등 다양한 클라우드 컴퓨팅 위협, 공격, 해킹방법론, 클라우드 보안 기술 및 도구
암호화	암호화 알고리즘, 암호화 도구, 공개키인프라(PKI, public key infrastructure), 이메일 암호화, 디스크 암호화, 암호화 공격 및 암호 분석 도구

[출처] https://iclass.eccouncil.org/

- **(응시자격)** 최소 2년의 IT 보안 분야 경험을 추천하며, 경력이 없다면 EC-Council에서 제공하는 기초 강의를 먼저 수강할 것을 권고
- **(인증시험)** 필기시험으로 CEH 자격증을 취득할 수 있으며, 실기시험까지 통과할 경우 CEH Master 자격

[표 2-7] CEH 인증시험

	필기 (CEH Knowledge Exam)	실기 (CEH Practical Exam)
시험시간	4시간	6시간
시험문항	125문항	20개 도전과제
시험방식	온라인 시험 (ECC 시험센터와 Pearson Vue 시험센터)	가상환경을 통한 테스트 (EC-Council iLabs[13] 활용)
합격기준[14]	60% ~ 85%	60% ~ 85%

[출처] https://iclass.eccouncil.org/

- **(응시료)** 교육 프레임워크의 어느 단계까지 할 지, 또는 어떤 교육방식을 선택하는지에 따라 차등
- **(응시언어)** 영어
- **(자격유효기간)** 연간 수수료 80달러를 지불하고, 인증 후 3년 동안 EC-Council 지속 교육(ECE, EC-Council Continuing Education)에서 120학점이 필요

○ 최고 정보보안책임자 인증(CCISO, Certified Chief Information Security Officer)

- **(목적)** 정보보호 최고 경영진 수준에서 필요한 감사, 거버넌스, IS 통제, 인적자원 관리, 전략적 프로그램 개발 등 정보보호 프로그램을 이끄는 데 필수적인 전문 지식을 결합
- **(검정내용)** 거버넌스 및 위험관리와 규정 준수, 정보보호 제어 및 감사관리, 보안 프로그램 관리 및 운영, 정보보호 핵심역량, 전략적 계획, 재무, 조달 및 제3자 관리 등 5개 부문의 세부내용으로 구성

13) EC-Council에서 운영하는 해킹, 침투테스트, 컴퓨터 포렌식, 보안코딩 등을 위한 가상환경을 제공하는 사이트 (https://ilabs.eccouncil.org/)
14) 다양한 문제유형을 제공하며, 이용자가 어떤 문제유형을 선택하는지에 따라 합격기준 점수에 차이

[표 2-8] CCISO 검정내용

부문	내용	
거버넌스, 위험, 규정준수	거버넌스	• 정보보안 거버넌스 프로그램의 정의, 구현, 관리 및 유지 • 조직의 목표에 따라 정보보호 거버넌스 프레임워크를 조정 • 정보보호 관리체계 구축 • 정보보호 거버넌스 모니터링을 위한 프레임워크를 구축 • 정보보호 거버넌스의 표준, 절차, 지침, 정책, 규정 및 법적 문제 • 기업 정보보호 규정 준수 프로그램
	위험관리	• 위험 관리 프로그램 정책 및 헌장 작성 • 위험성 평가 방법론 및 프레임워크 생성 • 위험 등록부를 생성하고 관리 • 위험 평가 일정 및 체크리스트 작성 • 위험 보고 지표 및 프로세스 생성
	규정준수	• 조직에 적용되는 법률, 규정, 표준, 모범 사례, 조직 윤리를 분석 • ISO 27000 및 31000 등 국제 보안 및 위험 표준 • 규제 위험을 줄이기 위한 정보보호 전략, 계획, 정책 및 절차 • 규제 정보보호 조직과 산업 그룹 및 이해관계자의 중요성 • 정보보호 규정준수 프로세스 및 절차, 감사, 인증 프로그램 • 정보 보안 준수 프로세스 및 절차 • 규정 준수 프로그램을 편집, 분석 및 보고 • 규정 준수 감사 및 심사 프로그램 • 조직 윤리
정보 보안 제어 및 감사 관리	정보보안 관리제어	• 조직의 운영 프로세스와 목표를 파악 • 운영의 필요와 목표에 따라 정보시스템 제어를 설계하고 구현 • 정보시스템 제어를 구현하고 유지하는 데 필요한 리소스를 식별 • 위험을 완화하기 위한 정보시스템 제어를 설계하고 구현 • 정보보호 통제를 설계하고 테스트를 수행 • 오류가 적시에 기록, 분석, 해결되도록 프로세스 설계 및 구현 • 정보시스템 제어 프로세스 자동화를 위한 도구와 기술을 평가 • 보안 제어 구현 및 효과 측정, 관리 및 보고
	감사관리	• IT 감사 프로세스와 IT 감사 표준 • 위험 기반 IT 감사 전략을 설계하고 구현 • 확립된 표준에 따라 감사 프로세스를 실행 • 감사 결과를 평가 • 비효율적이거나 누락된 통제로 인해 발생하는 노출을 평가 • IT 감사 문서화 프로세스를 개발 • 감사 결과에 따른 필요한 변경 사항을 적시에 효과적으로 구현
보안 프로그램 관리 및 운영	보안 프로그램 관리	• 조직 목표 따른 프로젝트 범위 설명서를 개발 • 정보시스템 프로그램 활동을 정의하고, 일정 및 인력 계획 • 정보보안 프로젝트를 확보, 개발 및 관리 • 명확한 정보 보안 인력 업무 기능을 할당하고 교육을 제공 • 정보보호 인력을 배치하고 커뮤니케이션과 팀 활동계획을 수립
	보안 프로그램 운영	• 시간, 비용, 품질 제약 내에서 인력 및 팀워크 문제 해결 • 공급업체 계약 및 커뮤니티를 식별, 협상 및 관리

부문	내용	
		• 조직의 위험을 관리하고 프로젝트 관리 관행 및 통제를 평가 • 정보 시스템 프로젝트의 효과를 측정하는 계획을 개발
정보보호 핵심역량	접근제어	• 접근제어에 대한 기준을 식별하고 접근제어 계획을 설계 및 구현 • 신분증 및 생체 인식 등의 접근제어 시스템을 식별
	사회공학, 피싱, 신원도용	• 사회공학 공격에 대응하기 위한 모범 사례를 개발 • 신원 도용 사건에 대한 대응 계획을 설계 • 피싱 공격을 극복하기 위한 계획을 식별하고 설계
	물리적 보안	• 물리적 보안을 위한 표준, 절차, 지침, 정책, 규정, 법률을 식별 • 조직 보안을 위해 물리적 보안 계획을 설계, 구현 및 관리
	재해복구 및 비즈니스 연속성	• 중단 이벤트 발생 시 비즈니스 연속성, 비즈니스 복구, 비상 계획 및 재해 복구 계획을 개발, 구현 및 모니터링 • 위험을 관리하기 위한 비상 계획, 운영 및 프로그램 • 연속성 운영 계획에 정보보호 요구사항을 통합
	방화벽, IDS/IPS 및 네트워크 방어	• 조직의 정보보호를 위한 침입 탐지 및 방지 시스템을 식별 • 방화벽을 모니터링하고 방화벽 구성 문제를 식별 • 그리드 센서 및 라우터, 방화벽 등 경계 방어 시스템을 이해 • 하드웨어 및 소프트웨어에 대한 모니터링, 테스트 및 문제 해결 • 계정, 네트워크 권한, 시스템 및 장비에 대한 액세스 관리
	무선보안	• 무선 네트워크와 관련된 취약성 및 공격을 식별
	바이러스 및 악성코드	• 바이러스, 트로이 목마 및 멀웨어의 위협을 평가 • 바이러스, 트로이목마 및 멀웨어에 대처하기 위한 프로세스를 개발
	보안코딩 및 웹 애플리케이션 보안	• 보안코딩 원칙 및 시스템개발 수명주기에 따라 소프트웨어 보증 프로그램을 개발하고 유지관리 • 소프트웨어 취약성 분석 기술을 이해 • 프로그램 코드를 손상시키지 않고 IT 시스템을 설치, 운영 • 웹 애플리케이션 취약점과 공격을 식별하고 공격에 대응
	OS 강화	• OS 취약점과 공격을 식별하고 OS 시스템 강화 계획을 개발 • 정보시스템 보안을 위한 시스템 로그, 패치 관리 프로세스
	암호화 기술	• 암호 시스템의 다양한 구성 요소를 식별 • 정보보안 암호화 기술에 대한 계획을 개발
	취약성 평가 및 침투 테스트	• 침투 테스트 프로그램을 설계, 개발 및 구현 • 관련된 정보시스템 및 법적문제와 관련된 취약성을 식별 • 펜 테스트 보고 및 기술적 취약성 수정 구현을 위한 계획 개발 • 취약성 관리 시스템 개발
	위협관리	• 위협관리 프로그램을 만들고 관리
	사고 대응 및 컴퓨터 포렌식	• 잠재적인 보안 위반을 평가하고 영향을 평가하며 증거를 보존 • 사고대응 절차 설계 • 다양한 포렌식 조사 도구 구성 및 사용 • 포렌식 방지 기술 설계

부문	내용	
정보보호 핵심역량	애플리 케이션 보안	• 보안 SDLC 모델 • 개발, 테스트 및 프로덕션 환경 분리 • DevSecOps • 폭포수 방법론 및 보안 • Agile 방법론 및 보안 • 애플리케이션 강화 및 보안 기술 • 데이터베이스 보안 및 강화
	가상화 보안	• 가상화 개요 및 위험 • 가상화 보안 문제와 보안 제어
	클라우드 컴퓨팅 보안	• 보안 및 복원력 클라우드 서비스 • 클라우드 보안 제어 • 클라우드 컴퓨팅 보호 고려 사항
전략적 계획, 재무, 조달 및 제3자 관리	전략적 계획	• 엔터프라이즈 정보보호 아키텍처를 설계, 개발 및 유지 관리 • 조직의 목표에 맞춘 정보보호 프로그램을 개발 • 조직의 목표를 이해하기 위해 이해관계자를 파악하고 협의 • 정보 보안 프로그램의 역할에 대한 전략 계획을 정의 • 핵심 성과 지표를 정의하고 지속적으로 효과를 측정 • 전략 활동을 모니터링하고 업데이트
	재무, 조달	• 보안 부서의 운영 예산을 분석, 예측 및 개발 • 정보보호 계획의 이행 및 관리를 위한 자원을 확보하고 관리 • 정보보호 프로젝트의 비용관리, 투자 수익률을 모니터링하고 감독 • 재부 지표를 식별하여 이해관계자에게 보고 • 기업의 보안 우선순위에 따라 IT 보안 투자 포트폴리오의 균형 • 비즈니스 영향 분석을 수행 • 정보시스템 조달 전략을 식별하고 비용 편익 분석 • 목표명세서, 작업명세서, 총 소유비용 등 기본 조달 개념을 이해 • 다양한 이해 관계자 와 협력하여 IT 보안 제품 및 서비스 조달 • 인수 계획, 비용 견적, 작업 설명서, 서비스 수준 계약 및 기타 관련 조달문서에 위험기반 보안 요구 사항을 포함 • 디자인 공급업체 선정 프로세스 및 관리 정책 • 조달되는 IT 및 소프트웨어의 보안 평가를 위한 계약 관리 정책 • 조달의 주요 목표를 측정, 보고하기 위한 표준 개발 • 작업 설명서 및 기타 조달 문서에 IT 보안 요구 사항을 이해
	제3자 관리	• 제3자 관리 정책, 측정항목 및 프로세스 설계 • 조달의 주요 목표를 측정하고 보고하기 위한 표준 개발 • 기업의 조달 문서에 위험 기반 보안 요구 사항을 포함 • 작업 명세서 및 기타 조달 문서에 보안, 개인정보 보호규정 준수

[출처] https://iclass.eccouncil.org/

- **(응시자격)** CCISO 5개 검정부문 각각에서 5년의 경력이 필요하며, 시험 전 교육에 참여할 경우에는 3개 부문에서 5년의 경력이 필요
- **(시험시간)** 2시간 30분
- **(합격기준)** 60% ~ 85%(총 150문항)
- **(응시료)** 교육 프레임워크의 어느 단계까지 할 지, 또는 어떤 교육방식을 선택하는지에 따라 차등
- **(시험방식)** 온라인 시험(ECC 시험센터와 Pearson Vue 시험센터)
- **(응시언어)** 영어
- **(자격유효기간)** 연회비 100달러를 지불하고, 매년 최소 20개의 CPE를 취득하고 3년 동안 총 120개의 CPE 취득이 필요

□ 아마존, AWS(Amazon Web Services) Certification

- **AWS는 아마존에서 제공하는 클라우드 컴퓨팅 플랫폼으로, 아마존은 자사의 클라우드 서비스에 필요한 기술적 스킬과 전문지식을 검증하기 위한 자격제도를 운영**
  - 주요 클라우드 직무 내용과 경력에 따라 자격을 구분하여 운영하고 있으며, 자신의 직무에 따라 다양한 경로의 자격증 취득 가능

[표 2-9] AWS 자격제도

AWS 자격제도		내용
기초 (Foundational)	AWS 클라우드 실무자 인증 (Certified Cloud Practitioner)	AWS 클라우드 서비스 및 클라우드 컴퓨팅에 대한 기초 지식
	AWS AI 실무자 인증 (Certified AI Practitioner)	인공 지능, 머신러닝, 생성형 AI 개념 및 사례에 대해 검증
초급 (Associate)	AWS SysOps 관리자 인증 (Certified SysOps Administrator)	AWS에서 워크로드를 배포, 관리, 운영하는 데 필요한 기술 능력 검증
	AWS 개발자 인증 (Certified Developer)	AWS 클라우드 기반 개발, 테스트, 배포, 디버깅 등에 필요한 기술 숙련도 검증
	AWS 초급 솔루션 설계자 인증 (Certified Solutions Architect)	AWS 서비스 전반에서 기술 지식과 기술 능력 검증
	AWS 데이터 엔지니어 인증 (Certified Data Engineer)	데이터 모델 설계, 관리, 데이터 품질 보장에 대한 능력 검증
	AWS 머신러닝 엔지니어 인증 (Certified Machine Learning Engineer)	ML 워크로드를 구현하고 운영하는 데 필요한 기술 능력을 검증

AWS 자격제도		내용
중급 (Professional)	AWS 중급 솔루션 설계자 인증 (Certified Solutions Architect)	보안, 비용 및 성능을 최적화하고, 프로세스를 자동화하기 위한 고급 지식 및 기술
	AWS DevOps 엔지니어 인증 (Certified DevOps Engineer)	AWS 플랫폼에서 분산 애플리케이션 시스템을 프로비저닝, 운영 및 관리
고급 (Specialty)	AWS 고급 네트워킹 (Certified Advanced Networking)	클라우드 이니셔티브 구현에 중요한 기술을 갖춘 인재를 식별하고 개발
	AWS 보안 인증 (Certified Security)	AWS 클라우드에서 보안 솔루션을 만들고 구현하는 데 필요한 전문성을 검증
	AWS 머신러닝 인증 (Certified Machine Learning)	클라우드 이니셔티브 구현에 중요한 기술을 갖춘 인재를 식별하고 개발

[출처] https://aws.amazon.com/

- 전체 자격제도에서 보안에 대한 내용은 포함되어 있으나, AWS보안에 대한 주요 자격증은 AWS 보안인증(Certified Security)이라고 볼 수 있음
- AWS 보안인증(Certified Security)은 전체 AWS 자격증에서 심화과정으로 분류되며, 필수는 아니지만 시험에 응시하기 전에 AWS 초급 솔루션 설계자 인증(Certified Solutions Architect- Associate)과 AWS 중급 솔루션 설계자 인증(Certified Solutions Architect - Professional)을 취득할 것을 권고

AWS 보안인증 자격(Certified Security)

- **(검정내용)** 위협감지 및 사고대응, 보안로깅 및 모니터링, 인프라 보안, ID 및 엑세스 관리, 데이터 보호, 관리 및 보안 거버넌스 등 6개 부문의 세부내용으로 구성

[표 2-10] AWS 보안인증 검정내용

부문	가중치	내용
위협감지 및 사고대응	14%	• 인시던트 대응 계획 설계 및 구현 • AWS 서비스를 사용하여 보안 위협 및 이상 감지 • 손상된 리소스 및 워크로드에 대응
보안로깅 및 모니터링	18%	• 보안 이벤트 해결을 위한 모니터링 및 경고 설계 및 구현 • 보안 모니터링 및 알림 문제를 해결 • 로깅 솔루션을 설계하고 구현

부문	가중치	내용
인프라 보안	20%	• 엣지 서비스를 위한 보안 제어의 설계 및 구현 • 네트워크 보안 제어 설계 및 구현 • 컴퓨팅 워크로드에 대한 보안 제어의 설계 및 구현 • 네트워크 보안 문제 해결
ID 및 엑세스 관리	16%	• AWS 리소스 인증의 설계, 구현 및 문제 해결 • AWS 리소스 권한 부여의 설계, 구현 및 문제 해결
데이터 보호	18%	• 전송 중인 데이터에 기밀성과 무결성을 제공하는 제어의 설계 및 구현 • 저장된 데이터에 기밀성과 무결성을 제공하는 제어의 설계 및 구현 • 저장된 데이터의 수명 주기를 관리하기 위한 제어의 설계 및 구현
관리 및 보안 거버넌스	14%	• AWS 계정을 중앙에서 배포하고 관리하기 위한 전략의 개발 • AWS 리소스의 규정 준수 평가 • 아키텍처 검토 및 비용 분석을 통해 보안 허점 식별

[출처] https://aws.amazon.com/

- **(응시자격)** 보안 솔루션의 설계 및 구현 분야에서 최소 3년의 경험이 있어야 하며, AWS 워크로드 보안에 대해 최소 2년의 실무 경험
- **(시험시간)** 170분
- **(합격기준)** 1,000점 만점에 합격 최소 점수는 750점
- **(응시료)** $300
- **(시험방식)** Pearson VUE 테스트 센터 또는 온라인 감독 시험.
- **(응시언어)** 한국어, 영어, 스페인어, 포르투갈어, 일본어, 중국어
- **(자격유효기간)** 자격은 3년 동안 유효하며, 유효기간 내에 AWS 클라우드 실무자 재인증 교육(AWS Cloud Quest : Recertify Cloud Practitioner)[15]을 완료하거나, 자격증의 최신버전 시험에 합격하면 자격기간이 연장

15) 별도의 재시험 없이 실습을 통해 AWS의 심화과정을 배울 수 있는 교육과정(https://explore.skillbuilder.aws/learn/course/external/view/elearning/17623/aws-cloud-quest-recertify-cloud-practitioner)

□ Microsoft, **Microsoft Certifications**

- Azure는 Microsoft에서 만든 클라우드 컴퓨팅 플랫폼 및 인프라스트럭처 서비스이며, 직무에 따라 필요한 다양한 기술을 검증하여 직무기반 기술의 신뢰성을 높일 수 있는 MS 인증(Microsoft Certifications)을 제공
  - 직무 내용과 경력에 따라 다양한 인증을 제공하고 있으며, 원하는 직무에 따라 필요한 자격증을 취득하는 방식

[표 2-11] MS의 정보보호 분야 자격제도

구분	자격증명	제품군	레벨	직군
기본 (Fundamentals)	보안, 규정 준수 및 ID 기본 (Security, Compliance, and Identity Fundamentals)	Azure	초급 (Beginner)	보안 엔지니어
직무기반 (Role-based)	Azure 보안 엔지니어 (Azure Security Engineer Associate)	Azure	중급 (Intermediate)	보안 엔지니어
	ID 및 액세스 관리자 (Identity and Access Administrator Associate)	Azure	중급 (Intermediate)	보안 엔지니어
	보안 운영 분석가 (Security Operations Analyst Associate)	Azure	중급 (Intermediate)	보안운영 분석가
	정보 보호 및 규정 준수 관리자 (Information Protection and Compliance Administrator Associate)	Microsoft 365	중급 (Intermediate)	보안 엔지니어
	사이버 보안 설계자 전문가 (Cybersecurity Architect Expert)	Microsoft Defender	고급 (Advanced)	관리자

[출처] https://aws.amazon.com/

  - 고급과정인 사이버 보안 설계자 전문가(Cybersecurity Architect Expert) 자격을 얻기 위해서는 Azure 보안엔지니어, ID 및 액세스 관리자, 보안 운영 분석가 중 하나의 자격을 사전에 취득할 필요

- **Azure 보안 엔지니어**(Azure Security Engineer Associate) 자격
  - **(검정내용)** ID 및 액세스 관리, 보안 네트워킹, 컴퓨팅, 스토리지 및 데이터베이스 보호, 보안 작업 관리 등 4개 부문의 세부 항목으로 구성

[표 2-12] AWS 보안인증 검정내용

부문	내용
ID 및 액세스 관리	• Microsoft Entra ID에서 ID 관리 • Microsoft Entra ID를 사용하여 인증 및 권한부여 관리 • Microsoft Entra ID에서 애플리케이션 액세스 관리
보안 네트워킹	• 가상 네트워크에 대한 보안 계획 및 구현 • Azure 리소스에 대한 프라이빗 액세스 보안 계획 및 구현 • Azure 리소스에 대한 공용 액세스 보안 계획 및 구현
컴퓨팅, 스토리지 및 데이터베이스 보호	• 컴퓨팅을 위한 고급 보안 계획 및 구현 • 스토리지 보안 계획 및 구현 • Azure SQL Database 및 Azure SQL Managed Instance에 대한 보안 계획 및 구현
보안 운영 관리	• 클라우드용 Microsoft Defender를 사용하여 보안 태세 관리 • 클라우드용 Microsoft Defender를 사용하여 위협 방지 구성 및 관리 • 보안 모니터링 및 자동화 솔루션 구성 및 관리

[출처] https://aws.amazon.com/

  - **(응시자격)** 필수 경력요건은 없으나, 기초레벨인 Azure 기본인증(Azure Fundamentals) 자격을 먼저 취득할 필요
  - **(시험시간)** 100분
  - **(합격기준)** 1,000점 만점에 700점
  - **(응시료)** $115
  - **(시험방식)** Pearson Vue를 통해 예약
  - **(응시언어)** 한국어, 영어, 독일어, 프랑스어, 스페인어, 포르투갈어, 아랍어, 러시아어, 이탈리아어, 인도네시아어, 일본어, 중국어
  - **(자격유효기간)** 12개월간 유효하며, 온라인 갱신평가를 통해 기간 연장

2. 영국

□ 민간기관 중심으로 운영하고 정부기관에서 자격제도를 인증

- **민간 교육기관인 UKPDA와 NCFE에서 사이버보안 관련 자격제도를 시행**
  - 영국 전문개발 아카데미(**UKPDA**, UK Professional Development Academy)는 원격학습 및 전문 교육과정을 제공하는 영국의 온라인 아카데미
  - **NCFE**[16]는 학습자는 누구도 뒤쳐져서는 안된다는 목표에 따라 1848년부터 이어져 내려온 교육 자선 단체
- **영국의 자격 및 시험 규제기관(Ofqual, Office of Qualifications and Examinations Regulation)[17]에서 관련 자격, 시험 및 평가를 규제**
  - Ofqual의 자격은 공식적이며, 교육 및 취업 훈련을 목적으로 자격제도를 9개 자격수준(qualification levels)으로 분류

[표 2-13] Ofqual의 자격수준

레벨	내용
입문	입문레벨 기술, 입문레벨 자격증(entry level certificate, entry level diploma)
레벨1	GCSE[18] 1~3학년, 초급견습과정, 1급 국가직업자격, 레벨1 자격증(level1 certificate, level1 diploma)
레벨2	GCSE 4~9학년, 중급견습과정, 2급 국가자격증, 레벨2 자격증(level2 certificate, level2 diploma)
레벨3	A레벨[19], 고급견습과정, 3급 국가자격증, 레벨3 자격증(level3 certificate, level3 diploma)
레벨4	고등교육 증명서, 상위국가자격증, 레벨4 자격증(level4 certificate, level4 diploma)
레벨5	고등교육 졸업장, 고등국가학위, 레벨5 자격증(level5 certificate, level5 diploma)
레벨6	일반 학사학위, 대학 졸업장, 레벨6 자격증(level6 certificate, level6 diploma)
레벨7	석사학위, 대학원 졸업장,, 레벨7 자격증(level7 certificate, level7 diploma)
레벨8	박사학위, 레벨8 자격증(level8 certificate, level8 diploma)

[출처] https://www.gov.uk/government/organisations/ofqual

16) 원래 명칭은 북부 고등교육 위원회(Northern Council for Further Education) 였으나, 1990년대 초 법인화 과정에서 조직의 이름이 적절하지 않다는 판단 하에 약어를 포기하지 않고 NCFE로만 표기
17) https://www.gov.uk/government/organisations/ofqual
18) GCSE(General Certificate of Secondary Education)는 영국 학생들이 중등학교를 졸업하면서 치르는 자격시험
19) 고등교육과정까지 모두 마친 영국 학생이 치르는 대학입학시험레벨

- 자격제도의 인증 기준은 아래의 4가지[20)]

  • **(정체성, 규정 및 거버넌스)** 영국에서 설립되고 운영되는지 여부와 운영 규정 및 거버넌스 등

  • **(무결성)** 조직과 고위 직원이 자격증을 공정하고 무결하게 개발, 제공하고 수여하는지 여부

  • **(자원 및 자금조달)** 사업 계획과 3년분의 재무 예측을 포함하여 자격을 개발, 제공 및 관리하는 데 필요한 시스템, 프로세스, 리소스 및 재정이 갖춰져 있다는 증거

  • **(역량)** 지속적으로 유효한 자격증을 개발하고 제공하는 데 필요한 적절한 수준의 역량을 갖추고 있는지 여부

o Ofqual 자격 외에는 CPD 자격인증(Step Ahead CPD Qualifications)[21)] 등 개별기관에서 지속적인 전문성 개발(CPD, Continuing Professional Development) 인증이 가능

- CPD 자격인증은 CPD 제공자의 품질 보증을 검토하고 인정하여 독립적인 CPD 인증을 제공
- 인증 운영기관에게 아래의 항목에 대한 평가를 통해 CPD를 인증
  - 평가정책
  - 항소 및 불만 처리 정책
  - 부정행위, 부정행정 및 표절 정책
  - 데이터 보호 정책
  - 평등, 다양성 및 포용 정책
  - 건강 및 안전 정책
  - 내부 품질 보증 정책
  - 직원 개발 정책

□ 영국 전문개발 아카데미(**UKPDA**, UK Professional Development Academy)

o UKPDA는 사이버 보안을 포함한 다양한 분야의 CPD 인증과 ofqual 인증을 제공

- 사이버보안 분야는 CPD 인증으로 제공하고 있으며, IT 보안, 사이버 보안, 운영 및 사이버 보안 관리, 사이버 보안 인증서 등 4개 자격제도를 시행 중
- 각 자격제도는 일정시간 학습 후 자격시험을 통해 증명서를 발급해주는 형태

20) https://www.gov.uk/government/publications/application-for-recognition-supporting-information/supporting-information-application-for-recognition#the-general-conditions-of-recognition
21) https://stepaheadcpd.co.uk/

○ UKPDA의 사이버보안 분야 자격제도

- **(시험방식 및 합격기준)** 교육이 끝난 후 온라인 객관식 시험을 치르게 되며, 합격점수는 75%
- **(응시언어)** 교육 및 자격시험은 영어로만 제공

[표 2-14] UKPDA의 사이버보안 분야 자격제도

자격 명	레벨	검정내용	응시료
사이버 보안 인증 (Cyber Security Certificate in Cyber Security)	초보자 과정	• 사이버 보안 기본 사항 • 멀웨어의 종류 • 사이버 보안 침해 • 사이버 공격의 종류 • 모바일 보호 • 소셜 네트워크 보안 • 예방 소프트웨어 • 중대한 사이버 위협 • 해커에 대한 방어	교육 : £49 PDF 인증서 발급 : £29
IT 보안 (Level 3 Diploma in IT Security)	3단계 전문가레벨	• 사이버 보안 • 디지털 시민권 • 감성 지능 • 위험 평가 및 관리	교육 : £149 PDF 인증서 발급 : £37
사이버 보안 (Level 3 Diploma in Cyber Security)	3단계 전문가레벨	• 사이버 보안 • 디지털 시민권 • 감성 지능 • 위험 평가 및 관리 • Microsoft Office	교육 : £149 PDF 인증서 발급 : £37
운영 및 사이버 보안 관리 (Level 5 Diploma in Operations and Cyber Security Management)	5단계 전문가 레벨	• 공급망 관리 • 인적자원 관리 • 스트레스 관리 • 위험 평가 및 관리 • 프로젝트 관리 • 성과 관리 • 협상 기술	교육 : £249 PDF 인증서 발급 : £42

[출처] https://ukpdacademy.co.uk/

□ NCFE

○ NCFE는 교육 자선단체로, 업계 전문가 팀을 통해 제공되는 맞춤형 프로그램과 더불어 Ofqual이 규제하는 1,000개 이상의 자격증을 보유

- 14세 이상의 청소년을 위한 기술교육 프로그램이나, 성인의 직업교육을 다양한 분야를 통해 지원
- 입문자를 위한 필수 디지털 기술부터 해당 분야에서 경력을 쌓고자 하는 사람을 위한 사이버 보안, 코딩, UX/UI까지, 다양한 레벨의 디지털 자격증을 지원

NCFE의 사이버보안 분야 자격제도

- **(시험방식 및 합격기준)** 검정과목의 학점을 모두 이수하면서 과제 및 평가에서 합격점 이상이면 합격
- **(응시언어)** 영어

[표 2-15] NCFE의 디지털부문 교육

레벨	자격	검정내용	응시료
입문 레벨	필수 디지털 기술 입문 (Entry Level 3 Essential Digital Skills)	• 온라인 및 디지털 기기에서 안전하고 책임감 있는 서비스 제공 • 디지털 장치 사용 및 정보 처리 • 개발 및 편집 • 디지털 커뮤니케이션 및 거래	£22
레벨1	필수 디지털 기술 레벨1 (Level 1 Essential Digital Skills)		£22
레벨2	사이버 보안 원칙 레벨2 (Level 2 Certificate in the Principles of Cyber Security)	• 사이버 보안 소개 • 사이버 보안에 사용되는 용어 이해 • 사이버 보안의 법적 및 윤리적 측면 이해 • 사이버 보안에 대한 일반적인 위협 이해 • 사이버 보안 유지 방법 이해 • 사이버 보안 분야의 다른 사람들과 협력하기	£65
	코딩 이해 레벨2 (Level 2 Certificate in Understanding Coding)	• 코딩의 원리 및 용어 이해 • 코딩 설계 원리 이해 • 코딩의 프로세스와 실무 이해 • 코딩에서 커뮤니케이션 및 프로젝트 관리의 중요성 이해	£65
	데이터 분석 인증 레벨2 (Level 2 Certificate in Data Analysis)	• 데이터 분석 소개 및 데이터 분석가의 역할 • 데이터 수집, 처리 및 준비 • 데이터 해석 • 데이터 커뮤니케이션 및 프레젠테이션	£62
레벨3	사이버보안 실습 레벨3 (Level 3 Certificate in Cyber Security Practices)	• 사이버 보안 원칙 이해 • 사이버 보안의 위협 인텔리전스 • 사이버 보안 테스트, 취약점 및 제어 • 사이버 보안 사고 대응 • 사이버 보안 내 법률 및 윤리적 행위 이해	£80
	코딩실습 레벨3 (Level 3 Certificate in Coding Practices)	• 코딩 요구 사항 및 계획 • 코딩 설계 이해 및 구현 • 소프트웨어 테스트 • 배포, 유지 관리 및 구성 관리 이해	£80
	디지털 지원 레벨3 (Level 3 Certificate in Digital Support)	• 디지털 지원 부문에서 일하기 • 네트워크 인프라 및 클라우드 서비스 • 데이터 관리, 보안 • 디지털 서비스 지원 • 디지털 혁신 지원	£75

레벨	자격	검정내용	응시료
레벨4	사이버 보안 엔지니어 레벨4 (Level 4 Diploma Cyber Security Engineer)	• 사이버 보안의 원칙 • 사이버 보안 아키텍처 • 사이버 보안의 법률, 정책 및 절차 • 사이버 보안의 위협 인텔리전스 • 사이버 보안의 위험 평가 • 사이버 보안 관리	£200
	데이터 분석가 레벨4 (Level 4 Diploma Data Analyst)	• 데이터 분석에 적용되는 법률 및 보안 표준 • 데이터 펀더멘털 및 라이프사이클 • 데이터 구조 및 데이터베이스 • 데이터 분석에 대한 이해관계자 참여 및 사용자 경험 • 데이터 마이닝 및 통계 분석	£200

[출처] https://www.ncfe.org.uk/

3. 호주

□ 전문 교육기관에서 제공하며, 정부기관이 교육기관을 등록 및 관리

- 호주는 국가 직업교육 및 훈련 규제법(National Vocational Education and Training Regulator Act 2011)에 따라 등록된 훈련기관(RTO, Registered Training Organisation)이 되면 호주 내에서 직업 교육 및 훈련(VET, Vocational Education and Training) 제공이 가능
- **VRQA, ASQA에서 정보보호를 포함한 RTO를 검증하고 등록 및 관리**
  - 빅토리아 등록 및 자격기관(**VRQA**, Victorian Registration and Qualification Authority)은 빅토리아 주와 서부호주에서 기존 대학을 제외한 모든 교육 및 훈련 기관에 대한 등록 및 인증을 담당
  - 호주 기술품질국(**ASQA**, Australian Skills Quality Authority)은 빅토리아주와 서부호주 외 지역에서의 직업교육 훈련 부문의 규제기관
  - **VRQA, ASQA**와 같은 기관에서 사이버 보안 관련 과정평가형 자격제도를 운영하고 있음

[표 2-16] VRQA, ASQA의 사이버 보안 관련 과정평가형 자격제도

명칭	인증기관	자격내용
Certificate IV in Cyber Security (사이버 보안 인증서 IV)	Victorian Registration and Qualification Authority	다양한 조직과 정부 기관 사이버 보안 기술자에게 필요한 지식과 다양한 기술을 제공하는 기술자 수준의 과정
Certificate IV in Offensive Cyber Security (사이버 보안 인증서 IV)	Australian Skills Quality Authority (ASQA)	인프라, 네트워크 및 애플리케이션에 대한 해킹 및 모의해킹 등 취약점 평가 수행 과정

[출처] VRQA, ASQA 각 사이트

- 호주 정부는 호주 자격 프레임워크(**AQF**, Australian Qualifications Framework)를 통해 자격수준을 명시

[표 2-17] AQF의 자격수준

단계		내용
레벨1	1급 자격증 (Certificate I)	초기 작업, 지역 사회 참여 및 추가 학습을 위한 기본적인 기능적 지식과 기술
레벨2	2급 자격증 (Certificate II)	알려진 일상 업무와 절차에 관한 일상적인 지식과 기술
레벨3	3급 자격증 (Certificate III)	업무에 필요한 이론적이고 실무적인 지식과 기술
레벨4	4급 자격증 (Certificate IV)	다양한 맥락에서 평가 및 분석 기능을 포함한 광범위한 기술 응용 분야
레벨5	고등교육 졸업 (Diploma)	본 원리와 복잡한 기법을 바탕으로 한 기술과 지식을 스스로 적용
레벨6	고급 전문학사, 준학사 학위 (Advanced Diploma, Associate Degree)	일부 분야에 대한 심도 있는 지식과 기술을 요하며, 준전문가/고도 기술
레벨7	학사 학위 (Bachelor's Degree)	전문적인 업무와 추가 학습을 위한 광범위하고 일관된 지식과 기술을 제공
레벨8	학사 우등 학위, 대학원 수료증, 대학원 전문학사 학위 (Bachelor Honours Degree, Graduate Certificate, Graduate Diploma)	학사 학위의 기본이 되는 학위에 더해 더 높은 수준의 전문성
레벨9	석사 학위 (Master's Degree)	고도로 기술적이고 전문적인 업무에 필요한 고급 지식이 필요
레벨10	박사 학위 (Doctoral Degree)	고급 연구 기술 적용에 중점을 두고 가장 높은 수준의 학문적 성과

[출처] https://www.aqf.edu.au/

□ **Lumify Learn, 모나크 연구소** 등에서 정보보호 관련 자격을 제공

- 루미파이 교육원(**Lumify Learn**)은 온라인 교육을 통해 IT 학위와 자격증을 제공하는 호주의 교육 훈련기관
- 모나크 연구소(**Monarch Institute**)는 비즈니스 분야의 교육 및 훈련 서비스를 제공하는 기관으로, 온라인으로 실무 중심의 교육을 지원

☐ Lumify Learn

- **Lumify Learn는 온라인을 통해 실무 전문가의 강의를 제공**
  - 웹개발, 사이버보안 등 IT분야의 학위, 자격인증을 제공
  - AWS, Azure 등과 같은 국제 자격증은 온라인 부트캠프를 통해 지원

[표 2-18] Lumify Learn의 자격제도

구분	자격 명
학위증	정보기술 학사(사이버보안)
	정보기술학 석사(고급네트워킹)
	정보기술학 석사(백엔드 웹개발)
자격 인증	정보기술 3급
	정보기술 3급(Certificate III) 사이버보안 기본
	정보기술 4급 프로그래밍
	정보기술 4급 웹개발
	정보기술 4급 클라우드 컴퓨팅
	정보기술 4급 네트워킹
	정보기술 4급 시스템관리 지원
	정보기술 4급 프런트엔드 웹사이트 개발

[출처] https://lumifylearn.com/

- **정보기술 3급, 사이버보안 기본**(Basic Cyber Security Awareness)
  - 클라이언트 장치 보안, 조직보안, 온라인 보안 등 3개 부문의 세부 내용으로 구성
  - 교육기간은 12개월이며, 교육이 끝나면 자격을 인정하는 방식

[표 2-19] Lumify Learn의 자격제도

부문	내용
클라이언트 장치 보안	• 산업별 기술 식별 및 활용 • 네트워크 시스템 관리 제공 • 비판적이고 창의적인 사고 능력을 개발
조직 보안	• 네트워크 운영 체제 구성 및 관리 • 온라인 보안 위협 식별 및 보고 • 개인식별정보 및 직장정보 관리
온라인 보안	• ICT 환경에서 IP, 윤리 및 개인정보 보호 정책 식별 • 프로그래밍 기술 적용 • 사이버 보안 위협으로부터 개인 온라인 프로필을 보호 • 디지털 기기의 보안을 유지

[출처] https://lumifylearn.com/

□ 모나크 연구소(Monarch Institute)

○ 실무 전문가를 중심으로 전문지식을 교육하고, 자격증을 발급

- 회계, 금융, 마케팅, 물류 등 비즈니스 중심의 교육을 제공하고 있으며, 정보기술 부분 자격도 일부 포함
- 정보기술학 석사와 정보기술 4급 자격을 과정을 운영 중

[표 2-20] 모나크 연구소의 정보기술 자격제도

부문	내용
정보기술 4급	웹사이트 개발, 프로그래밍 등 웹 개발자 과정
정보기술학 석사	정보기술 전체를 포괄하는 학위과정
정보기술학 석사 (사이버 보안 및 고급 네트워킹)	사이버 보안 및 네트워킹 기본 사항
정보기술학 석사 (프런트엔드 및 백엔드 웹개발)	프런트엔드 및 백엔드 웹 개발을 전문으로 웹사이트, 온라인 애플리케이션 제작

[출처] https://www.monarch.edu.au/

○ 정보기술 4급 자격

- 12~ 24개월의 교육과정 중 객관식 문제, 단답형 테스트, 프로젝트, 롤플레이 등으로 종합 평가하여 자격증을 발급
- IT 산업, 클라이언트 개발, 웹사이트 강화, 프로그래밍 기본, 품질 관리 등 5개 부문의 세부 항목으로 구성

[표 2-21] 정보기술 4급 자격 검정과목

부문	내용
IT 산업 업무 (Work effectively in the IT industry)	• ICT 산업에서 협업 • ICT 환경에서 IP, 윤리 및 개인정보 보호 정책 준수 • 새로운 기술 및 관행을 식별하고 평가 • 고급 비판적 사고를 업무 프로세스에 적용
클라이언트 개발 (Client-side development)	• 웹사이트 레이아웃 디자인 • 간단한 마크업 언어 문서 만들기 및 스타일 지정 • 기본 클라이언트 측 스크립트 생성
웹사이트 강화 (Enhancing a website)	• 웹사이트 접근성 확인 • 웹 호스팅 서비스 평가 및 선택 • 웹사이트로 콘텐츠 전송 • 검색 엔진 최적화 구현
프로그래밍 기본 (Programming basics)	• 기초 프로그래밍 기술 적용 • 사용자 인터페이스 구축 • 객체 지향 언어의 기초 기술 • 다양한 언어로 기초 프로그래밍 기술을 적용
품질 관리 (Managing quality)	• 개발 환경에서 버전 제어 시스템 사용 • 테스트 소프트웨어 개발 • 사이버 보안 위험 관리에 기여 • 클라이언트 ICT 문제 식별 및 해결

[출처] https://www.monarch.edu.au/

제2절. 국내 자격제도와 비교

1. 국내 자격제도

□ 공공기관에서는 자격기본법, 국가기술자격법에 따라 정보보호 자격제도를 관리·운영하고, 민간단체는 자율적으로 자격제도 운영

- 자격기본법에서 '자격'은 직무수행에 필요한 지식·기술·소양 등의 습득 정도가 일정한 기준과 절차에 따라 평가 또는 인정된 것으로 정의
- 국가직무능력표준을 바탕으로 자격체계를 구축
  - 주요 직무 부문[22]에 대한 자격증은 국가자격증으로 신설하여 관리
  - 민간자격증은 예외조항을 명시하여, 그 외 분야에서는 민간기관이 자격을 등록하고 운영 가능
- 정보보안기사와 정보보안산업기사는 국가기술자격증으로 분류되어, 국가자격 중 산업과 관련있는 기술 분야의 자격증으로 구분

□ 정보보안기사

- **(개요)** 정보보호에 대한 지식과 운용 경험을 바탕으로 실무적인 시스템과 서버, 네트워크 장비 및 보안시스템 운용을 통해, 보안업무 및 보안정책수립과 보안대책 구현, 정보보안 관련 법규 준수 여부를 판단하는 등의 업무를 수행할 수 있는 자격
- **(정보보안기사 직무)** 시스템 및 솔루션 개발, 운영 및 관리, 컨설팅 등의 전문 이론과 실무능력을 기반으로 IT기반시설 및 정보에 대한 체계적인 보안업무 수행
- **(시행처)** 한국방송통신전파진흥원
- 응시자격 및 경력인정 기준
  - 「국가기술자격법 시행령」 제12조의2(국가기술자격의 등급과 응시자격)
  - 「국가기술자격법 시행규칙」 제10조의2(응시자격) 별표 11의 2에 근거하여 모든 직무분야에서 응시 가능

22) 국민의 생명·건강 및 안전에 직결되는 분야, 국방·치안·교육 및 국가기간산업 등 공익에 직결되는 분야, 자격 취득수요가 적어 민간자격의 운영이 곤란한 분야, 그 외 그 밖에 국가가 필요하다고 인정하는 분야 등

- **세부응시자격**[23)]
  - 산업기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 1년 이상 실무에 종사한 사람
  - 기능사 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 3년 이상 실무에 종사한 사람
  - 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 기사 등급 이상의 자격을 취득한 사람 직무분야별 학과
  - 관련학과의 대학졸업자 등 또는 그 졸업예정자
  - 3년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사직무분야에서 1년 이상 실무에 종사한 사람
  - 2년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사직무분야에서 2년 이상 실무에 종사한 사람
  - 동일 및 유사 직무분야의 기사 수준 기술훈련과정 이수자 또는 그 이수예정자
  - 동일 및 유사 직무분야의 산업기사 수준 기술훈련과정 이수자로서 이수 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 2년 이상 실무에 종사한 사람
  - 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 4년 이상 실무에 종사한 사람
  - 외국에서 동일한 종목에 해당하는 자격을 취득한 사람

- **(검정방법)** 정해진 일자에 시험에 응시하여 자격을 취득하는 검정형 방식이며, 필기시험과 실기시험을 모두 합격해야 자격취득

[표 2-22] 정보보안기사 검정방법

구분	출제유형 (시험시간)	합격기준	응시 수수료
필기	객관식 4지선다형 (2시간30분)	100점 만점에서 매과목 40점 이상, 전과목 평균 60점 이상(과목당 20문항)	18,800원
실기	필답(3시간)	100점 만점에서 60점 이상	21,900원

[출처] https://www.cq.or.kr/

23) 정보보안 분야는 학과와 직무분야 구분 없음(모든 학과, 모든 직무분야 응시 가능)

- **(사후관리)** 갱신없음
- **(자격증 혜택)** 공무원, 장교, 공기업, 민간기업, 학점인정 등 혜택 제공
- 검정과목

[표 2-23] 정보보안기사 검정과목

과목명		주요항목	세부항목
필기	시스템보안 (문제 수 20)	정보시스템의 범위 및 이해	단말 및 서버시스템, 운영체제, 시스템정보
		시스템 보안위협 및 공격기법	시스템 보안위협, 시스템 공격기법
		시스템 보안위협 및 공격에 대한 예방과 대응	시스템보안 대응기술, 시스템 분석도구, 시스템 보안솔루션
	네트워크 보안 (문제 수 20)	네트워크 일반	네트워크 개념 이해, 네트워크의 활용
		네트워크 기반 공격기술의 이해 및 대응	서비스거부(DoS), 분산서비스 거부(DDoS) 공격, 스캐닝, 스푸핑 공격, 스니핑 공격, 원격접속 공격
		네트워크 보안 기술	보안 프로토콜 이해, 네트워크 보안기술 및 응용
	어플리케이션 보안 (문제 수 20)	인터넷 응용 보안	FTP 보안, 메일 보안, Web/App 보안, DNS 보안, DB 보안
		전자상거래 보안	전자상거래 보안기술
		어플리케이션 보안 취약점	어플리케이션 보안취약점 대응, 어플리케이션 개발 보안
	정보보안 일반	보안요소 기술	인증, 접근통제, 키 분배 프로토콜, 디지털서명
		암호학	암호 알고리즘, 해시함수
	정보보안 관리 및 법규	정보보호 관리	정보보호 관리 이해, 정보보호 위험평가, 정보보호 대책구현 및 사고대응, 정보보호 인증제도 이해
		정보보호 관련 윤리 및 법규	정보보안 윤리, 정보보호 관련 법제, 개인정보보호 관련 법제
실기	정보보안 실무	시스템 및 네트워크 보안 특성 파악	운영체제별 보안특성 파악하기, 프로토콜별 보안특성 파악하기, 서비스별 보안특성 파악하기, 보안장비 및 네트워크 장비 별 보안특성 파악하기
		취약점 점검 및 보완	운영체제 보안설정 점검과 보완하기, 서비스 보안설정 점검 과 보완하기, 네트워브 및 보안장비 설정 점검과 보완하기, 취약점 점검이력과 보완내용 관리하기
		보안관제 및 대응	정보수집 및 모니터링, 로그분석 및 대응
		위험분석 및 정보보호 대책 수립	IT 자산 위험 분석하기, 조직의 정보자산 위협 및 취약점 분석 정리하기, 위험평가하기, 정보보호 대책 선정 및 이행계획 수립하기

[출처] https://www.cq.or.kr/

□ 정보보안산업기사

- 보안에 관련한 시스템과 응용 서버, 네트워크 장비 및 보안장비에 대한 전문지식과 운용기술을 갖추고, 시스템/네트워크/어플리케이션 분야별 기초 보안업무를 수행할 수 있는 자격
- 검정형과 과정평가형 두 가지 방법 중 선택하여 자격취득이 가능
  - 검정형은 정해진 일자에 시험에 응시하여 자격을 취득하는 방법으로 필기시험과 실기시험을 모두 합격해야 자격취득

[표 2-24] 정보보안산업기사 검정방법

구분	과목	출제유형 (시험시간)	합격기준	응시 수수료
필기	1. 시스템보안 2. 네트워크보안 3. 어플리케이션보안 4. 정보보안일반	객관식 4지선다형 (2시간)	100점 만점에서 매과목 40점 이상, 전과목 평균 60점 이상 : 과목당 20문항	18,800원
실기	정보보안 실무	필답형 (2시간 30분)	100점 만점에서 60점 이상	20,200원

[출처] https://www.cq.or.kr/

  - 과정평가형은 일정요건을 충족하는 교육 및 훈련과정을 충실히 이수한 자가 내부·외부 평가를 거쳐 자격을 취득할 수 있으며, 국가직무능력표준(NCS, National Competency Standards)에 따른 과정으로 구성

[표 2-25] 정보보안산업기사 과정평가 내용

구분	NCS 능력단위명	최소훈련시간	합격기준
직업 기초능력	의사소통능력, 정보능력	18시간	내부평가와 외부평가 결과를 1:1로 반영하여 평균 80점 이상
필수능력단위 (420시간)	애플리케이션 보안 운영	45시간	
	SW개발 보안 구축	45시간	
	시스템 보안 구축	45시간	
	정보시스템 진단	90시간	
	보안로그 분석	60시간	
	네트워크 보안 운영	45시간	
	NW보안 구축	45시간	
	시스템 보안 운영	45시간	
선택능력단위 (150시간 이상)	관리적 보안 구축	45시간	
	관리적 보안 운영	30시간	
	DB보안 구축	45시간	
	물리적 보안 구축	30시간	
	암호 분석	180시간	
	물리 보안 운영	30시간	

[출처] 한국방송통신전파진흥원

□ 개인정보관리사(CPPG, Certified Privacy Protection General)

- **검정기준**
  - 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 갖춘 인력 또는 향후 기업 또는 기관의 개인정보 관리를 희망하는 자로서, 다음의 업무능력을 보유한 자
  - 개인정보보호와 관련된 보안정책의 수립, 기업/기관과 개인정보보호의 이해, 개인정보 취급자 관리, 관련법규에 대한 지식 및 적용
- **(시행처)** (사)한국CPO포럼
- **(응시료)** 130,000원(단체 15인 이상 20% 할인, 학생 50% 할인)
- **(응시자격)** 제한 없음
- **(합격기준)** 과목 당 40% 이상, 총점 60% 이상

[표 2-26] 개인정보관리사 과목별 문항 및 합격기준

검정과목		문항 수	배점	출제형태	시험시간
개인정보보호의 이해	개인정보의 개요 개인정보보호의 중요성 기업의 사회적 책임	10	10	객관식 5지선다	120분
개인정보보호 제도	개인정보보호 관련 법률 체계 개인정보보호 원칙과 의무 정보주체의 권리 분쟁해결 절차	20	20		
개인정보 라이프사이클 관리	개인정보 수집·이용 개인정보 저장·관리 개인정보 제공	25	25		
개인정보의 보호조치	법적 개요 개인정보의 기술적·관리적 보호조치 기준	30	30		
개인정보관리체계	개인정보 관리체계 개요 주요 개인정보 관리체계	15	15		

[출처] https://cpptest.or.kr/

□ 인터넷보안 전문가

- **서버를 보호하고 보안 설정, 보안 분석, 해킹방지, 서버복구 등 서버에 대한 해킹에 효과적으로 대처하고 정보를 보호할 수 있는 인터넷 보안 관련 기술력에 대한 자격**
  - (1급) Linux, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해사고 대응, 해킹예방, 시스템 분석 등의 전문능력을 검정
  - (2급) Linux, Windows 계열을 기반으로 한 서버에서 인터넷 보안과 관련한 보안관리, 침해사고 분석 및 대처의 실무능력을 검정
- **(시행처)** (사)한국정보통신자격협회
- **(검정방법)** 필기시험과 실기시험을 모두 합격해야 자격을 취득할 수 있는 검정형 방식

[표 2-27] 인터넷보안 전문가 검정방법

구분	출제유형	합격기준	응시 수수료
1급	필기	100점 만점에서 60점 이상	43,000원
	실기		100,000원
2급	필기		43,000원
	실기		78,000원

[출처] https://www.icqa.or.kr/

- 검정과목

[표 2-28] 인터넷보안 전문가 검정과목

등급	검정과목		문항 수	시간	유형
1급	필기	정보보호개론, 운영체제, 네트워크, 보안	60문항	60분	택일형
	실기	침해사례 분석, 침해과정 분석, 시스템서비스 관리, 코드분석, 해결책 및 예방책, 시스템 보안관리, 시스템침해분석, 방화벽구축	1 SET (1~20문항)	120분	작업/서술/ 선택형 등
2급	필기	정보보호개론, 운영체제, 네트워크, 보안	60문항	60분	택일형
	실기	침해사례 분석, 침해과정 분석, 시스템서비스 관리, 코드분석, 해결책 및 예방책	1 SET (1~20문항)	120분	작업/서술/ 선택형 등

[출처] https://www.icqa.or.kr/

□ 해킹보안전문가(Hacking & Security Expert)

- 해킹보안 전문가로서 갖추어야 할 지식에 대한 검정과 실무에 적응할 수 있는 능력을 검정
- **(시행처)** 한국해킹보안협회
- **(검정내용)**
  - **(1급)** 해킹보안에 대한 고급 지식과 실무능력을 검증하며, 정보보안 분야의 전문가임을 인증
  - **(2급)** 해킹보안에 대한 좀 더 깊이 있는 지식을 다루며, 실무에서 필요로 하는 내용을 평가 및 인증시험에 반영
  - **(3급)** ICT에 관심있는 고교생 및 직장인 등 해킹과 보안에 대한 올바른 윤리관과 기본지식을 쌓을 수 있도록 하여 정보화 사회에 대비한 관련 분야의 기본실력을 갖춘 인력을 양성
  - **(주니어급)** 초등학생 수준의 자격급수로 해킹보안 관련 기초지식의 습득 정도를 확인
- **(검정방법)** 1급과 2급은 필기시험과 실기시험을 모두 합격해야하고, 3급과 주니어는 필기시험만 검정

[표 2-29] 해킹보안 전문가 검정방법

구분	출제유형	합격기준	응시장소	수수료
1급 (준비 중)	필기	400점 만점에서 60점 이상(과목별 40점 이상)	(준비 중)	(준비 중)
	실기	100점 만점에서 60점 이상		
2급	필기	400점 만점에서 60점 이상(과목별 40점 이상)	오프라인	50,000원
	실기	100점 만점에서 60점 이상	온라인	50,000원
3급	필기	100점 만점에서 60점 이상	온라인	50,000원
주니어	필기	100점 만점에서 60점 이상	온라인	25,000원

[출처] https://nahs.or.kr/

- 응시자격

[표 2-30] 해킹보안 전문가 응시자격

구분	합격기준
1급	대학교 졸업자 또는 졸업예정자 2급 자격을 취득한 자
2급	3급 자격을 취득한 후 6개월 이상이 경과한 자 2년제 IT직업전문학교 관련학과 졸업자 또는 졸업예정자 4년제 대학졸업자 또는 졸업예정자 직업학교 또는 직업전문학교 컴퓨터 관련학과 졸업자 또는 졸업예정자
3급	자격제한 없음
주니어	자격제한 없음

[출처] https://nahs.or.kr/

□ 금융보안관리사(CFSE, Certified Financial Security Expert)

- **(시행처)** 사단법인 금융보안원
- **(응시조건)** IT 및 정보보호 경력 3년 이상인 사원기관 재직자 중 전체 교육과정 80% 이상 수료자
- **(교육 및 검정방법)** 4개 과목 교육 수강 후 자격시험(4지선다 객관식)

[표 2-31] 금융보안관리사 검정방법

과목명	교육시간	문항 수	배점	합격기준
금융비즈니스	7시간 내외	10문항	10점	4점
금융보안 관리체계	17시간 내외	25문항	25점	10점
금융IT보안	25시간 내외	30문항	30점	12점
전자금융보안	26시간 내외	35문항	35점	14점
합격기준		100문항	100점	60점 이상

[출처] https://www.fsec.or.kr/bbs/151

- **(자격증 갱신요건)** 자격증 유효기간 3년 이내 42시간(매년 최소 10시간 이상)의 자격유지교육(Continuing Professional Education) 인정 활동을 수행한 경우 자격증 갱신

□ 정보보안관제사

- **(시행처)** 사단법인 한국사이버감시단
- **(응시수수료)**
  - (1급) 필기 55,000원, 실기 66,000원
  - (2급) 필기 44,000원, 실기 55,000원
  - (3급) 필기 44,000원
- **(검증기준, 수행직무)**
  - (1급) 정보시스템의 서버(시스템), 네트워크 장비 및 정보보안장비에 대한 전문지식과 운용기술을 갖추고 실시간 정보보안관제 기술/능력 보유 여부, 보안정책수립과 보안대책 구현, 취약점 진단 및 침해사고 분석의 기술 보유 여부, 정보보호 관련 법규 준수 여부를 판단하는 등의 업무 수행 능력을 갖춘 최고급 수준의 능력을 가진 자
  - (2급) 정보보안관제사 1급 업무를 보조할 수 있는 기초 이론과 실무능력 등의 업무 수행 능력을 갖춘 중급 수준의 능력을 가진 자

- (3급) 정보보안관제사 2급 업무를 보조할 수 있는 기초 이론과 실무능력 등의 업무 수행 능력을 갖춘 초급 수준의 능력을 가진 자
- (3급 주니어) 정보보안관제사 3급 업무를 보조할 수 있는 기초 이론과 실무능력 등의 업무 수행 능력을 갖춘 초급 수준의 능력을 가진 자

(응시자격)

[표 2-32] 정보보안관제사 응시자격

등급	세부응시자격	연령/학력
1급	1. 기사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야 1년 이상 실무에 종사한 사람 2. 기능사 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 3년 이상 실무에 종사한 사람 3. 4년제 대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 1년 이상 실무에 종사한 사람 4. 3년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 2년 이상 실무에 종사한 사람 5. 2년제 전문대학 관련학과 졸업자 등으로서 졸업 후 응시하려는 종목이 속하는 동일 및 유사 직무 분야에서 3년 이상 실무에 종사한 사람 6. 응시하려는 종목이 속하는 동일 및 유사 직무분야에서 5년 이상 실무에 종사한 사람 7. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람	4년제 대학 관련학과 졸업 후 (기사 자격 후)경력 1년 이상 2급 취득 후 관련 실무경력 2년 이상 응시가능
2급	1. 기능사 등급 이상의 자격을 취득한 후 응시하려는 종목이 속하는 동일 및 유사 직무분야에 1년 이상 실무에 종사한 사람 2. 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 산업기사 등급 이상 자격을 취득한 사람 3. 관련학과의 2년제 또는 3년제 전문대학졸업자 등 또는 그 졸업예정자 관련학과 2학년 80학점이상(학점은행제 포함) 이수자부터 응시 가능 4. 동일 및 유사 직무분야에서 1년 이상 실무에 종사한 사람 5. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람 6. [3급] 자격취득 후 실무경력 1년 이상 습득한 사람	전문대학 졸업예정자 80학점 이상 기능사 자격 후 경력 1년 이상 3급 취득 후 응시가능
3급	1. 응시하려는 종목이 속하는 동일 및 유사 직무분야의 다른 종목의 기능사 등급 이상의 자격을 취득한 사람 2. 중등학교 졸업자 등 또는 그 졸업예정자 제한 없음 3. 동일 및 유사 직무분야의 기능사 수준 기술훈련과정 이수자 또는 이수예정자 4. 외국에서 동일한 종목에 해당하는 자격을 취득한 사람	중등학교 졸업예정자 이상 제한없음

[출처] http://www.isc16.com/

(검정과목)

[표 2-33] 정보보안관제사 검정과목

구분		1급	2급	3급		유형	검정시간	합격 기준
				일반	주니어			
필기	보안관제일반	20문항	20문항	20문항	25문항	객관식 4지선다	2,3급 60분 1급 90분	60점 이상, 과목당 40점 이상
	보안관제 기술	20문항	20문항	20문항	25문항			
	보안관제 운용	20문항	20문항	20문항	x			
	취약점 진단기술	20문항	20문항	x	x			
	침해사고 분석기술	20문항	x	x	x			
	합계	100문항	80문항	60문항	50문항			
실기	정보보안관제실무	고급형	중급형	x	x	필답형	2급 90분 1급 120분	60점 이상

[출처] http://www.isc16.com/

□ 디지털포렌식전문가

(시행처) (사)한국포렌식학회·한국인터넷진흥원

(개요)

- 디지털 포렌식 분석자의 전문성을 검증하기 위하여 디지털포렌식전문가 1급 자격제도를 운영
- 2급 시험은 현장에서 디지털 증거의 무결성 및 원본성을 증거수집자의 능력을 검증
- 1급 시험은 2급 시험에서 요구되어지는 능력에 더하여 디지털 증거 분석에 수반되는 더 높은 수준의 전문성에 초점을 두어 분석자의 전문성을 검증

(합격기준) 각 과목 40점 이상, 평균 60점 이상

(검정과목)

[표 2-34] 디지털포렌식전문가 검정과목

급수	검정과목			유형	합격기준
1급	필기	필수	디스크포렌식	서술형	각 과목 40점 이상, 평균 60점 이상
			증거법		
		선택	네트워크포렌식		
			데이터베이스 포렌식		
			모바일포렌식		
			침해사고 대응 포렌식		
	실기	필수	디스크포렌식	실습형	
		선택	네트워크포렌식		
			데이터베이스 포렌식		
			모바일포렌식		
			침해사고 대응 포렌식		

급수	검정과목		유형	합격기준
2급	필기	컴퓨터 구조와 디지털 저장매체	객관식 선다형	
		파일시스템과 운영체제		
		응용프로그램과 네트워크의 이해		
		데이터베이스		
		디지털포렌식 개론(기초실무, 법률이론)		
	실기	디지털포렌식 기초실무	실습형	

[출처] https://exam.forensickorea.org/

(1급 응시자격) 24)

- 디지털포렌식 전문가 2급 자격을 보유하고 2년 이상 유관경력이 있는 사람 (단, 자격 취득 후 학회 주관 보수교육을 매년 8시간 이상 이수한 사람에 한함)
- 석사 이상의 유관학력을 취득한 후, 2년 이상의 유관경력이 있는 사람
- 변호사나 변리사, 공인회계사로서 3년 이상의 유관경력이 있는 사람
- 유관자격을 보유한 사람으로서 3년 이상의 유관경력이 있는 사람

(응시료)

- (1급) 필기 100,000원, 실기 250,000원 (자격증 발급 10,000원)
- (2급) 필기 60,000원, 실기 150,000원 (자격증 발급 10,000원)

2. 자격제도 비교분석

□ 자격제도의 의의

자격제도는 전통적인 교육과 함께 특정 수준의 숙련도를 공식적으로 인정하는 과정을 의미

- 교육이 정해진 학제에 따라 학문을 연구하는 과정이라면, 자격은 노동시장에서 필요한 특정 분야에 대한 숙련도를 확인
- 영국과 호주는 교육과 자격을 연계하여 운영하고 있으며, 자격제도가 교육과정의 학위를 포괄하는 의미로 통용
- 우리나라와 미국은 교육과 자격을 분리하여 운영하고 있으며, 자격제도는 전문기관에 의해 별도의 검정과정에 따라 인정

24) 2급 응시는 자격제한 없음

○ 자격이 노동시장에서 효용성을 갖기 위해서는, 자격의 신호기제와 선도기제의 활성화 필요

- 노동시장에서 자격은 신호기제(Signal), 선도기제(Guide), 선별(screening)의 기능을 수행[25)]

[표 2-35] 자격의 기능

기능	내용	기능 활성화 조건
신호기제 (signal)	근로자의 능력의 정도를 나타내는 신호	자격의 검정과정에 능력의 식별, 평가, 지표화를 적절하게 반영
선도기제 (Guide)	사회(노동시장)에서 필요로 하는 능력의 형성과 향상을 선도	자격이 사회(노동시장)에서 요구하는 능력을 적절하게 반영
선별 (screening)	기업이 근로자를 채용할 때 기업에 필요한 직업능력인지 판단하는 요소	기업의 요구분야에 대한 최소기준으로 자격의 소지여부가 중요

[출처] 자격제도의 비전과 발전방안

- 신호기제와 선도기제가 제대로 작동하면 자격이 기업의 선별장치로 인정되면서 자격의 기능에 효용성이 높아지는 효과
- 신호기제와 선도기제 기능이 활성화되기 위해서는 **자격이 투명하고 공평하게 관리 및 운영**되어야 하며, 이를 위해 각국의 정부는 자격 인증기관에 공신력을 부여할 수 있는 다양한 정책을 마련
- 대부분의 국가는 **자격증 부여기관의 자격증 관리 및 운영 방침에 대한 인증제도**를 가지고 있으며, **자격의 내용에 대한 직무 표준**을 통해 자격제도의 공신력을 확보

□ 자격제도의 비교분석

○ **자격제도의 운영**은 각 국의 사회적, 문화적 차이에 따라 차이

- 미국은 전세계 IT를 선도함에 따라, **전문 교육기관**이 제공하는 보안자격증이나 **기업을 중심**으로 클라우드 보안 자격제도를 **국제적으로 시행**
- 영국과 호주는 **교육과정과 연계된 직업교육**의 일환으로 사이버보안 자격제도를 운용
- 우리나라는 사이버보안을 **중요한 국가기술**로 인식하고 공공기관에서 국가기술자격증으로 운영하는 것과 민간단체에서 자율적으로 운영하는 자격증으로 구분됨

○ **검정내용**은 정보보호 기술을 중심으로 **실무자**를 위한 과정과 전체 거버넌스를 포괄하는 **관리자** 과정으로 구분

- CISSP, CISA는 정보보호 관리자를 위한 대표적인 자격시험으로 정보보호 기술뿐만 아니라, 조직의 이해관계자와 커뮤니케이션, 법률, 계약 등을 포함하는 포괄적인 내용

25) 강순희·김안국·박성재·김주섭·김승택·김덕호·정주연·박충렬 '자격제도의 비전과 발전방안', 한국노동연구원, 2003.

- AWS, CEH, 정보보안기사 등은 해당 부분의 실무 전문가를 대상으로 하는 기술적인 내용이 중심
- 영국과 호주의 자격과정은 실무자 중심으로 초급부터 고급까지 과정을 교육과 함께 제공

- **평가**는 대부분 **검정형**이나, 영국과 호주는 교육을 포함하는 **과정평가형**
  - CISSP, CISA는 자격검정만 시행하고 있으며, CEH는 응시 자격이 충족된다면 자격검정만도 가능하지만 응시를 위한 경력이 부족할 경우에는 별도의 교육옵션을 제공
  - 영국과 호주는 경력과 상관없이 교육을 신청하고 자격취득이 가능한 과정평가형
  - 우리나라의 정보보안산업기사는 검정형과 과정평가형을 모두 지원하고 있으며, 정보보안기사는 검정형만 가능

P·A·R·T 03

정보보호분야 교육 프로그램

제1절. 국가별 교육기관의 운영현황

1. 미국

□ 사이버보안강화법에 따라 NICE 설립

- **국가 사이버보안에 대한 공공과 민간의 협력을 강화하고, 사이버보안 개선, 연구강화, 인력양성과 인식제고를 위해 사이버보안강화법(Cybersecurity Enhancement Act of 2014)을 제정**
  - 2008년 국가 사이버보안 이니셔티브(CNCI, Comprehensive National Cybersecurity Initiative)에서 국가 사이버보안 강화를 위해 미국 내 방어선 구축, 교육 및 연구 등의 목표를 수립
  - CNCI는 연방인력이 사이버보안 문제를 해결하기 위한 목적이었으나, 이후 민간부문까지 확대
  - 이후 사이버보안강화법에 따라 국립표준기술원(NIST, National Institute of Standards and Technology)이 주도하여 NICE[26]를 설립

- **NICE는 사이버보안 교육, 훈련 및 인력 개발의 통합 생태계를 발전시키기 위해 아래의 5가지 목표를 수립**
  - 사이버보안 경력과 다양한 학습 경로의 발견 촉진
  - 다양하고 숙련된 인력을 구축하고 유지하기 위한 학습 혁신
  - 사이버 보안 기술 격차를 해소하기 위한 인재 관리 프로세스 현대화
  - 사이버 보안을 위한 인력 프레임워크 사용 확대(NICE 프레임워크)
  - 사이버 보안 인력 개발을 위한 효과적인 관행에 대한 연구 추진

- **NICE는 직접 교육을 제공하는 기관은 아니며, 사이버보안 인력개발을 위해 필요한 교육과 산업현장의 니즈를 연결할 수 있도록 지원**
  - NICE 프레임워크를 통해 사이버 보안에 필요한 지식, 기술 및 능력(KSA: Knowledge, Skills, and Abilities)을 정의
  - 학생, 실무자들은 자신의 KSA를 점검하고 부족한 부분은 확인하여 개별 교육기관을 통해 필요한 학습을 수행하는 방식

26) 2008년 설립 당시에는 국가 사이버 보안교육 이니셔티브(NICE, National Initiative for Cybersecurity Education)의 약어였으나, 2014년 사이버보안 강화법에 따라 이니셔티브가 아닌 장기적인 교육에 목표를 두게 되면서 더 이상 약어를 사용하지 않고 NICE로만 표기

□ NICE 프레임워크[27]를 통해 업무역할과 경력경로를 매칭

- **사이버 보안을 위한 NICE 인력 프레임워크(NICE Framework)를 발행하여 개인이나 팀이 사이버 보안 작업을 수행하는 데 필요한 업무, 지식 및 기술을 설명**
  - 사이버 보안의 정의, 포괄적인 사이버보안 업무 목록, 해당 업무를 수행하기 위해 필요한 KSA를 정의
  - 사이버보안의 업무역할을 7가지 범주로 나누어 업무역할을 구분(총 52가지)하여 사이버보안의 직무와 책임을 이해하고, 사이버보안 운영, 경력 경로 선택에 도움

[표 3-1] NICE 프레임워크 업무역할 범주

업무 역할 범주	설명	업무 역할 수
감독 및 거버넌스 (Oversight and Governance)	조직이 사이버보안 위험을 효과적으로 관리하고 사이버보안을 수행할 수 있는 리더십, 관리, 방향(direction), 변론(advocacy) 등을 제공	16
디자인 및 개발 (Design and Development)	경계(perimeter) 및 클라우드 기반 네트워크를 포함하여 보안기술 시스템에 대한 연구를 수행하고, 개념화, 설계, 개발 및 테스트	8
구현 및 운영 (Implementation and Operation)	효과적이고 효율적인 기술시스템 성능과 보안을 보장하기 위해 구현, 관리, 구성, 운영 및 유지보수(maintenance)를 제공	7
보호 및 방어 (Protection and Defense)	기술시스템 또는 네트워크의 위험을 보호하고, 식별 및 분석하고, 사이버 보안 이벤트 또는 범죄를 조사	7
조사 (Investigation)	디지털 증거의 수집, 관리, 분석을 포함하여 국가 사이버 보안 및 사이버 범죄 조사를 수행	2
사이버공간 인텔리전스 (Cyberspace Intelligence)	국가 정보에 유용한지 판단하기 위해 유입되는 사이버보안 정보에 대한 전문화된 검토와 평가	5
사이버공간 효과 (Cyberspace Effects)	사이버공간 방어를 위해 사이버공간 역량을 위한 계획, 지원, 실행	7

[출처] https://www.nist.gov/

  - NICE 프레임워크는 조직 내 사이버보안 위험을 효과적으로 관리하기 위해 특정 사이버보안 관련 지식과 기술이 필요한 사이버보안 인력이 주로 사용

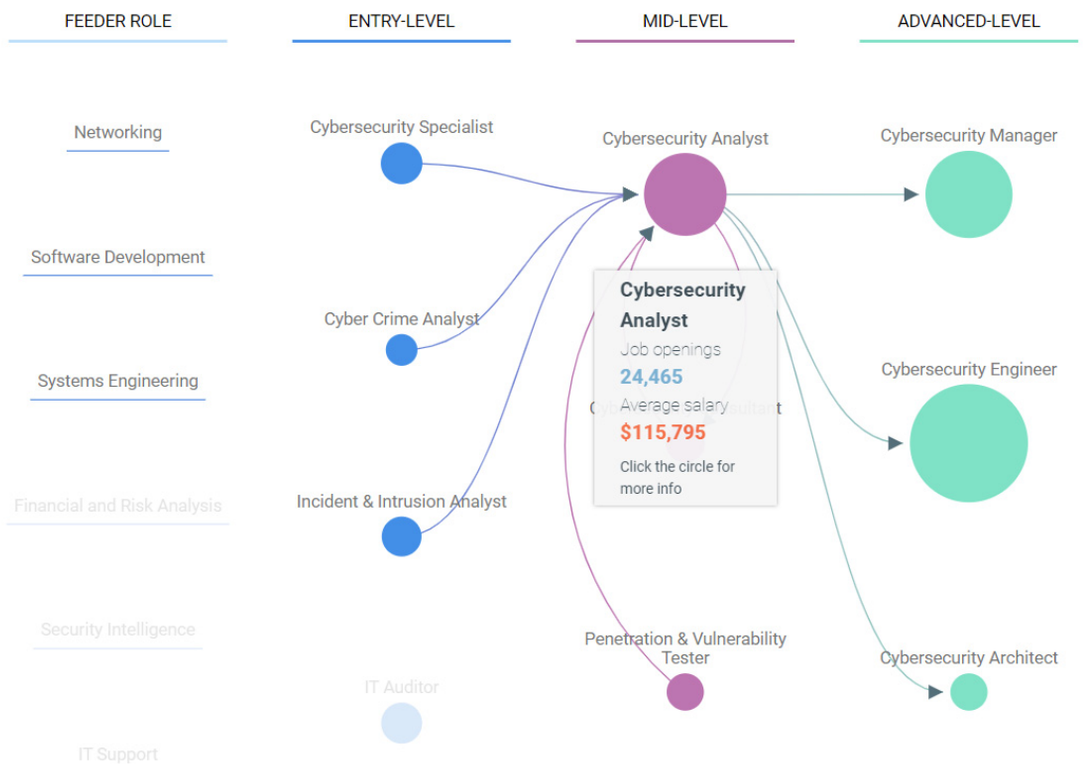
- **(고용주)** 인력평가를 실시하고 인력격차를 파악하여 직원 교육 및 경력 개발 경로를 제공
- **(대학 및 단과대학)** 고용주의 요구를 반영하는 과정 내용을 개발하고 조정
- **(교육자)** 학생들이 사이버보안 관련 업무를 탐구하고 미래 학습 방향을 계획하도록 지원

27) https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started

- **(교육 및 인증 제공자)** 현재 시장 수요를 반영하는 국가 표준에 맞춰 교육 및 인증 프로그램과 매핑
- **(학생, 구직자, 직장인)** 직무 역할과 관련 지식과 기술을 알아보고, 미래 학습과 경력 발전을 위한 경로를 계획
- **(사이버보안 인력 서비스 제공업체)** 개발 및 공급되는 제품과 서비스에 NICE 프레임워크를 통합

- NICE 프레임워크는 도구에 통합하거나 사용자가 직접 매핑할 수 있는 방법을 제공하는 등 각 기관에서 다양한 방법으로 활용
  - **(CyberSeek)**[28] NICE 프레임워크를 활용하여 사이버보안 일자리 시장에 대한 데이터와 경력 경로를 제공하고 있으며, 지도를 이용해 가까운 교육 및 훈련 제공업체 확인이 가능

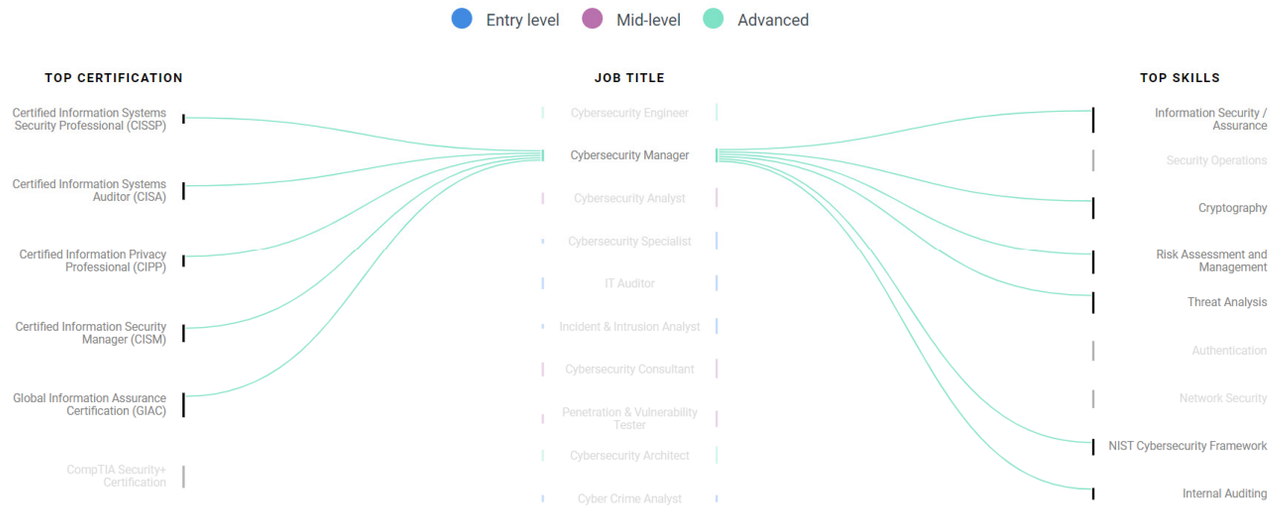
[그림 3-1] CyberSeek의 일자리 데이터 화면



[출처] https://www.cyberseek.org/

28) 사이버보안 인력의 공급이 수요를 따라가지 못한다는 판단 하에 사이버 보안인력의 저변확대를 위해 NICE, CompTIA, Lightcast가 공동으로 설립(https://www.cyberseek.org/)

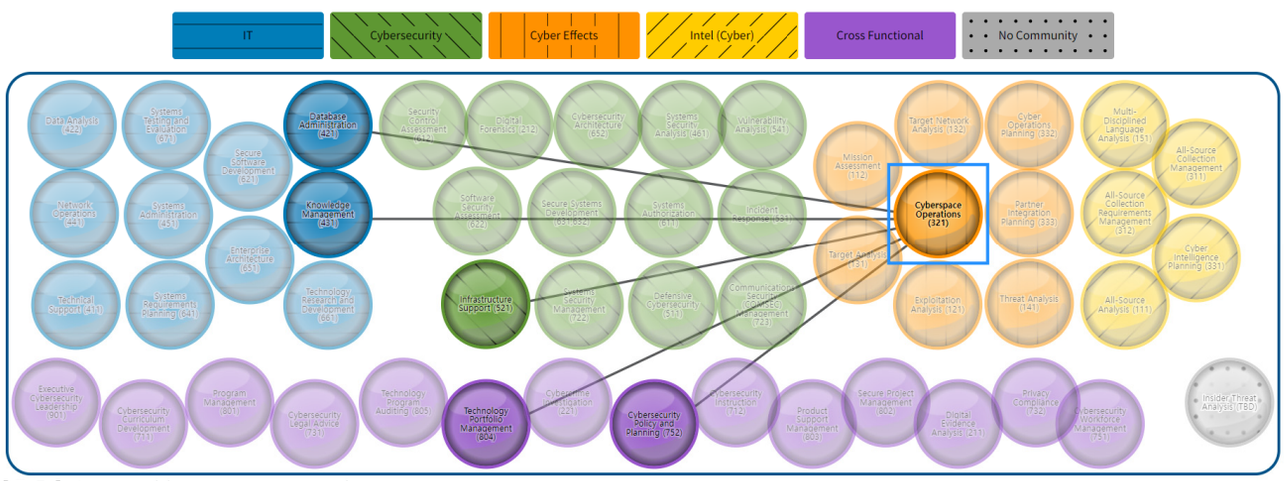
[그림 3-2] CyberSeek의 경력경로 매핑화면



[출처] https://www.cyberseek.org/

- **(NICCS)**[29] 사이버 인력을 5개 영역으로 구분하고 NICE 프레임워크의 52가지 업무역할과 연결하여 경력경로를 제공하고, 교육 및 훈련 카탈로그를 통해 사이버 보안 전문가가 사이버 보안 관련 과정을 찾을 수 있도록 지원

[그림 3-3] 사이버 경력경로 도구



[출처] https://niccs.cisa.gov/

29) 사이버 보안 경력 및 연구를 위한 국가 이니셔티브(NICCS, National Initiative for Cybersecurity Careers and Studies)는 사이버 보안 및 인프라 보안 기관(CISA, Cybersecurity and Infrastructure Security Agency)에서 정부 직원, 학생, 교육자 및 산업을 전국의 사이버보안 리소스 및 교육 제공자와 연결을 위해 설립한 산하기관(https://niccs.cisa.gov/)

[그림 3-4] NICCS의 교육 및 훈련 카탈로그

[출처] https://niccs.cisa.gov/

2. 이스라엘

□ 이스라엘 사이버캠퍼스에서 사이버보안 교육을 제공

- 텔아비브 대학(Tel Aviv University)[30]은 비즈니스 네트워킹 기업인 Improvate[31]와 함께 사이버보안 교육을 위한 이스라엘 사이버캠퍼스(Israel Cyber Campus)[32]를 개설
  - 이스라엘은 국내 총생산 규모가 한국의 20% 수준이지만 정보보안산업 매출은 우라나라의 3배 이상인 사이버 보안 강국[33]
  - 특히 사이버 보안 및 사이버전 능력으로 유명한 8200부대[34] 출신을 중심으로 다양한 보안 스타트업이 창업되어, 글로벌 기업에 매각되거나 미국 주식시장에 상장[35]

30) 이스라엘의 최대 도시 텔아비브에 위치한 이스라엘의 공립 종합대학으로, 과학 분야에서 우수한 평가(https://www.tau.ac.il/)
31) 2020년 창립되었으며, 이스라엘 기업을 글로벌 리더, 의사결정권자 및 투자자와 연결해주는 서비스를 제공(https://www.improvate.net/)
32) https://www.israelcybercampus.com/
33) IITP GT 주간브리프, '이스라엘의 사이버 보안 산업 및 정책 현황', 2020.11.30.
34) 이스라엘 정보부대로 비밀 작전, 신호정보 수집 및 코드해독, 방첩, 사이버전, 군사 정보 및 감시를 담당하고 있으며, 기능면에서 미국 국가안보국과 유사한 것으로 평가
35) 아시아투데이, '이스라엘 사이버보안 부대, 실리콘밸리 점령', 2024.09.01.

- Improvate은 스타트업과 글로벌기업, 투자자를 연결해주는 서비스를 제공하는 비즈니스 네트워킹 기업으로, 인적자원에 대한 투자의 일환으로 사이버캠퍼스를 지원

- **사이버캠퍼스는 8200부대 출신의 강사와 기업과 연계된 실습 중심의 커리큘럼으로 학생, 관리자, 실무자를 위한 사이버보안 교육을 제공**

□ 이스라엘 사이버캠퍼스 운영현황

- **(운영형태)** 텔아비브 대학 내의 공간을 활용하고, Improvate에서 지원하여 외부연구와 기업 연계 등 교육을 외부로 확장
  - 학업 프로그램 외 연구 개발에도 적극적으로 참여하여 전 세계의 사이버 보안를 해결하기 위한 다양한 프로젝트를 진행
  - 수업에 성실하게 참여하고 수업에서 평균 75점 이상의 점수 획득하고 강사의 추천이 있을 경우 이스라엘의 주요 사이버기업 대표와 개인 인터뷰를 통해 취업
  - EC-Council의 CEH, CSA, Linux의 LPIC-1 등 외부 자격증 취득 과정도 포함

- **(주요설비)** AI 시뮬레이터를 포함하여 첨단 기술과 리소스를 갖추고 있으며, 실제 사이버 공격을 시뮬레이션하고 학생 수준에 따라 시나리오를 업그레이드

- **(과정)** 네트워크 보안, 클라우드 보안, 침투 테스트, 디지털 포렌식 등 광범위한 사이버 보안 기술에 대한 실습 교육을 제공
  - 8200부대 출신, 학계 및 전문 분야의 강사와 전문가가 커리큘럼을 구성하고 교육을 진행
  - 청소년, 관리자, 실무 전문가를 위한 다양한 과정이 개설

- **(비용)** 비용 정보는 공개되어있지 않으나, 학생을 위한 자금지원이 있다고 명시되어 있어 개인의 부담은 크지 않을 것으로 추정

3. 영국

□ NCSC가 다양한 교육프로그램을 지원

- **국가사이버보안센터(NCSC, National Cyber Security Centre)[36]는 영국의 사이버 위협 및 정보 보증(IA, Information Assurance)을 위한 국가기관으로, 영국의 정보보안부서[37]를 통합하여 2016년 설립**
  - 일반 대중부터 공공기관, 산업, 중소기업까지 사이버보안에 대응하는 방법을 제공하고 복구를 지원
  - 보안역량을 육성하기 위한 교육과 기술을 지원하고 보안 안내지침을 통해 사이버보안에 대한 인식을 제고
  - 사이버보안과 관련된 다른 법집행기관, 국방부, 영국의 정보보안기관 및 국제파트너와 협력
- **청소년, 학사 및 대학원, 전문가를 위한 다양한 프로그램을 지원**
  - **(사이버퍼스트, CyberFirst)**[38] 7세 ~ 17세의 아동 및 청소년을 위한 프로그램으로, 사이버 보안을 소개하고 장학금, 경쟁대회, 게임 등으로 일찍부터 사이버보안 기술과 경험에 노출
  - **(NCSC 인증학위, NCSC-certified degrees)** 사이버보안 교육이 포함된 학위를 제공하는 영국 대학을 대상으로 제공되는 학위의 질을 평가하고 특정 경력경로에 적합한 학위를 파악하기 위한 인증을 제공
  - **(사이버 보안교육 우수 학술센터, ACEs-CSE)** NCSC 학위 인증을 받은 대학이 사이버 보안 교육 부분에서 우수성을 입증할 경우, 골드 또는 실버 상을 수여
  - **(NCSC 인증 교육, NCSC Certified Training)** 일반인을 위한 사이버보안 교육의 콘텐츠와 전달 방식의 품질을 보장하기 위한 제도로, 교육내용이 CyBOK의 지식영역과 매핑될 것을 요구
- **사이버보안지식체계(CyBOK, Cyber Security Body of Knowledge)[39]를 통해 사이버 보안의 기본 지식 체계를 수립하여 학습 및 경력 경로, 커리큘럼 및 전문교육 개발을 지원**
  - CyBOK은 수학, 물리학 등 전통과학이 중등교육부터 대학까지 명확한 학습단계를 갖추고 있는 것에 착안하여, 사이버 보안 부분에 존재하는 기술격차를 줄이고 명확한 기초지식을 확립하기 위한 지식 체계

---

36) https://www.ncsc.gov.uk
37) 영국정보통신본부(GCHQ, Government Communications Headquarters)의 통신전자보안그룹(CESG, CommunicationsElectronics Security Group), 사이버 평가 센터(CCA, , Centre for Cyber Assessment), 영국 컴퓨터 비상 대응 팀(CERT UK) 및 국가 기반 시설 보호 센터 (CPNI, Centre for the Protection of National Infrastructure) 등
38) https://www.ncsc.gov.uk/cyberfirst/overview
39) https://www.cybok.org/

- 교과서, 학술 연구 논문, 기술 보고서, 백서 및 표준 등의 문헌에서부터 온라인 설문조사, 인터뷰 등 다양한 커뮤니티의 협의를 포함하여 지식영역(KA, Knowledge Areas)을 제작

[표 3-2] CyBOK의 21가지 지식영역(KA)

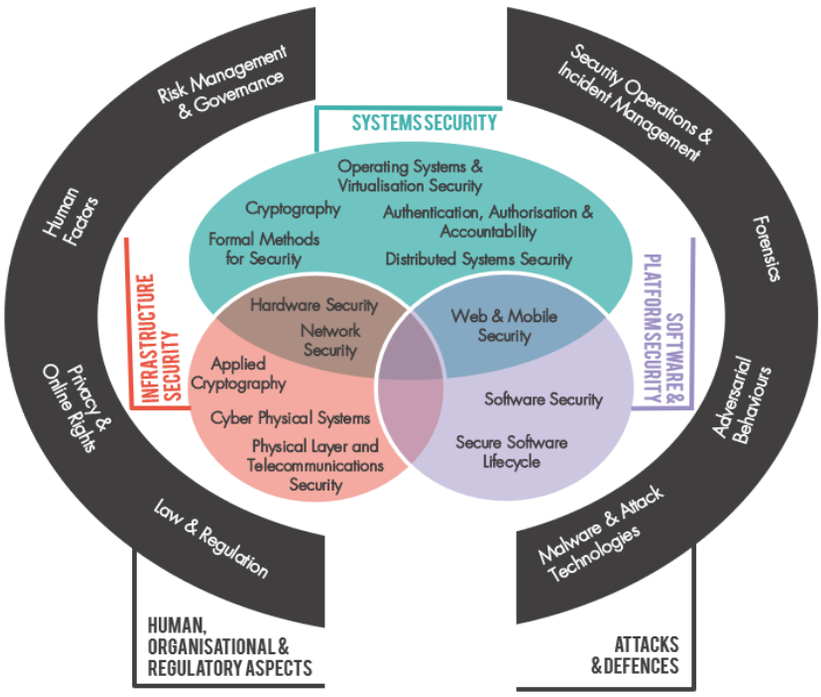
지식영역(KA)		설명
인적, 조직 및 규제	리스크 관리 및 거버넌스	표준, 모범 사례, 위험 평가 및 완화 접근 방식을 포함한 보안 관리 시스템 및 조직 보안 제어
	법률 및 규정	데이터 보호 및 사이버 전쟁에 관한 교리 개발을 포함한 국제 및 국가의 법적 및 규제 요건, 규정 준수 의무, 보안 윤리
	인적 요인	보안, 보안문화 및 인식에 영향을 미치는 보안, 사회 및 행동 요인과 보안 제어가 사용자 행동에 미치는 영향
	개인정보보호 및 온라인 권리	데이터베이스 및 데이터 처리에서 커뮤니케이션, 애플리케이션, 추론을 포함한 개인정보를 보호하는 기술이며, 검열 및 우회, 비밀유지, 전자선거, 결제 및 신원 시스템 등의 온라인 권리를 포함
공격 및 방어	멀웨어 및 공격기술	익스플로잇 및 분산 악성 시스템에 대한 기술적 세부 정보와 관련 검색 및 분석 접근 방식
	적대적 행동	멀웨어 공급망, 공격 벡터, 송금 등 공격자의 동기, 행동 및 방법
	보안운영 및 사고 관리	보안사고 탐지 및 대응, 위협 인텔리전스 수집 및 사용을 포함한 보안 시스템의 구성, 운영 및 유지보수
	포렌식	사건을 뒷받침하는 디지털 증거의 수집, 분석 및 보고
시스템 보안	암호화	암호화의 핵심 기본 알고리즘, 분석기술 및 프로토콜
	운영체제 및 가상화 보안	운영체제 보호 메커니즘, 하드웨어 추상화 구현, 다중 사용자 시스템의 격리, 가상화, 데이터베이스 시스템에서의 보안 등
	분산 시스템 보안	P2P 시스템, 클라우드, 멀티 테넌트 데이터 센터, 분산원장 등 대규모 조직화된 분산 시스템과 관련된 보안 메커니즘
	보안을 위한 공식적인 방법	기본 접근방식, 기술 및 도구 지원을 포괄하는 시스템, 소프트웨어 및 프로토콜의 보안에 대한 공식 사양, 모델링 및 추론
	인증, 승인 및 책임	신원관리 및 인증 기술의 모든 측면, 격리된 시스템과 분산된 시스템 모두에서 승인 및 책임을 지원하는 아키텍처와 도구
소프트웨어 및 플랫폼 보안	소프트웨어 보안	보안 버그를 초래하는 프로그래밍 오류와 코딩 연습 및 언어 설계를 통해 오류를 방지, 기존 시스템의 오류 감지, 기술 및 방법
	웹 및 모바일 보안	다양한 프로그래밍 패러다임과 보호 모델을 포함하여 디바이스와 프레임워크에 분산된 웹 애플리케이션 및 서비스와 관련된 문제
	보안 소프트웨어 수명 주기	전체 시스템 개발 수명 주기에 보안 소프트웨어 엔지니어링 기술을 적용

지식영역(KA)		설명
인프라 보안	응용 암호화	구현, 키 관리, 프로토콜 및 프로토콜 내에서의 사용에 관한 문제를 포함한 암호화 알고리즘, 체계 및 프로토콜의 적용
	네트워크 보안	라우팅 보안, 네트워크 보안 요소 및 네트워크 보안에 사용되는 암호화 프로토콜의 보안을 포함
	하드웨어 보안	신뢰할 수 있는 컴퓨팅 기술과 무작위성 소스를 포함한 범용 및 전문 하드웨어의 설계, 구현 및 배포 보안
	사이버 물리 시스템 보안	사물인터넷 및 산업제어 시스템, 공격자 모델, 안전한 설계, 대규모 인프라 보안과 같은 사이버 물리 시스템의 보안 문제
	물리계층 및 통신보안	무선 주파수 인코딩 및 전송 기술, 의도하지 않은 방사선 및 간섭의 측면을 포함한 물리 계층의 보안 문제와 한계

[출처] https://www.cybok.org/

- 21가지 지식영역(KA)는 직교화되지 않고 여러 면에서 서로 관련있는 다중구조로 되어 있음

[그림 3-5] CyBOK의 지식영역 간 관계



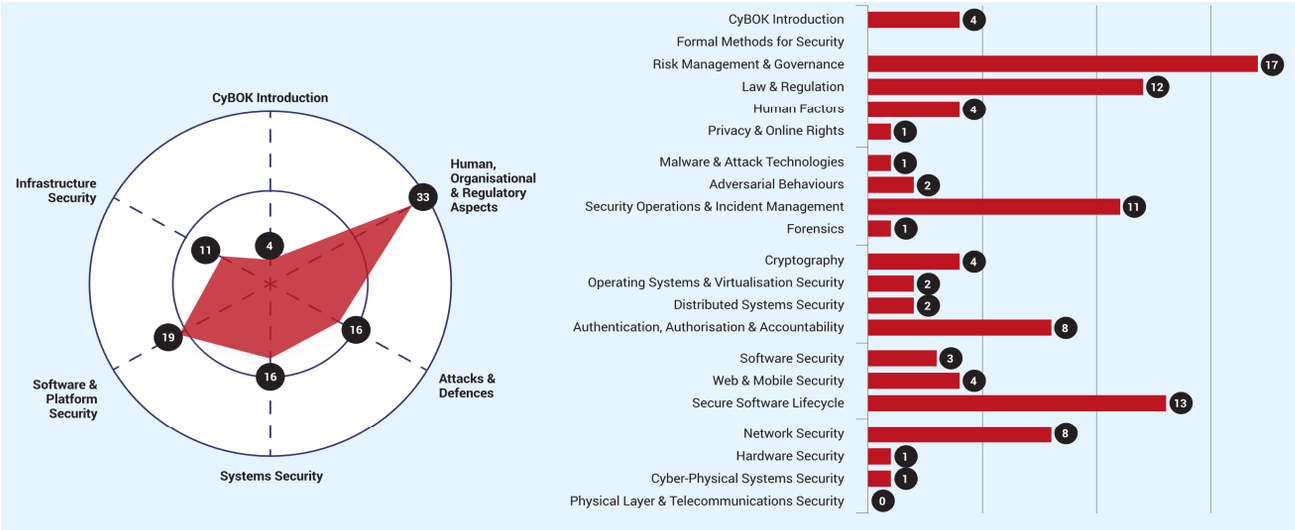
[출처] https://www.cybok.org/

- CyBOK의 세부 내용은 모두 공개되어있으며, 다양한 방법으로 소개하거나 이를 활용하여 다양한 리소스를 재생산

• 고등교육 프로그램 책임자가 NCSC 인증을 신청하는 기본자료로 활용하거나, 교육제공자가 CyBOK에 대한 교육프로그램을 매핑

• 제공되는 사이버보안 교육이나 자격증이 어떤 지식체계를 가지고 있는지 점검할 수 있는 자료로 활용

[그림 3-6] CyBOK 활용사례(CISSP 매핑)



[출처] https://www.cybok.org/

□ 영국 정보보호 공인연구소(CIISec)는 사이버 보안교육인 CyberEPQ를 제공

- **영국 정보보호 공인연구소(CIISec, Chartered Institute of Information Security)는 사이버 및 정보 보안 분야의 지식의 발전 및 보급을 촉진하고 관련 교육을 진행하는 비영리단체**
  - 사이버 및 정보 보안 기관으로, 업계리더들이 모여 정보보호 전문가의 인정을 위한 이슈를 해결하기 위해 설립(2006년)
  - 2018년에는 왕실헌장을 수여받고 독립적인 법인으로 출범하면서 사이버 및 정보보안 직업에 대한 표준을 제공
- **사이버 보안 분야에서의 경력을 고려하는 모든 사람에게 시작점을 제공할 수 있는 사이버 보안 확장 프로젝트 자격(CyberEPQ, Cyber security Extended Project Qualification) 교육을 제공**
  - CyberEPQ는 City & Guilds 공인 기술 자격증 과정으로 영국 대학입학에 필요한 GCSE 또는 A레벨과 동등하게 인정되어, 자격증 취득 후 대학 또는 직장에 진학이 가능
  - 교육 및 사이버 보안 파트너와의 협업을 통해 개발되었으며, CyBOK 지식영역과 연계된 과정으로 구성
- **실무 전문가를 위한 CPD, ICDIP 등의 인증 과정도 지원**
  - CIISec 이벤트 및 웨비나 참석을 포함한 다양한 수단을 통해 지속적인 전문 개발(CPD, Continuing Professional Development) 인증
  - 사이버 디지털 조사 전문가(ICDIP, Institute of Cyber Digital Investigation Professionals)는 사이버 디지털 조사에 참여하는 실무자의 전문성, 성실성, 우수성을 위한 과정으로, 동료평가와 면접으로 인증

4. 싱가포르

□ CSA에서 사이버 보안 인력의 성장 및 개발을 지원

- **싱가포르 사이버안보국(CSA, Cyber Security Agency of Singapore)[40]은 싱가포르의 사이버 공간을 보호하기 위해 2015년 설립**
  - 총리실 내 디지털개발 및 정보부(MDDI, Ministry of Digital Development and Information)에서 관리하고 있으며, 싱가포르 사이버 비상대응팀(SingCERT)을 포함하는 등 싱가포르의 정보보호를 총괄
  - 주요업무는 싱가포르의 사이버공간을 안전하고 보안되게 유지하고, 국가 안보를 뒷받침하며, 디지털 경제를 활성화하고, 디지털 생활 방식을 보호하는 것

- **안전한 사이버 공간 및 국가안보를 뒷받침할 인력 개발을 위해 학교, 산업계와 협력하여 다양한 교육 프로그램을 운영**
  - 학생, 학교, 노인과 일반 대중에게 사이버 보안에 대한 경각심을 일깨워줄 수 있는 정보를 제공하고 캠페인, 워크숍 등을 시행
  - 사이버 보안 분야에서 경력을 쌓고자 하는 대학원생과 전문가를 위해 싱가포르 컴퓨터 협회(SCS, Singapore Computer Society)와 협력하여 사이버 보안 경력 멘토링 프로그램을 조직
  - 다른 정부기관, 협회, 산업 파트너 및 학계와 협력하여 사이버 보안 인력을 성장시키고 개발하기 위한 SG Cyber Talent 이니셔티브를 운영

□ SG Cyber Talent 이니셔티브

- **(운영형태)** SG Cyber Talent 이니셔티브는 재능 있는 사이버 보안 애호가를 어린 나이부터 육성하고, 사이버 보안 전문가가 기술을 심화하도록 돕고 있음. SG Cyber Talent는 기존 인재 유치 및 전문 개발 이니셔티브를 기반으로 구축
- **(비용)** 외부 교육업체를 활용하는 사물 인터넷 보안교육 외에는 CSA가 진행하는 프로그램으로 무료로 진행
- **(과정)** 청소년을 대상으로 하는 SGSG 사이버 청소년 오디세이는 SG Cyber Youth를 포함해 다양한 프로그램을 제공

40) https://www.csa.gov.sg/

[표 3-3] SG Cyber Talent의 주요 과정

과정 명	대상	내용	
SG Cyber Associates	비사이버 보안 전문가	기초교육	ISC2와 협력하여 사이버 보안에서 엔트리 레벨 인증을 취득하고자 하는 싱가포르 참가자에게 기초 교육을 제공
		타깃교육	싱가포르 엔지니어 협회(IES, Institution of Engineers Singapore)와 지역 교육 제공업체와 협력하여 IES 회원을 위한 사물 인터넷 보안교육(IoT Security Fundamentals)
SG Cyber Leaders	보안 실무자	현재 및 미래의 사이버보안 리더가 사이버보안 전략을 형성하는 주요 동인에 대한 이해를 개발하고, 혁신 문화를 육성하고, 조직에서 사이버 보안 기능을 효과적으로 이끌 수 있도록 지원	
SG Cyber Educators	교사 및 학교진로 상담사	사이버 보안 산업 및 학계의 파트너와 협력하여 주도하는 이 프로그램은 교장, 교사 및 학교 진로 상담사에게 다가가 사이버 보안 및 관련 경력 기회에 대한 지식을 접할 수 있는 기회를 제공	
SG Cyber Women	여성	전문대 입학 전 연령의 여성이 사이버보안 분야에 진출하도록 장려	
SG Cyber Youth	청소년	청소년 사이버 탐험 프로그램(YCEP, Youth Cyber Exploration Programme) 부트 캠프와 학생 자원봉사 및 인정 프로그램, 사이버 보안 경력 멘토링 프로그램 등	

[출처] https://www.csa.gov.sg/

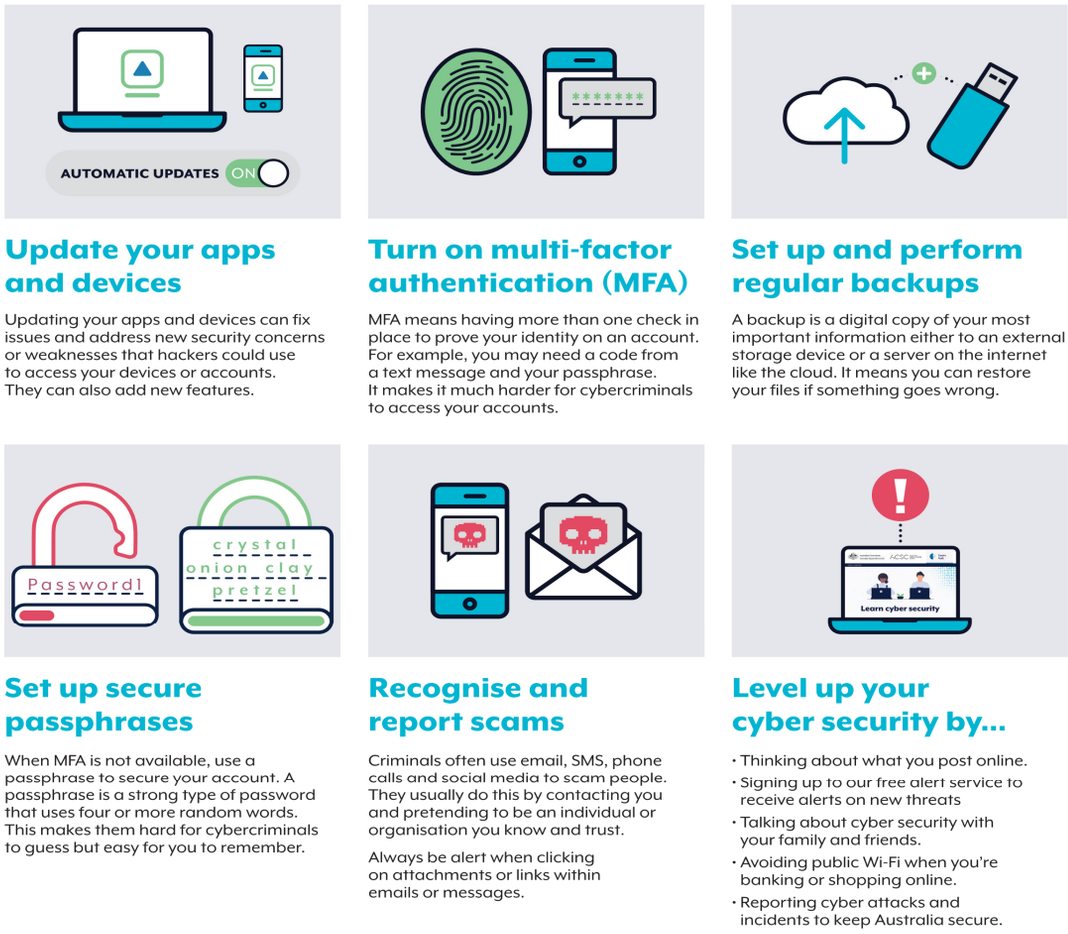
5. 호주

□ ACSC는 사이버보안 위협을 예방하기 위한 지침과 교육을 제공

- 호주 사이버 보안 센터(ACSC, Australian Cyber Security Centre)[41]는 호주 신호국(ASD, Australian Signals Directorate) 내의 사이버 보안에 대한 민간 및 공공 부문의 협력과 정보 공유를 위한 허브
- 일반 국민을 대상으로 온라인에서 자신을 보호할 수 있는 방법에 대한 다양한 정보를 제공
  - 계정보안, 장치보안, 이메일 보안 등에 대한 정보를 제공하고 지식퀴즈와 사례퀴즈 통해 실제 보안위협에 대한 자기평가가 가능
  - 사이버 보안 피해를 겪었을 경우 대응 및 신고절차를 안내

41) https://www.cyber.gov.au/

[그림 3-7] ACSC의 개인을 위한 사이버보안 안내



[출처] https://www.cyber.gov.au/

□ 사이버보안 교육은 인증과 동일하게 RTO에서 제공

- 호주는 국가 직업교육 및 훈련 규제법(National Vocational Education and Training Regulator Act 2011)에 따라 VRQA(Victorian Registration and Qualifications Authority)와 ASQA(Australian Skills Quality Authority)에서 정보보호 교육을 위한 RTO(Registered Training Organisation, 등록된 교육기관)를 검증하고 등록 및 관리
- 각 RTO는 사이버보안 학위를 위한 교육과정과 인증과정이 다양하게 제공되며, 일반국민은 인증된 RTO를 검색하여 필요한 교육에 등록

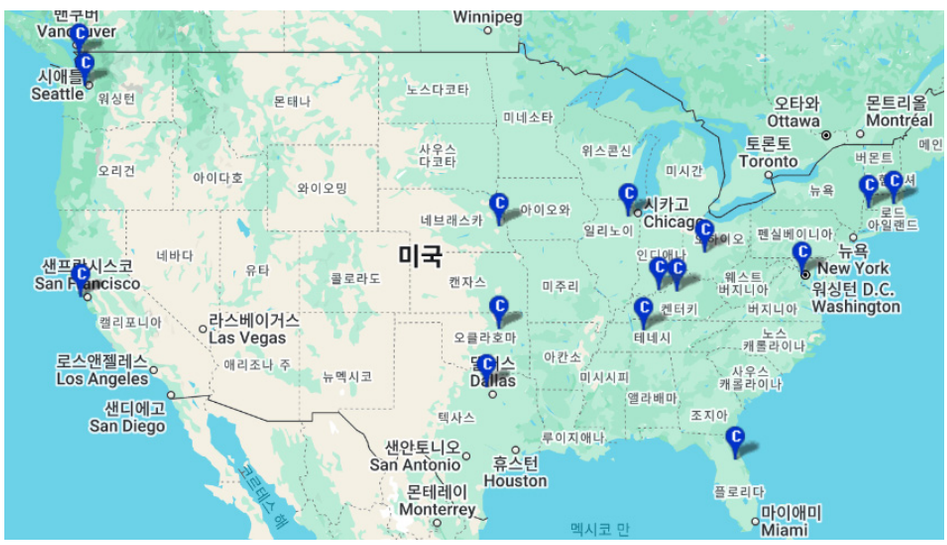
제2절. 교육 프로그램별 커리큘럼 및 운영현황

1. 미국

□ 교육체계

- 국가 사이버보안 이니셔티브(CNCI, Comprehensive National Cybersecurity Initiative)를 기반으로 사이버보안 인력양성 정책을 본격적으로 추진하기 위해, NIST가 설립한 NICE를 중심으로 추진
- 국가과학재단(NSF, National Science Foundation)은 첨단기술교육(ATE, Advanced Technological Education)의 보안기술(Security Technologies) 부분에서 사이버보안 인력양성 센터를 운영

[그림 3-8] **정보 및 보안기술 분야 ATE 센터**



[출처] https://atecentral.net/centers

- NSF는 기초과학의 발전을 위해 잠재력을 가진 솔루션 중심으로 미국의 대학과 대학교의 교육과정에 자금을 지원하는 연방기관
- ATE 프로그램은 국가 경제를 주도하는 산업을 위한 고도로 숙련된 기술자의 교육을 지원[42)]
- 2024년 11월 기준으로 미 전역의 정보 및 보안기술(Information and Security Technologies) 분야 센터는 총 15개

42) ATE 프로그램에서 지원하는 기술 분야에는 첨단 제조 기술(advanced manufacturing technologies), 농업 및 생명 공학(agricultural and bio-technologies), 에너지 및 환경 기술(energy and environmental technologies), 엔지니어링 기술, 정보 기술, 마이크로 및 나노 기술, 보안 기술(security technologies), 학습(learning), 평가(evaluation), 연구(research)가 포함되지만 이에 국한되지는 않음(https://atecentral.net/)

- 보안기술 분야는 National CyberWatch Resource Center, National Cybersecurity Training and Educati | on(NCyTE), National Information Technology Innovation Center(NITIC) 등 총 3개 센터가 운영 중

[표 3-4] 보안기술 분야 ATE 인력양성센터

명칭	운영 프로그램		운영기관	제휴기관
National CyberWatch Center (NCC)[43]	커리큘럼 가이드	• 준학사학위 및 인증 프로그램을 위한 정보 보안 커리큘럼 개발 가이드	Prince George's Community College	고등교육 기관, 공립, 사립학교, 기업 및 정부기관 등 200개 이상
	학위 프로 그램	• 사이버보안 • 디지털포렌식 • 네트워크포렌식 • 네트워크보안 • 보안소프트웨어 개발 • 시스템보안관리		
	자격증 과정	• 클라우드보안 • 디지털포렌식 • 네트워크포렌식 • 네트워크보안 • 보안소프트웨어 개발 • 시스템보안관리 • 무선보안		
National Cybersecurity Training and Education (NCyTE)[44]	K12 커리 큘럼	• AP 컴퓨터과학 원리(사이버 보안) • C5 사이버 보안 개념 수업 • 사이버캠프 • Girls Go Tech 워크숍 • Sticker Heist	Whatcom Community College	고등교육 기관, 공립, 사립학교, 기업 및 정부기관 등
	대학 커리 큘럼	• C5 사이버 보안 개념 수업 • CMMC 인증 워크숍 • 중요 인프라 사이버 보안 과정 • 중요 인프라 보안 및 복원력 • 사이버 인텔리전스 커리큘럼 • 사이버 보안 모듈 • 거버넌스, 위험 관리 및 규정 준수 워크숍 • 건강 IT 개인정보 보호 및 보안 • IoT 기초 워크북 과정		
National Information Technology Innovation Center (NITIC)[45]	• KSAs 사이버 보안 : 사이버 보안에 대한 지식, 기술 및 능력 • 사이버 보안 연구소 및 기술 인큐베이터 : 마이크로 인턴십을 통한 사이버 보안 연구소 및 기술 인큐베이터 구축 • FLEXTech 프로그램 : IT 및 사이버 보안 산업을 위한 응용 견습 모델 가이드		Columbus State Community College	고등교육 기관, 기업 및 정부기관 등

[출처] 각 사이트

43) https://www.nationalcyberwatch.org/
44) https://www.ncyte.net/
45) http://www.nitic.org

2. 이스라엘

□ 교육체계

- **국립대학, 정부 보조금 지원 비영리단체 등 다양한 기관에서 사이버보안 전문가를 양성하기 위한 교육을 제공 중**
  - (Israel Cyber Campus, 이스라엘 사이버 캠퍼스) Tel Aviv 대학에 위치하여 초급에서 고급까지 네트워크 보안, 클라우드 보안, 모의해킹, 디지털 포렌식 등 광범위한 사이버 보안 기술에 대한 교육 제공

[표 3-5] Israel Cyber Campus 교육과정

교육과정명		교육 내용	대상	수강방식
Stage1 (1단계)	SOC Analyst (SOC 분석가)	이론 및 실습 교육을 통해 SOC Analyst가 되기 위해 필요한 기초 과정 교육	사이버보안에 대한 경험이 없는 자	주 2회, 총 75회 온라인
	Super Executives (슈퍼 경영진)	경영진에게 사이버 위협, 리스크 관리, 데이터 보호, 사고 대응 등 사이버 보안에 대한 지식과 기술 제공	기초 사이버보안에 대한 이해도를 높이고 싶은 자	총 10시간 온라인
	Cyber For Managers (관리자)	관리자를 위한 사이버 방법론 지식 및 정보 보안 문제와 용어 교육	신규 보안관리자	온라인 또는 대면
Stage2 (2단계)	From IT To Cyber (IT에서 사이버로)	이론 및 실습 교육을 통해 SOC Analyst가 되기 위해 필요한 기술 제공 (대부분의 수업은 실습 위주로 진행)	경력 초기 IT 전문가 및 정보학, 네트워크, 컴퓨터공학 학위취득자 등	주 2회, 총 30회, 온라인
	Chief Information Security Officer (최고 정보 보안 책임자)	경영진의 관점에서 최고의 정보 보안 표준을 달성하기 위한 정보 보안 및 개인 정보 보호 표준 숙지, 서버 및 사용자 관리의 설계, 역할 및 기능에 대한 개요 등 교육	보안관리자, 보안감사원, 정보 보안 책임자 등	주 2회, 총 30회 온라인
Stage3 (3단계)	Digital Forensics & Incident Response (디지털 포렌식 &사고 대응)	디지털 정보 및 증거를 수집, 보존, 분석, 제시하는 디지털 포렌식 및 사고 대응 블루 팀 양성을 위한, 사고 대응 계획, 포렌식, 사이버 공격 탐지 등 교육	사고대응팀 지망 SOC Analyst	총 120시간 온라인
	Ethical Hacking (윤리적 해킹)	네트워크 스캔, 취약성 평가, 웹 공격 등의 애플리케이션 및 인프라 공격, 모의해킹 과정 수행을 위한, 공격 방법, 모델, 및 프로세스 숙지 및 보안시스템, 포렌식 등 교육	보안 전문가 및 침투테스트 지망 SOC Analyst	총 80시간 온라인

[출처] https://www.israelcybercampus.com/

  - (ITC, Israel Tech Challenge) 정부 보조금 지원으로 이스라엘 첨단산업 인적 자본 부족의 극복을 위한 교육을 제공하는 비영리 단체로 사이버 보안 전문가 양성을 위한 엘리트 프로그램을 운영

[표 3-6] ITC 교육과정

교육과정명		교육 내용	대상
Cyber Security Analyst program (사이버 보안 분석 프로그램)	엘리트 교육 과정 (4.5개월)	1. 인트로 : SQL, 악성공격 등	사이버보안 분야에서 커리어를 시작해 주요 기업에서 교육받기를 희망하는 우수 졸업생
		2. SOC : SEIM, SOC 등	
		3. 운영체계: Windows, Linux 등	
		4. 프로그래밍 : Python, SQL&NoSQL	
		5. 네트워크 : Protocols, Tools, LAN 등	
		6. 기업보안 : 서버, FW, FireEye, GDPR 등	
		7. 암호작성 : Hash, Xor-ing Symmetric & Asymmetric 암호화	
	2개월 프로젝트	사이버 보안 회사와의 워크샵, 기술 인터뷰 준비 등 커리어 준비 및 스킬 연마	

[출처] https://www.itc.tech/

□ 청소년을 위한 사이버보안 교육

- **(교육대상)** 중학생과 고등학생(13학년~17학년)을 대상으로 하며, 사이버 보안에 대한 사전 기술지식이나 경력을 요구하지 않으나, 고급 영어능력, 논리적 사고력 등 교육을 위한 기본적인 학습능력은 필요

- **(커리큘럼)** 네트워크에 대한 기본지식에서부터 암호화, 해킹까지 사이버보안의 다양한 부문을 학습
  - TCP/IP 모델 및 네트워크/애플리케이션 프로토콜 이해
  - Sysinternals 툴을 이용하여 Windows 운영체제 악성코드 감염 분석
  - 암호화 알고리즘, 암호화 모델 및 프로토콜
  - Mitre Att&ck 및 Cyber Kill Chain 모델을 이용한 사이버 공격 실행
  - 비밀번호 열거 및 공격 기술을 사용하여 네트워크 및 호스트에 대한 액세스 권한 획득
  - 웹 애플리케이션 침투 능력

- **(교육이수 조건)** 총 75시간을 수강하며, 수업에 85% 이상 출석하고, 개인과제와 최종 시험을 성공적으로 통과
- **(교육의 특징)** 청소년에게 기술기반을 제공하고 문제해결 능력과 업계 표준 도구에 대한 이해를 통해 십대 경력에 도움
  - 코딩, 프로그래밍 및 기타 기술에 대한 실무 경험을 제공
  - 창의적 사고와 모든 분야에 적용할 수 있는 문제해결 기술을 개발

- 산업에서 사용되는 최신 도구와 기술을 접하여 경력을 쌓기 위한 좋은 출발점을 제공
- 보안 모범사례와 정보보호의 중요성에 대해 학습하여 다양한 직업, 특히 기술 및 금융 분야에서 귀중한 자산
- 이스라엘 정보군에서 중요한 직책을 맡기를 원하는 청소년은 사이버보안에 관한 기본사항을 학습할 필요[46)]
- 비슷한 관심사를 가진 또래를 만나고 연결될 수 있는 기회

□ 관리자를 위한 사이버교육

- **(교육대상)** CEO, 정보보호 관리자, 개인정보보호 관리자, 변호사, 정보 시스템 관리자, 영업사원, 경찰관 및 군인 등 고위 관리자 및 이사를 대상으로 교육

- **(커리큘럼)** 사이버보안의 기본 이해에서부터 조직관리, 국제표준까지 관리자가 알아야 할 다양한 내용을 학습
  - 사이버 및 정보보안의 이해와 기본 용어
  - 사이버보안의 삼요소 : 기밀성, 무결성, 가용성
  - 위협 : 알려진 것과 알려지지 않은 것, 내부와 외부
  - 위험 관리 및 GRC 프레임워크
  - 거버넌스, 위험 및 규정 준수
  - 조직의 이상적인 사이버 보안 계획
  - 사이버보안 사건에 대한 대응 계획 준비
  - SIEM/SOC : 전체 SOC 팀 구성의 중요성
  - 비즈니스 연속성
  - 사이버 공격 중 관리
  - 개인 정보 보호 규정 및 ISO27001/27701 표준

46) 이스라엘 정보군인 8200부대는 대부분 18세~ 21세로 구성되며 군복무를 마친 후에는 대부분 글로벌 IT기업이나 실리콘밸리에서 중요한 직책을 담당

- **(교육이수 조건)** 전체 강의수강으로 이수되며, 약 7개 세션을 주1회 4시간씩 오프라인과 온라인을 번갈아가며 진행

- **(교육의 특징)** 조직 사이버 공격이 발생한 경우 관리자에게 책임이 있으며, 관리자가 현장을 이해하는 것이 중요하다는 목표

□ 실무자를 위한 전문교육

- **(교육대상)** 보안전문가 또는 보안시장을 목표로 하는 IT 기술자 및 전문가
- **(교육과목)** SOC 분석가, IT부터 사이버까지(From IT to Cyber), CISO, 윤리적해킹, 디지털포렌식 및 사고대응 등 성인 전문가 과정이 개설
- **(교육이수 조건)** 전체 강의수강으로 이수되며, 수업에 85% 이상 출석하고, 개인과제와 최종 시험을 통과할 경우
- **(교육의 특징)** 초보자부터 사이버 보안으로 전환하고자 하는 다른 IT 분야 전문자까지 다양한 집단을 대상으로 실습 중심의 수업은 온라인과 오프라인으로 제공

[표 3-7] **이스라엘 사이버보안캠퍼스 전문교육 커리큘럼**

	대상	커리큘럼	교육시간
SOC 분석가	초보자	• 사이버 및 정보 보안의 세계와 기본 용어 • Windows PowerShell 및 배치 스크립트 개발 • TCP/IP 통신 모델 및 네트워크 프로토콜에 대한 이해 • Sysinternals 도구를 사용하여 악성 코드에 감염된 Windows 엔드포인트 분석 • 암호화 알고리즘, 모델 및 프로토콜 이해 • Windows 환경 구축 및 유지 관리 • SQL을 사용하여 데이터베이스를 관리하고 분석 • 클라이언트-서버에서 스크립트를 사용하여 웹 애플리케이션 개발 • 조직이나 애플리케이션에 대한 공격 프로세스 계획 • Miter Att&ck 및 Cyber Kill Chain 방법으로 사이버 공격 • 인터넷 및 네트워크 애플리케이션에서 침투 테스트 수행 • 방화벽, EDR, IDS/IPS, SIEM 등 보안시스템 구성 및 유지 관리 • Office 파일, PDF 및 이메일 분석	총 300시간 온라인 수업
IT에서 사이버	사이버 보안에 관심있는 IT 전문가	• 공격 방법, 모델 및 프로세스 • 악성 오피스 파일을 생성하기 위한 매크로 개발 • 암호공격 기술을 사용하여 네트워크 및 호스트에 액세스 • 공격을 위한 익명 환경 구축 • 웹 애플리케이션 침투 • 터널링 방법 • PowerShell을 사용하여 Windows 환경에서 공격 • 방어자의 관점 이해 – 보안 시스템, 디지털포렌식 • 바이러스 백신, IDS 및 방화벽의 감지를 방지 • 파이썬을 사용하여 멀웨어를 작성하고 악용	총 120시간 온라인 수업

	대상	커리큘럼	교육시간
디지털 포렌식 및 사고 대응	숙련된 보안 전문가	• 사이버 및 정보 보안의 세계와 기본 용어 • Windows PowerShell 및 배치 스크립트 개발 능력 • TCP/IP 통신 모델 및 네트워크 프로토콜 • Sysinternals 툴을 활용하여 악성코드에 감염된 Windows 엔드포인트 분석 • 암호화 알고리즘, 모델 및 프로토콜 이해 • Windows 환경 구축 및 유지 관리 • SQL을 사용하여 데이터베이스 관리 및 분석 • 클라이언트 및 서버 측(클라이언트-서버)에서 스크립트를 사용하여 웹 애플리케이션 개발 • 조직 또는 애플리케이션에 대한 공격 프로세스 계획 • Mitre Att&ck 및 Cyber Kill Chain 방법론을 사용하여 사이버 공격 • 인터넷 및 네트워크 애플리케이션에서 침투 테스트 수행 • 방화벽, EDR, IDS/IPS, SIEM 등 보안시스템 구축 및 유지관리 • 사이버사고 대응 • Office 파일, PDF 및 이메일 분석	총 120시간 온라인과 오프라인 수업 병행

[출처] https://www.itc.tech/

3. 영국

□ NCSC(국가사이버안보센터) 중심

- **안전한 사이버 공간을 위한 공공기관, 산업체, 중소기업 및 일반 대중 대상 교육 진행 및 가이드 제공**

[표 3-8] NCSC 교육과정

구분		프로그램 내용	대상
Schools (학교)	Practical resources for schools	학교의 사이버 위협 관리 및 사이버보안 인식제고를 위한 무료 사이버 보안 교육	학교 관계자
	CyberFirst (사이버퍼스트)	대학교 학부생 대상 장학금 제도	재능있는 젊은 사람들
		CyberFirst Girls Competition 개최	
		11-17세 대상 영국 내 대학교 CyberFirst 과정의 강의 제공	
	Early Years practitioners	우발적인 피해 및 온라인 범죄로부터 민감 정보와 아동을 보호하기 위한 4단계 지침 제공	모두
Higher education (고등 교육)		NCSC가 인증하는 사이버 보안에 관한 15개의 학사 및 통합 석사 학위와 2개의 학위 프로그램 운영	학생, 기업, 대학교
		기존 학위 인증 프로그램을 기반으로 대학, 기업, 학생에게 학위 과정에 대한 품질 평가 및 교육 과정 정보를 제공하는 ACE-CSE 운영	
		조직이 사이버 보안에 대해 체계적이고 사전에 예방하는 접근 방식을 채택할 수 있도록 돕고, 사이버 공격의 가능성과 피해를 줄이기 위한 기본적인 안전 조치를 설명한 Board Toolkit 배포	

구분		프로그램 내용		대상
Professional skills & training (전문기술 & 훈련)		고품질의 사이버 보안 교육 과정을 보장하기 위해 설계된 NCSC 인증 교육 실시	인식 수준 : 사이버 보안에 대한 기초 내용 제공	모두
			응용프로그램 수준 : 전문성 개발을 위한 심화 과정	
			코스웨어 : 공인 강사와 품질 관리 시스템 연계	
Research and academia	ACE-CSR (사이버보안 연구 우수 학술 센터)	정부, 산업 및 학계의 파트너와 협력하여 사이버 보안 교육과 연구의 우수성 지원 및 학술 연구에 대한 업계의 투자 장려		

[출처] https://www.ncsc.gov.uk/

□ 사이버퍼스트(CyberFirst)

- **(교육대상)** 7세부터 대학입학을 준비하는 상급학년까지 연령에 따른 사이버 보안 교육을 제공
- **(교육의 특징)** 저학년을 위한 게임형 교육과 사이버보안을 소개하는 짧은 무료캠프로 구성되어 있으며, 진로를 선택한 중등교육과정 이후(14~15세 이상)에는 사이버보안의 기초과정을 교육
- **(커리큘럼)** 연령과 학년에 맞춘 다양한 교육내용으로 구성

[표 3-9] 연령별 사이버퍼스트 과정

연령	과정명	내용
7세 ~ 11세	Sprinters[47]	• 어린이를 대상으로 한 대화형 온라인 보안 리소스로, 교사가 주도하는 학습 활동과 가정에서 즐길 수 있는 게임으로 구성
11세 ~ 14세	Navigators	• 대화형 비디오서비스로, 사춘기 및 청소년 인터넷 사용자가 접할 수 있는 흔한 사이버 사기와 악성 활동을 강조
12세 ~ 13세	Trailblazers	• 학생을 위한 무료 행사로, 컴퓨터 과학이 미래의 직업에 어떤 역할을 할 수 있는지 생각할 수 있는 교육
	Adventurers	• 학생을 위한 무료 행사로, 컴퓨터 과학이 어떻게 미래의 경력 경로를 향상시킬 수 있는지 확인할 수 있는 기회를 제공
	Investigators	• 학생을 위한 무료 행사이며, 사이버 보안 내의 전문 분야에 대한 이해를 높이고 다양한 기술을 학습
14세 ~ 15세	Defenders	• 일반적인 사이버 보안 위협의 출처 및 영향 식별 • 1차 사이버 방어 정의 및 적용 • 홈 네트워크 구축, 구성 및 보안 • 개인 디지털 발자국을 관리하기 위한 단계 수행
15세 ~ 16세	Futures	• 사이버 공격의 동기 탐구 • 사이버 공격으로부터 자신을 보호하는 방법 • 네트워크에 대한 지식과 이해 개발 • 네트워크를 공격으로부터 보호하는 방법 • 리소스를 다른 사람들에게 제공하고 안전하게 보호하는 방법
16세 ~ 17세	Advanced	• 디지털 포렌식 구현 • 암호화 기술 이해 • 오픈소스 인텔리전스 기술 활용 • 침투 테스트

[출처] https://www.ncsc.gov.uk/cyberfirst

□ Cyber EPQ(Extended Project Qualification)

- **(교육대상)** 14세 이상 일반인이면 누구나 참여할 수 있으며, 중등교육과정인증(GCSE 레벨) 또는 이와 동등한 수준을 권고

- **(커리큘럼)** 10개의 핵심 필수 모듈과 3개의 전문가 모듈이 포함된 총 11개의 모듈로 구성

[표 3-10] Cyber EPQ 커리큘럼

모듈	설명
사이버 보안 소개	• 윤리적 해킹의 간략한 역사 • 데이터의 기밀성, 무결성, 가용성(CIA 3요소) • 컴퓨터 오용 방지법
컴퓨팅 및 암호화의 역사	• 코드와 암호 체계에 대한 연구 • 비밀 문자를 코드나 암호로 만들고 사용하는 절차, 프로세스, 방법
사이버범죄	• 사이버 의존 범죄(정보 통신 기술을 사용하여 저지르는 범죄)와 사이버 지원 범죄(전통적인 범죄를 정보통신 기술을 활용하여 규모나 범위를 확대하는 범죄)를 이해
위험평가, 관리 및 거버넌스	• 조직의 자본과 수입에 대한 위협을 식별, 평가 및 통제하는 프로세스 • IT 보안위협과 데이터 위험, 위험관리 전략 • 거버넌스 원칙을 위험의 식별, 평가, 관리 및 커뮤니케이션에 적용 • 사이버 보안 관행의 윤리
보안테스트 및 취약성 평가	• 시스템의 위협을 식별하고 잠재적인 취약성을 측정 • 주어진 시스템의 위협에 대한 가능한 취약성을 식별, 정량화
디지털포렌식	• 데이터 저장 매체에서 정보를 추출하고, 사용가능한 형태로 변환하고, 처리 및 해석
사고대응관리	• 보안 침해 또는 사이버 공격의 후유증을 해결하고 관리
ID 및 엑세스 관리	• 조직 내에서 사용자 신원을 관리하고 사용자 액세스를 규제하는 데 사용되는 제품, 프로세스, 정책 • 네트워크 및 애플리케이션 액세스를 중재하기 위한 공통 보안 프레임워크 • 조직에서 수집, 관리, 저장 또는 처리하는 모든 개인정보보호 원칙
보안감사, 규정 준수 및 보증	• 회사가 모든 해당 법률, 규칙 및 규정, 내부행동 강령, 정책 및 절차를 준수하고 있는지 합리적으로 보장하기 위한 감사 준수 기능 • 회사의 내부 통제 환경을 적절성, 효율성 및 효과성에 대해 모니터링하고 평가
사이버보안의 인적오류	• 비밀번호 공유, 패치 관리 부족, 안전하지 않은 URL을 두 번 클릭, 개인 기기를 통한 조직적 접근 등의 인적오류
침투테스트	• 적이 사용하는 것과 동일한 도구와 기술을 사용하여 해당 시스템의 보안 중 일부 또는 전체를 테스트
소프트웨어 보안 및 아키텍처	• 소프트웨어를 악의적인 공격 및 기타 해커 위험으로부터 보호하여 소프트웨어가 이러한 잠재적 위험에도 불구하고 계속 올바르게 작동할 수 있도록 구현 • 회사의 목표에 맞춰 조직을 사이버 위협으로부터 안전하게 보호하도록 설계된 보안 원칙, 방법 및 모델 세트

[출처] https://cyberepq.org.uk/

- **(교육이수 조건)** 온라인 수업에 대한 출석과 퀴즈 등 과정 평가

- **(교육의 특징)** 학생은 1년~2년으로 과정을 분산할 수 있으며 기존 교사가 감독 및 평가를 시행하고, 일반인은 1년 간 CIISec에서 임명한 감독자가 제공하는 감독 및 지원

47) https://www.ncsc.gov.uk/collection/cybersprinters/the-game

4. 싱가포르

□ CSA, 싱가포르 사이버 안보국

- 2015년 설립, 정보통신부 산하로 안전한 사이버 공간 및 국가 안보를 뒷받침하는 인력 구축을 위해 학교, 산업계와 협력하고 다양한 교육 프로그램을 운영

[표 3-11] 싱가포르의 사이버 보안 교육 프로그램

구분	프로그램명	내용
Talents & Skills Development (인재 및 기술 개발)	Cybersecurity Career Mentoring Programme (사이버보안 진로 멘토링 프로그램)	CSA와 SCS의 공동 계획으로 2017년 시작하여 사이버 보안 업계 전문가로부터 진로 지도 및 지원을 받을 수 있는 플랫폼 제공
	SG Cyber Talent (SG 사이버 탤런트)	재능 있는 사이버 보안 인력을 육성하고, 사이버 보안 전문가들이 기술을 심화할 수 있도록 지원 프로그램 운영
Support for Enterprises (기업 지원)	SG Cyber Safe Programme (SG 사이버 안전 프로그램)	싱가포르 기업이 디지털 영역에서 사이버 보안을 강화할 수 있도록 정보 및 교육 제공
	PSG Cybersecurity Solutions (PSG 사이버보안 솔루션)	중소기업의 디지털화 단순화를 목표로, 시장에서 입증되고, 비용이 합리적이며, 신뢰할 수 있는 사전 승인된 디지털 솔루션 업체 리스트를 제공하고, 사용하는 중소기업에게 자금 지원
Cybersecurity Outreach (사이버보안 지원활동)	SG Cyber Safe Seniors (SG 사이버 안전 시니어)	시니어들의 사이버 보안에 대한 인식을 높이기 위한 프로그램
	SG Cyber Safe Students (SG 사이버 안전 학생)	학생들에게 사이버 보안에 대한 인식을 높이고 좋은 사이버 보안 관행 채택 장려를 목표로 교육 프로그램을 계획
Innovation Schemes (혁신 계획)	CSA Cybersecurity Co-Innovation and Development Fund	국가 사이버 보안 요구 충족을 위해 혁신적인 사이버 보안 솔루션 개발을 촉진하는 프로그램
	ICE71	급증하는 사이버 보안 위험을 완화하기 위한 역량과 심층 기술을 유치하고 개발

[출처] https://www.csa.gov.sg/

□ SG 사이버 청소년 오디세이(SG Cyber Youth Odyssey)

- **(교육대상)** 중등 및 고등교육 수준의 학생을 대상으로 사이버 보안 직업을 탐구하고, 관련 기술지식에 노출될 수 있는 기회를 제공
- **(커리큘럼)** '흥미(Excite)', '탐색(Explore)', '경험(Experience)', '뛰어남(Excel)[48]'의 4단계로 구분하여 다양한 수준의 사이버보안 지식을 가진 학생들이 사이버보안을 점진적으로 탐구하고 발전

[표 3-12] SG 사이버 청소년 오디세이 커리큘럼

		흥미(Excite)	탐색(Explore)	경험(Experience)
대상		• 사이버보안에 대한 지식이 전혀 없는 학생	• 사이버 보안에 대한 지식이 제한적인 학생	• 사이버보안에 대한 지식이 있고, 사이버보안을 미래의 직업으로 고려하는 학생
실습 단계		• 모바일장치 보안	• 네트워크 보안	• 웹앱, IoT 및 침투테스트
커리큘럼	사이버 보안 기본	• 사이버보안 환경 • 직업전망 • 인증(자격증명, 암호화)의 개념	• 윤리적 해커에 대한 이해 • 사이버보안 직무역할의 이해 • 사이버보안 원칙, 용어	• 보안사고 관리 및 대응 프레임워크
	암호학	-	• 암호학 개념	• 암호학 기초(대칭 암호 알고리즘과 비대칭암호알고리즘의 차이, 암호화를 사용하여 메시지 보내기)
	모바일 보안	• 사회공학 • 모바일보안 이해	-	• 모바일보안 기초(루팅, 탈옥 등 기본 침투테스트)
	네트워크 보안	• 네트워트 기본사항 이해 • 무선네트워크 보안	• 심층네트워킹(네트워크 프로토콜 및 장치, MAC 주소, VPN, IPS/IDS/방화벽, ARP 및 일반 네트워크 맨인더미들 공격	• 네트워크 정찰(프로토콜분석, 네트워크 스캐너, 무선 스캐너. 크래커)
	침투 테스트	-	• 침투테스트 이해	• 침투테스트 수행(SQL 주입, 버퍼, 오버플로, 오타스쿼팅 및 ARP 중독)
	기술 및 스크립팅	-	-	• 자바스크립트 • HTML
	운영체제, IoT 장치 및 멀웨어	• 컴퓨터 및 위협 이해(컴퓨터의 구조, 작동방식)	• 멀웨어 기본(악성코드 이해) • 리눅스의 이해 • IoT 디바이스 이해	• 윈도우 운영체제 이해
	오픈소스	-	• 검색엔진, 소셜미디어의 이해	-

[출처] https://www.csa.gov.sg/

48) excel 단계는 수업이 아닌 SG Cyber Olympians 대회에 참여하는 과정

- **(교육의 특징)** SG 사이버 청소년 오디세이 사이버보안에 대한 학습 로드맵이며, 교사, 진로상담사가 훈련 부트 캠프, 대회, 학습, 진로 멘토링 세션 및 학교 강연을 통해 청소년의 활동 및 교육수행은 안내

□ 엔지니어를 위한 IoT보안 기본 코스

- 싱가포르 엔지니어 협회(IES, Institution of Engineers Singapore)에서 IES 회원을 위해 사물인터넷 보안 과정을 개발하고 구성
- **(교육대상)** IoT 보안에 대한 기초 지식을 필요로 하는 전문가
- **(커리큘럼)** 수강 이후 별도의 평가가 없는 2일간 진행되는 직장인을 위한 단기코스

[표 3-13] **IoT보안 기본코스 커리큘럼**

차수	내용
1일차	• IoT 보안 소개 – 네트워크 기본(X.200 – OSI-RM) – 보안 기본(CIA/AAA) • 임베디드 장치 보안 – 컴퓨팅 기초(폰 노이만 아키텍처) – 센서(변환기) 액추에이터 및 보안 • 통신 보안 – 액세스 네트워크 및 보안(IEEE/ETSI) – TCP/IP 네트워크 및 보안(IETF) • 애플리케이션 보안 – IoT 프로토콜 및 보안(MQTT/OPC-UA) – 웹 및 코드 보안(OWASP)
2일차	• 표준 및 규정 – 중요 정보 인프라 v2 – 컴퓨터 오용 방지법 및 개인정보보호법 • 위험, 위협, 취약성 및 결과 – 위험 관리 – 컴퓨터 측정(CIS 벤치마크) • IoT 보안 사례 연구 및 실습 활동 • IIOT 데모 및 평가 • 전문가 참여 토론

[출처] https://www.ies.org.sg/

- **(교육의 특징)** 교육의 마지막에는 전문가 참여 토론이 있어, 실무 전문가와 질의응답이 가능

5. 호주

- ACSC(호주 사이버 보안 센터)에서 사이버 보안에 대한 민간 및 공공 부문의 협력과 정보 공유를 위한 허브로, 사이버 보안 위협을 예방하고 피해를 최소화하기 위한 지침 제공 및 교육 실시

[표 3-14] 기초 교육과정

교육과정	교육 내용
ISM: Information Security Manual (정보 보안 매뉴얼)	ISM 사용에 대한 지침 제공
	ISM의 사이버보안 원칙에 따라 시스템 및 데이터 보호법
	사이버 위협으로부터 시스템 및 데이터를 보호하는 방법 지침 제공
	사이버보안 용어에 대한 지침 제공
	ISM 발간 기록 목록
	과거와 현재의 OSCAL 포맷에서의 ISM 발간
Essential Eight (사이버보안 사고 대처를 위한 8가지 필수 전략)	Essential 8에 대한 개요
	Essential 8 평가 방법
	Essential 8 구현 방법
	Essential 8과 ISM(정보 보안 매뉴얼) 내 컨트롤 간의 매핑
Protecting your business and employees (기업체 및 직원 보호)	통제된 환경에서 사이버보안 관행 평가 및 개선을 위한 플랫폼 제공
	사이버보안 사고에 대응하기 위한 사고 대응 계획 수립
	사이버보안 전문가를 위한 개발 경로를 제공
	기술, 지식을 국내 및 국제 산업 표준에 맞게 개선, 개발
Small Business Cyber Security (중소기업 사이버 보안)	중소기업 사이버 보안 가이드
	중소기업 클라우드 보안 가이드
	랜섬웨어로부터 보호하는 방법
	비즈니스 이메일 보안 가이드
	사이버보안 테스트 법
Strategies to Mitigate Cyber Security Incidents (사이버보안사고 완화전략)	사이버보안사고 대처를 위한 고급 전략 개발 및 교육

[출처] https://www.cyber.gov.au/

[표 3-15] 장치 및 시스템 유지 관련 교육과정

교육과정	교육 내용
Cloud security guidance (클라우드 보안 지침)	정부 및 업계 전반에 걸쳐 안전한 클라우드 서비스를 지원하는 클라우드 평가
	클라우드 서비스 구현 방식에 따른 클라우드 컴퓨팅 보안 고려 사항
	사이버 보안 팀, 클라우드 설계자 및 비즈니스 담당자가 공동으로 리스크 평가를 수행하고 클라우드 서비스를 안전하게 사용할 수 있도록 지원
	클라우드 서비스 보안 상태 검증을 위한 클라우드 컴퓨팅 보안

교육과정	교육 내용
Critical infrastructure (중요 인프라 기반)	데이터를 캡처, 통신 및 분석하는 스마트 정보 통신 기술(ICT) 지원 시스템 및 장치 모음을 사용하여 시민에게 향상된 서비스를 제공하도록 설계된 스마트 플레이스 보안
	중요 인프라에 사용되는 장비에 결함 발생을 대비한 산업 제어 시스템 원격 액세스 프로토콜
	산업 제어 시스템에 대한 사이버 위협 이해 및 피해 예방
	운영 기술 환경에 대한 원격 액세스
Outsourcing and procurement (외주 및 조달)	사이버 공급망 위험 관리
	관리되는 서비스의 제공 및 사용
Remote working and secure mobility (원격 근무 및 안전한 기기사용)	원격 근무 증가에 따른 모바일 기기의 안전한 사용 및 보안 방법
System hardening and administration (시스템 강화 및 관리)	도메인 보안
	게이트웨이 서비스 강화
	기타 사이버 보안 항목
	네트워크 인프라 강화
	안전한 시스템 관리
	응용 프로그램 및 ICT 장비의 강화
	효과적인 시스템 모니터링 수행
	World Wide Web을 통해 액세스할 수 있는 서비스 강화

[출처] https://www.cyber.gov.au/

□ 모나크 연구소(Monarch Institute)의 학위과정

- **모나크 연구소는 전문지식을 교육하고, 관련 자격증을 발급하고 있으며, 기술 자격인증 과정과 함께 학위과정을 제공**
- **정보기술학 석사(사이버 보안 및 고급 네트워킹)**
  - **(교육대상)** 사이버 보안에 관심있는 IT전문가
  - **(검정내용)** 기초기술, 사이버보안, 네트워킹, 사고 테스팅, 리더십기술 증 5개 부문의 세부 항목으로 구성

[표 3-16] 사이버 보안 및 고급 네트워킹 과목

부문	내용
기초 기술	• 필수적인 사이버 보안 기본사항과 모범 사례를 학습 • 광역 네트워크(WAN) 기술, 기본 보안, 경로 및 스위치 작업을 포함한 네트워킹 기본 사항을 활용하는 방법 • Java를 사용한 입문 프로그래밍 작업 수행
사이버 보안	• 위협 데이터를 수집, 분석, 해석하는 방법 • 중요한 인프라를 보호하고 특정 설계 방법론을 사용하여 보안 아키텍처를 설계하는 데 필요한 도구와 지식 • ICT 환경에서 윤리 및 개인 정보 보호 정책을 적용하는 방법
네트워킹	• 가상 컴퓨팅 환경을 설치, 구성 및 관리하는 방법 • 운영 체제 설치 및 업그레이드, 조직의 전략적 방향과 ICT 요구 사항의 일치
사고 테스팅	• 사고 대응 계획을 개발하고 재해 복구 및 비상 계획을 검토하고 업데이트하는 기술 • 이메일, 웹 포털 또는 협업 도구와 같은 엔터프라이즈 커뮤니케이션 솔루션의 배포 및 관리를 관리하는 방법 • 요구 사항을 충족하고 보안이 유지되도록 네트워크 서버를 설계, 구축 및 테스트하는 방법
리더십 기술	• 네트워크 보안 관리와 클라이언트 문제에 필요한 지식 • 복잡한 ICT 네트워크를 설치하고 관리하는 방법을 배우고 팀 환경에서 효과적인 리더가 되는 방법

[출처] https://www.monarch.edu.au/

- **(교육이수 조건)** 사례연구, 단답형 테스트, 프로젝트, 롤플레이 등으로 종합 평가

- **(교육의 특징)** 18개월~ 24개월 간 진행되는 온라인강의로 제공되며, 수강생과 커뮤니티를 운영

제3절. 국내 주요 교육프로그램과 비교

1. 국내 정보보호 교육 프로그램

□ 한국인터넷진흥원(KISA, Korea Internet Security Agency)은 정보보호 인력양성을 위한 대학 지원 및 교육을 제공

○ 정보보호 특성화 대학 지원

- 정보보호 직무별 특화된 융합·연계 전공 운영 및 산학협력 기반의 교육과정 개발을 통한 직무 중심의 정보보호 전문인력 양성
- 국내 4년제 대학의 정보보호 관련 유관 학과·전공에 정보보호 직무별 특화된 학과·전공 등 운영에 필요한 전문 실습장 구축, 커리큘럼 개발 및 산학협력 등 지원

○ K-Shield 주니어

- **(목적)** 정보보호 산업 실무 기반의 실습 교육(200시간) 제공을 통해 산업계 진출 시 즉각 실무 투입이 가능한 정보보호 인재 양성
- **(교육대상)** 고등학교 졸업자 또는 대학 최종학년 재학생 및 졸업자 대상(만 19세 ~ 34세)으로 서류 및 면접 평가 후 선발
- **(커리큘럼)** 정규과정과 단기 집중과정으로 구성

[표 3-17] **K-Shield 주니어 정규과정 커리큘럼**

부문	내용	
보안관리 및 진단	정보시스템	• 위험관리 및 정보서비스 흐름도 • 취약점 분석 평가 방법
	개인정보	• 개인정보의 이해 및 개인정보 흐름도 • 가명화 및 비식별화
침해사고 분석 대응	디지털 포렌식을 활용한 침해사고 분석 대응	• 디지털포렌식과 침해사고분석 • 윈도우 운영체제 아티팩트 • MITRE ATT&CK 등 침해사고 지표분석 • 메모리 분석 • 리눅스 운영체제 아티팩트 • 서비스 로그 및 취약점 흔적 분석

부문	내용	
취약점분석	웹 취약점 분석	• Python 웹 개발 • 웹 취약점 분석
	시스템 취약점 분석	• 시스템 해킹 기초 • 단위 공격 기술 학습 • 메모리 보호기법 • 1-Day 취약점 분석

[출처]https://academy.kisa.or.kr/

AI 보안관제

- **(목적)** AI 보안관제 실무 기반의 교육(230시간) 제공을 통해 산업계 진출 시 즉각 실무 투입이 가능한 정보보호 인재 양성
- **(교육대상)** 고등학교 졸업자, (전문)대학 최종학년 재학생 및 졸업자 대상으로 모집 후 선발
- **(교육의 특징)** AI 보안관제 실전형 훈련장에서 실습
- **(커리큘럼)** 공통과정과 실무과정으로 구성

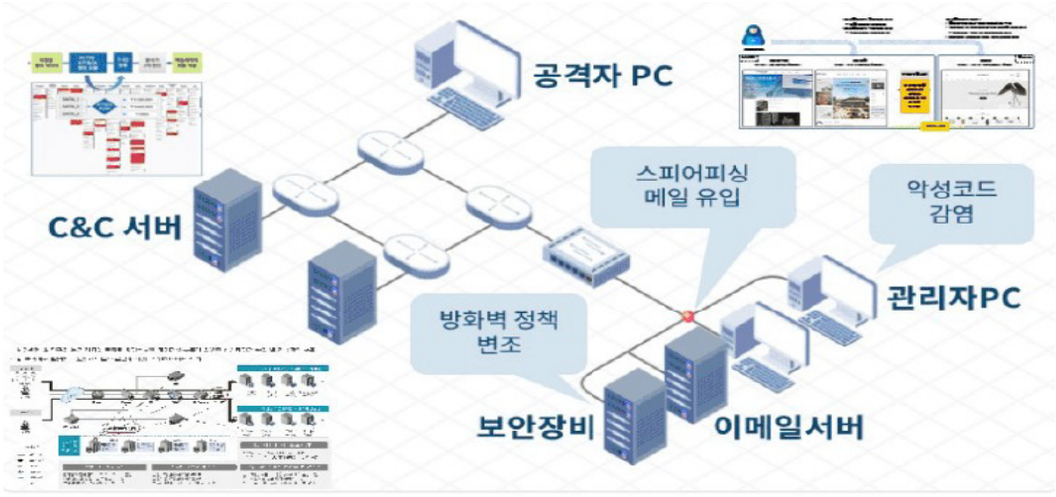
[표 3-18] AI 보안관제 커리큘럼

부문		내용	시간
공통과정	정보보호 개론	정보보호 개요	2H
		공격 및 방어 기법	2H
		정보보호 법률	1H
		직무소개	3H
	시스템 보안	운영체제 기초	8H
		시스템 공격 및 방어	16H
	네트워크 보안	네트워크 기초	8H
		네트워크 공격 및 방어	16H
	웹 보안	웹 기초	8H
		웹 공격 및 방어	16H
실무과정	보안관제 실무	정보보호강화를 위한 보안관제 고도화 방안	4H
		통합보안관제시스템 운영방안	4H
		공격 시나리오 기반의 보안관제 고도화 방안	24H
		보안관제 운영시 침해사고 대응방안	8H
	보안장비의 이해	침입차단시스템의 이해(F/W)	4H
		침입탐지시스템의 이해 (IDS/IPS)	4H
		네트워크 접근제어 시스템의 이해(NAC)	4H

부문		내용	시간
		Snort 룰의 이해(Snort)	4H
		통합보안 시스템의 이해(SIEM/SOAR)	24H
	보안관제 실무	머신러닝 기반의 보안관제	24H
		생성형 AI를 활용한 보안관제	16H

[출처] https://academy.kisa.or.kr/

[그림 3-9] AI 보안관제 실전형 훈련장 실습 시나리오



[출처] https://academy.kisa.or.kr/

○ 최정예(K-Shield) 정보보호 전문인력 양성

- **(목적)** 지능화되는 사이버 공격에 즉시 대응할 수 있는 최정예 정보보호 전문인력 양성
- **(교육대상)** 한국인터넷진흥원과 협약이 체결된 기업에 재직 중이며, 고용보험을 납부하고 있는 재직자 대상

[표 3-19] 최정예(K-Shield) 정보보호 전문인력 양성 과정

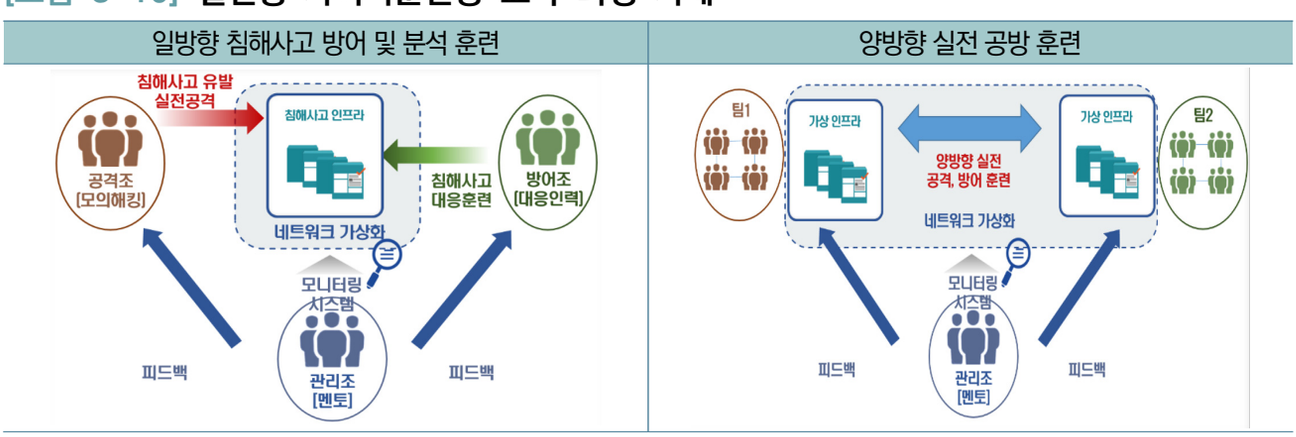
부문	내용
(입문) 운영보안	보안관제 등
보안컨설팅	위험평가, 보안컨설팅 실무, 관리자 컨설팅 등
침해사고 대응	취약점 점검, 사고 증거수집, ICS 보안 등
모의해킹	War게임 문제풀이, 웹 모의해킹, 모의침투 등
악성코드 분석	생성형 AI 활용, 리버싱 인증우회, 악성코드 분석 등
디지털 포렌식	사고 로그분석, 감사기법, 포렌식 분석 등
클라우드 보안	CSAP 이해, 클라우드 보안, 멀티클라우드 보안 등
WEB/SW 개발보안	안티바이러스 개발, 웹해킹 실무, Spring 프레임워크 등

[출처] https://academy.kisa.or.kr/

○ 실전형 사이버 훈련장(Security-Gym)

- **(목적)** 해킹공격 발생 시 즉각적인 탐지 및 대응이 가능하도록 보안기술 실전 훈련 프로그램을 통해 실전형 사이버보안 전문인력 양성
  - · 과학기술정보통신부와 KISA(한국인터넷진흥원)가 함께 '사이버보안 10만 인재양성 계획'의 일환으로 추진
  - · 침해사고 상황에 대한 충분한 이해와 함께 실습 훈련을 할 수 있어서 구직자 및 재직자들로부터 매년 높은 교육 수요
- **(교육시설)** 교육생 확대를 위해 교육훈련 서버 증설(4대 → 10대), 실시간 해킹방어 훈련 등 교육과정을 확대(7개 → 19개) 하고, 정보보호 제품 실습을 위한 제품군을 추가(2종 → 12종) 구비(2023년 7월)
- **(교육대상)** 보안 관련 구직자 및 재직자 대상
- **(교육방법)** 해킹 시나리오 기반으로 가상의 침해사고 환경을 구축하고, 침해사고 조사, 침해공격·방어훈련, 상용 정보보호 제품에 대한 실습 등 수준별 교육 과정을 편성·지원
  - · **(일방향 침해사고 방어 및 분석 훈련)** 가상의 기업 인프라 환경에 대한 침투를 방어하고, 침투 사례에 대한 취약점 정보수집·분석을 통한 대책을 수립
  - · **(양방향 실전 공방 훈련 과정)** 가상의 기업환경에 접속하여 각 팀별로 할당된 인프라에 대한 방어와 동시에 상대 인프라를 공격하는 절차와 방법을 훈련하면서 실질적인 침투사고에 대응

[그림 3-10] 실전형 사이버훈련장 교육 과정 사례



[출처] https://academy.kisa.or.kr/

- **(교육과정)** 침해사고 사례에 기반한 주요 위협행위, 악성코드, 아티팩트 등을 훈련콘텐츠로 제공

[표 3-20] 실전형 사이버훈련장 교육과정

구분	과정명	훈련과정 운영 방향개요
초급	MITRE ATT&CK 활용	MITRE ATT&CK 구성 요소 및 활용 사례를 설명, TTPs를 선정하여 분석하고 탐지 방법 실습
	정보보호제품군-기초1	보안제품의 이해를 위한 네트워크 및 서버 기본 구조
	정보보호제품군-기초2	시스템, 네트워크, 웹 어플리케이션 모의 해킹
	YARA 기반 정규 표현식 활용	정규 표현식 문법 학습 및 sed, awk를 활용한 텍스트 가공 실습, YARA 룰 활용을 통한 위협 탐지
	리버스 엔지니어링	IA-32/64, ARM 환경에서 실행 파일의 구조를 파악하고, 디스어셈블된 코드를 읽고 디버깅 실습
중급	정보보호제품군-기본1	UTM, WAF, Webproxy, Web Filter, SSL/TLS 가시화 도구 실습
	정보보호제품군-기본2	CDR, NAC, DLP로 확장된 제품군 활용 실습
	정보보호제품군-활용1	EDR, SIEM, SOAR로 확장된 제품군 활용 실습
	정보보호제품군-활용2	CTI, Threat Hunting로 확장된 제품군 활용 실습
	스피어피싱대응-기본	스피어피싱 과정을 이해하고 관련된 악성행위 분석
	스피어피싱대응-심화1	악성 HWP 파일 상세 분석
	스피어피싱대응-심화2	악성 MS-Office 파일 상세 분석
	멀웨어 식별 훈련	악성스크립트, 파일, 프로세스에서 사용하는 함수 및 동작기법 분석, 난독화 기법 이해 및 해제 실습
	위협 이벤트 식별 훈련	공격자의 위협 행위로 발생하는 시스템 이벤트를 식별하고 설명
고급	MITRE ATT&CK 기반 RedTeaming	사이버위협 인텔리전스 분석 및 TTPs 추출, 위협 에뮬레이션 플랜에 따른 공격 시나리오 구성 및 구현, 공격 인프라 구축 및 플랜에 따른 공격 수행
	침해사고 조사 훈련	공격자의 위협 행위로 발생하는 시스템 이벤트(로그 및 아티펙트)를 MITRE ATT&CK TTPs 기반으로 분석, 침해사고 원인 및 경과 분석
	시나리오 기반 침해사고 조사 및 공격 훈련	실제 해킹사건 시나리오 기반의 침해사고 환경에서 원인 분석 및 조사, 공격자 입장에서 공격 수행
	CTF기반 공격 및 방어 훈련	팀별로 동일하게 주어진 인프라에서 상대 인프라의 취약점을 공격하고, 자신의 취약점은 패치하는 훈련
	실시간 공격, 방어 훈련	실시간으로 발생하는 해킹(공격)을 방어하는 훈련

[출처] https://academy.kisa.or.kr/

□ KISIA는 정보보호 인력지원을 위한 교육을 시행

○ 한국정보보호산업협회(KISIA, Korea Information Security Industry Association)는 정보보호 산업 지원, 조사연구와 인재 지원을 위한 교육사업을 시행

[표 3-21] KISIA의 전문인력 양성 과정

과정 명	대상	내용	특징
S-개발자	정보보호분야 진출을 희망하는 SW개발 전문가	• 실습 위주의 보안전문화 집체교육(공통 1개월, 심화 2개월) 실시 • 정보보호제품 R&D 개발 주제 선정, 보안SW전문 기업의 멘토링을 통해 정보보호제품 기획·개발 실습	취·창업 지원
시큐리티 아카데미	정보보호분야 구직을 희망하는 대학졸업(예정)자 및 미취업자	• (기업형) 인력수요가 있는 기업의 채용직무에 따른 교육과정 • (직무형) 정보보호 직무에 대한 전문화된 커리큘럼 구성으로 다수의 정보보호 기업에 대한 폭넓은 채용직무 탐색	기업이 인재선발, 교육에 참여하는 채용연계형
ICT융합 산업보안 인력양성	해당 분야 관련 업계 재직자, 대학(원)생 및 졸업(예정)자	• 8개 산업분야(스마트 자동차, 스마트 제조, 스마트 홈·가전, 스마트 의료, 블록체인, 메타버스, 클라우드, SW공급망)에 대한 기초 및 심화과정	이론과 실습을 병행하는 보안사고 대응방안 교육
AI보안 기술개발 인력양성	대학(원)생 및 졸업(예정)자 등 정보보호 진출 희망자	• 악성코드, 네트워크, 개인정보보호에 대한 기초과정이며, 이후 S-개발자 과정 지원 시 서류전형이 면제	이론과 실습을 포함한 실무 기반의 융합보안 프로젝트 수행
온택트 융합보안	정보보호 역량 향상을 희망하는 누구나	• 융합보안의 기초(네트워크 보안, 시스템보안. 클라우드 보안, IoT보안, 디지털포렌식 등)	온라인 원격수업
개인정보보호 국가인적자원개발 컨소시엄	고용보험에 가입한 협약기업 해당 분야 관련 업계 재직자	• 개인정보보호 기초 • 개인정보 처리방침 작성 실무 • 개인정보 안전성 확보조치 • 가명정보 결합 및 반출 검토 • 가명정보 위험성 검토 및 처리 실무 • 개인정보 침해사고 매뉴얼 작성 • 개인정보 침해사고 유출 대응 • 개인정보 영향평가 지표 분석 • 개인정보보호 진단 및 점검 • 개인정보보호 예비 책임자 실무 • 디지털헬스 의료 개인정보 보호 및 처리 • 스마트홈(IoT) 정보보호 기술 • 모빌리티 분야 영상정보 활용 및 처리	재직자 역량강화 개인정보보호 교육프로그램
중소기업 기술보호 인력양성 교육	기술보호에 관심있는 중소기업 재직자 (집체 교육),예비 재직자(온라인 교육) 등	일반: • 중소기업 기술보호의 이해 • 중소기업 기술보호 지원체계 • 중소기업 기술보호 지원제도 심화: • 시스템 보안 : 기술유출 대응 전략(정보보안), 기술유출 방지 기술, 침해사고 대응 가이드 등 • 클라우드 보안 : 클라우드 기술유출 사례, 클라우드 도입 시 고려사항, 클라우드 기술 트렌드 이해 및 안전한 활용 방안 등 • AI 보안 : AI 기술유출 현황, 생성형 AI 관련 데이터 유출 대응, AI 구축 시 기술보호 쟁점, AI 활용 단계의 기업데이터 보안 방안 등	전액 무료 교육, 다과 지원, 현업 종사자의 실무교육 진행, 수료증 발급 등

과정 명	대상	내용	특징
청년취업 사관학교	정보보호 기초역량을 보유한 만 15세 이상 서울시민	• 보안관제, 네트워크 보안, 웹 구조 및 보안, 시스템 보안, 모의해킹, 침해사고 대응, 주요통신기반시설점검, 디지털 포렌식, 리눅스 기초/실습, 악성코드 분석, 컨설팅, 정보보호 법제도 등	채용연계형 교육과정

[출처] https://academy.kisa.or.kr/

- **대학 정보보호 동아리 지원사업을 통해 정보보호 기술력 향상 및 윤리관 함양을 위한 전문 실습교육 및 연구 활동, 취업 멘토링 지원**
  - 국내 2~4년제 대학(원) 정보보호 관련 동아리 20개를 지원하고, 활동에 따른 우수 동아리 선정
  - 세미나, 실습교육, 기업 견학, 멘토데이 등을 통해 정보보호 인식향상과 정보보호 기술력 향상을 지원

□ 과학기술정보통신부와 정보통신기획평가원은 **융합보안대학원** 선정 및 운영

- **정보보호 특성화 대학 지원**
  - ICT 융합산업 보안 위협 확대에 대응하여 융합보안 분야 석·박사급 고급 인재를 양성하기 위한 융합보안대학원 선정 및 운영
  - 융합보안에 특화된 교육과정 개발, 전용 실습장 구축, 장학금 지급, 산·학 연계 융합보안 프로젝트·인턴쉽 등을 통해 산업 현장 중심형 인력 양성 추진
  - 2024년 기준으로 현재 12개의 융합보안대학원을 운영하고 있음

□ 국내 정보보호 교육은 실무인력 양성을 위한 국비지원과정 중심

- **정보보호 산업의 높은 수요를 즉시 해결할 수 있는 실무자 양성 중심의 교육과정**
  - 사이버 보안 위협이 증가하면서 정보보호 인력의 수요는 급증하고 있으나, 보안인력의 공급은 이에 미치지 못하는 수급불균형이 지속[49)]
  - KISA와 KISIA는 즉시 현장에 투입할 수 있는 전문가를 양성하기 위한 교육을 제공하고 비용 및 실습 환경 등 다양한 지원

- **한국정보보호산업협회(KISIA, Korea Information Security Industry Association)는 고용노동부의 지원을 받아 정보보호 인적자원개발위원회(ISC, Industrial Skills Council)를 설립하고 인적자원개발, 관리, 활용 등 기준을 마련하여 인력수급불균형의 완화를 추진(2024년)**

49) 아주경제, '디지털 전환으로 정보보호 인력 수요 증가, KISA 전문인력 3만명 양성한다', 2022.02.28.

- 정보보호 및 유관기관, 단체(7개)와 산업계 기업(21개)의 참여로 발족되었으며, 운영위원회 및 실무위원회 외 제도개선 분과, NCS자격 분과, 직무연구 분과로 구성
- 국내 정보보호 산업인력 현황 분석, 전문 인력의 필요 수준 및 규모 등을 조사·분석하여, 사이버 보안 인재양성 교육을 지원

2. 정보보호 교육 프로그램 비교분석

□ **실습 중심**의 커리큘럼

- 사이버 보안은 **위협에 대응하는 방법을 연습하는 과정이 중요**한 특성이 있어, 대부분의 교육과정이 실습과 실전연습을 중심으로 구성
  - 이스라엘의 사이버캠퍼스 교육은 AI 시뮬레이터를 이용하여 실제 사이버 공격을 시뮬레이션하고 학생 수준에 따라 시나리오를 업그레이드
  - 싱가포르의 SG 사이버 청소년 오디세이 교육의 마지막 단계인 Excel과정은 수업이 아닌 SG Cyber Olympians 대회에 참여하여 실전연습을 시행하는 방식

- 실습 중심의 교육과정은 교육을 마친 후 **실무에 즉시 투입할 수 있는 인력이 필요**한 시장의 수요[50]가 있기 때문이며, 각 국은 자국의 사이버 보안을 위해 실무에 바로 투입될 수 있는 인력양성이 필요
  - 이스라엘 사이버캠퍼스는 과정 전체에 보안기업 실무자가 관여하며, 추천이 있을 경우 채용까지 연결
  - 싱가포르의 IoT 보안교육은 IoT 산업 내 보안이 필요한 실무자를 위한 타깃교육
  - KISIA의 시큐리티 아카데미는 교육생의 선발부터 채용까지 보안기업이 참여하는 기업연계형 교육과정

□ **직무를 세분화**하여 교육과 실무를 연계

- 미국과 영국은 사이버보안 관련 **지식체계와 직무를 세분화한 프레임워크를 제작하여 교육과 실무 사이의 갭을 최소화**
  - 미국의 NICE 프레임워크는 사이버보안의 업무역할을 총 52가지로 구분하여 특정 사이버보안 관련 지식과 기술이 필요한 사이버보안 인력을 매핑하고 실무에 적용

50) 지디넷코리아, '"무조건 억대 연봉"…점점 더 '귀한 몸' 될 직업은?', 2024.08.18.

- 영국의 CyBOK는 사이버보안의 기본 지식체계를 수립하여, 사이버 보안에 존재하는 기술격차를 줄이고 명확한 기초지식을 확립

- 국내의 정보보호 ISC에서도 국가직무능력표준(NCS, National Competency Standards)과 연계된 교육 제공을 준비 중

□ 유아부터 이어지는 정보보호 교육

- 영국, 이스라엘, 싱가포르는 **진로를 결정하는 청소년기부터 그에 맞는 정보보호 교육**을 시행
  - 이스라엘 사이버캠퍼스 과정은 13학년부터 시작하며, 싱가포르의 사이버 청소년 오디세이 과정도 고등교육과정부터 시작
  - 영국은 7세부터 시작하는 사이퍼퍼스트 과정이 있으며, 진로를 선택한 중등교육과정 이후(14~15세 이상)에는 사이버보안의 기초과정을 교육
  - 국내 사이버보안 과정은 고등학교 졸업 이후부터 지원 가능

- **영국**은 특히 7세부터 게임 등을 통해 정보보호에 대한 인식을 확대하고, **정보보호 교육을 일반 교육 학제와 동일하게 학년에 따라 점차 진행**하는 방향을 추구

P·A·R·T 04

정보보호인력 인력양성 방안

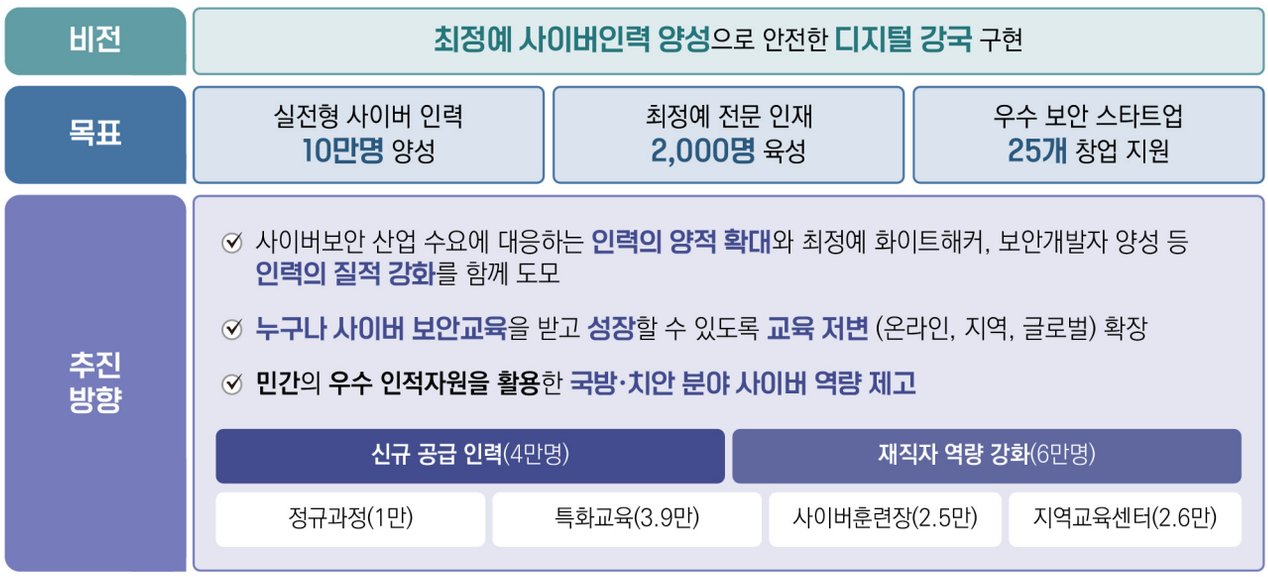
제1절. 우리나라의 정보보호인력 양성 계획

1. 10만 사이버보안 인재 양성 계획('22~'26)

□ 우리 정부는 2022년 7월 '사이버보안 10만 인재 양성 방안'을 발표하여, 2026년까지 4만 명의 신규 인력 양성과 6만 명의 재직자 역량 강화를 목표로 하고 있음

- 10만 사이버보안 인재 양성을 위한 주요 추진 방향
  - 사이버보안 산업 수요에 대응하는 인력의 양적 확대와 최정예 화이트해커, 보안개발자 양성 등 인력의 질적 강화를 함께 도모
  - 누구나 사이버 보안교육을 받고 성장할 수 있도록 교육 저변(온라인, 지역, 글로벌) 확장
  - 민간의 우수 인적자원을 활용한 국방·치안 분야 사이버 역량 제고

[그림 4-1] **10만 사이버보안 인재 양성 계획**



□ 이를 위해 정부는 첫째, 사이버보안 개발부터 대응까지 전주기 최정예 인력 양성체계를 추진하고 있음

- (미래인재 양성) 클라우드와 가상융합경제 등 변화하는 사이버 환경에 대응하기 위해 융합보안대학원과 정보보호특성화대학을 확대·개편하여, 2026년까지 각각 12개와 10개로 늘리고 있음

- 또한, 인력 양성의 질을 높이기 위해 대학원 지원 대상을 석사에서 석·박사 과정으로 확대하고, 대학 주도로 기업·연구소가 참여하는 연구개발을 추진하며, 이를 통해 연구개발 기반의 개발인력 육성을 지원하고 있음

- **(현장 연계 강화) 기업이 인재 선발, 실무 교육, 취업까지 전 과정을 주도하고 정부가 이를 지원하는 '시큐리티 아카데미'를 2023년부터 도입하여 연간 200명을 양성하고 있음**
  - 또한, 기업 내 의사결정자와 중소기업 보안 인력 대상 교육을 강화하고, 산업계 전문가를 강사로 활용하기 위해 대체 인건비 등 인센티브를 제공하여 교육과 현장 간의 연계를 촉진하고 있음

- **(최정예 육성 체계) 최고급 개발 인력을 양성하기 위해 IT 개발 인력을 선발하여 보안 교육과 창업을 지원하는 'S-개발자' 과정을 2023년부터 도입해 매년 50명을 육성하고 있음**
  - 또한, 화이트해커에 대한 진입장벽을 낮추고 잠재력 있는 보안 인재에게 기회를 제공하기 위해 '화이트햇 스쿨' 과정을 신설하여 연간 300명을 지원하고 있음

교육 대상		중급 과정		고급 과정
개발자 (제품 개발자)	:	(SW 등 IT개발 인력 선발)	⇨	'S-개발자' (신설)
화이트 해커 (사고대응)		'화이트햇 스쿨' (신설)		'차세대 보안리더(BoB)' (기존)

□ 둘째, 저변 확대를 위해 상시 육성 체계와 글로벌 연계 기반을 마련하고 있음

- **(훈련장 확대·고도화) 누구나 쉽게 보안 교육을 받을 수 있도록 실전형 '사이버훈련장(Security-Gym)'을 기존 판교에서 전국으로 확대하고 있음**
  - 또한, 실제 사고 대응 역량 강화를 위해 현장 기반 훈련 시나리오를 개발하고 팀 단위 훈련이 가능한 멀티훈련 플랫폼을 구축하고 있음

- **(지역 확산) 지역의 보안 인재 육성을 위해 지역교육센터를 중심으로 특성화대학과 융합보안 대학원 등 거점대학과 연계하여 교육을 지원하고 있음**
  - 또한, 지자체와 산·학 협력을 통해 '지역 정보보호 협의회'를 구성하고, 청소년 보안캠프와 대학 동아리를 통해 인식 제고와 기초 역량 강화를 추진하고 있음

- **(글로벌 진출) 개도국 인재 육성과 국내 기업의 해외 진출을 지원하기 위해 'K-사이버 글로벌 인력 네트워크'를 2022년부터 추진하고 있음**
  - 또한, 한·미 정상회담 후속 조치로 미국 사이버보안 관련 기관과 국내 침해 대응 기관 간 인력 교류를 2023년부터 시작하여 사이버 인력의 해외 진출을 촉진하고 있음

□ 셋째, 민·관·군 유기적 협력으로 사이버 전(戰)·범죄에 적극적으로 대응하고 있음

- **(전문 인력) 사이버 작전과 수사 분야의 전문 인력을 양성하기 위해 전문대에는 사이버부사관 전문대학을, 대학에는 사이버 전문 장교 특성화대학을 신설하며, 대학원에서는 융합보안대학원에 군·경 사이버보안 재직자를 위한 전문 과정을 도입하고 있음**
  - 또한, 군 사이버 인력의 운영을 개선하여 우수 인재의 민간 유출을 방지하기 위해 핵심기술직위 지정, 핵심인재 보직, 수당, 인사가점 등 인센티브를 제공하고, 전군 대상 사이버 전문 특기를 통합 지정·운영하는 경력 관리 방안을 검토하고 있음

- **(민·군 연계) 우수 인력을 선발해 군 사이버안보 분야에서 근무 후 취업이나 창업으로 연계하는 '사이버 탈피오트' 제도를 도입하고 있음**
  - 또한, 민간 인력을 사이버전 예비인력으로 조직화하는 '사이버 예비군'을 창설하여 유사시 군의 사이버 작전 수행 능력을 강화하고 있음

- **(공공 인력 역량 강화) 국가 공공기관 정보보안 담당자의 역량 강화를 위해 지역 대학과 연계한 지방 거점 사이버안보 교육 체계를 2023년부터 구축하고 있음**
  - 또한, 금융·국방·전력 등 유관기관 합동팀은 NATO의 '락드 쉴즈'와 미국의 '사이버 플래그' 같은 국제 훈련에 참가하며, 침해대응기관 재직자 대상의 나노 디그리 과정을 2024년부터 도입하고 있음

[그림 4-2] 10만 사이버보안 인재 양성 세부방안

정부의 "10만 사이버보안 인재 양성 방안('22년~'26년)"

분야	과정	양성 방안
신규 인력 공급 (4만명)	정규 과정 (1.0만명)	**[고급]** 대학원(0.1만명) · (확대)융합보안대학원 확대 (8개교 → 12개교, 석사 → 석·박사)
		[중급] 대학(0.4만명) · (확대)정보보호특성화대 확대(3개교 → 10개교)
		[초급] 특성화고·전문대학(0.4만명) · (신규)사이버부사관 특화 정보보호 전문대학
	특화 교육 (3.9만명)	**[고급]** 최정예 우수 인력 확보(0.1만명) · (신규)최정예 보안제품 개발과정 'S-개발자'(50명) · 정예 화이트해커(Best of Best BoB) 양성(200명)
		[중급] 실무형 인재 양성(3.6만명) · (확대)구직자 대상 K-Shield Jr.(300명 → 1,000명) · (신규)중급 화이트해커(화이트햇 스쿨) 양성(300명) · (신규)시큐리티 아카데미 도입(200명)
		[초급] 보안관리 인력 공급 확대(0.2만명) · (확대)정보통신기술 융합 보안교육 확대(400명 → 600명)
재직자 역량 강화 (6만명)	사이버 훈련장 (2.5만명)	'디지털 실전형 사이버훈련장' 구축(2.5만명) · [고급] 실전형 사이버 공격·방어 훈련 실시 · [중급] 침해사고 대응 등 해킹방어 기본기술 습득 · [초급] 동영상 강의, 실습 등 기초역량 교육
	지역 교육 (2.6만명)	'지역 정보보호교육센터' 설립(2.6만명) · [중·고급] 악성코드 분석·탐지 등 실무형 교육 · [초급] 사이버보안 소양, 보안제품 실습 등 기초 직무 교육

사이버보안 산업 종사(2.5만명)	일반기업·기관 보안관리(7.5만명)
· 사이버보안 제품·서비스 개발·공급 · 보안 취약점 진단 · 보안제품 설치 및 유지보수	· 기업·기관의 보안 관리 및 운영 · 보안정책 수립 및 적용

제2절. 정보보호 전문인력 양성을 위한 정책 제언

□ 정보보호 전문인력 양성을 위해 정부가 추진하고 있는 “10만 사이버보안 인재 양성 계획”에는 신규인력 공급방안, 재직자 역량 강화 방안으로 구분되어 있고, 정규과정 교육, 특화교육 뿐만 아니라 사이버 훈련장, 지역 교육을 세부 분류하여 고급/중급/초급 인력에 대한 구체적인 과제들이 적절하게 정의되어 있다고 판단됨.

□ 다만, 글로벌 정보보호 인력양성 방안들에 대한 조사 내용을 바탕으로 “10만 사이버보안 인재 양성”에 도움이 되고, 국내 정보보호 전문인력 양성에 추가적으로 적용 가능한 정책방안을 아래와 같이 제시하고자 함

[표 4-1] 정보보호 전문인력 양성을 위한 정책제언

추진전략	세부 정책제언	추진시기
정책연구	**[1] 초급, 중급, 고급, 특급 등 수준별 인력 수급차 분석 실시 및 맞춤형 수급차 해소 전략 추진**	매년
	[2] K-Security Education Framework 개발 및 확산	중기
인력양성 프로그램	**[3] 아동 및 청소년부터 정보보호 교육 프로그램 강화**	중기
	[4] 비전공자 대상 정보보호 교육로드맵 수립 및 재교육 프로그램 체계화	단기
	[5] 정보보호인력에 대한 AI 교육 및 보안윤리 교육강화	단기
	[6] 시니어 전문가를 위한 정보보호 감리사 제도 마련	중기

[제언 1] 초급, 중급, 고급, 특급 등 수준별 인력 수급차 분석 실시 및 맞춤형 수급차 해소 전략 추진

1) 추진배경 및 목적

- **산업 수요와 공급 간 불균형 해소**
  - 급변하는 디지털 환경에서 정보보호 인력에 대한 수요는 지속적으로 증가하고 있으나 적절한 공급이 이루어지지 않으면 보안 사고에 대응할 전문 인력이 부족해질 수 있음. 수급 차 분석은 현재와 미래의 수요를 정확히 파악하여 인력 양성 정책을 설계하는 데 도움을 줌

- **사이버 위협 대응력 강화**
  - 사이버 위협이 고도화됨에 따라, 특정 기술 분야(예: AI 보안, IoT 보안 등)에 대한 전문 인력이 중요해지고 있음. 기술 분야별 수준별 수급 분석은 이러한 특정 분야에서의 인력 부족 문제를 조기에 식별하고 대비할 수 있게 함

- **효율적인 정책 및 자원 배분**
  - 정보보호 인력 양성을 위한 자원(예: 교육, 연구개발 지원 등)은 제한적임. 수준별 수급차 분석을 통해 가장 필요한 분야에 집중 투자할 수 있어 자원의 효율적 활용이 가능함

2) 추진내용

- **매년 정보보호 인력에 대한 수준별 인력 수급차 분석 실시**
  - 현재는 3~4년 마다 필요시 KISA 등에서 수행하고 있어 시계열 분석에 활용이 어렵고 정책성과 평가에 활용하거나 중장기적인 인력양성 정책 과제 도출에 활용이 어려움

- **정보보호 직무별/수준별 인력 수급차 분석을 통한 맞춤형 수급차 해소전략 마련**
  - **수급 현황 분석**
    . 직무별 분석: 정보보호 분야의 직무를 세분화하여(예: 침해사고 대응, 보안 설계, 암호 기술, 클라우드 보안 등) 각 직무에서 요구되는 인력의 수요와 공급을 조사

    . 수준별 분석: 초급, 중급, 고급, 특급 전문가 등의 수준별로 인력 현황을 파악하여, 특정 수준에서 발생하는 부족 현상을 분석

    . 산업별 분석: 금융, 공공, 국방, 제조 등 각 산업에서 요구되는 정보보호 인력의 특성과 수요를 분석

- 문제 원인 파악

. 수요 요인 분석: 사이버 위협 증가, 법규 변화, 기술 발전 등으로 인해 특정 직무나 수준에서의 인력 수요가 증가하는 이유 분석

. 공급 요인 분석: 교육기관의 한계, 전문 교육 부족, 경력 개발 기회 부족 등으로 인해 인력 공급이 미흡한 원인 조사

- 맞춤형 전략 설계

. 직무별 맞춤형 전략: 직무별로 필요한 기술과 역량을 고려하여 맞춤형 인력 양성 프로그램을 설계 예) 클라우드 보안 전문가 양성을 위한 전문 과정 개설

. 수준별 전략: 신입 인력 부족 문제를 해결하기 위해 대학 교육과정을 개선하고, 고급 인력 부족에 대응하여 재직자를 대상으로 한 고급 교육 및 인증 프로그램을 개발

. 산업 특화 전략: 특정 산업의 보안 요구를 충족하기 위해 산업 맞춤형 훈련 프로그램을 운영 예) 금융 산업을 위한 데이터 보안 전문가 양성.

- 실행 계획 및 지원

. 교육 및 훈련 프로그램 개발: 실습 기반 사이버 보안 훈련장 구축, 지역별 보안 교육센터 운영 등 실질적인 교육 기회를 제공

. 정책적 지원: 정부/산/학/연 협력으로 인센티브 제공, 관련 인증 제도 개선, 연구개발 지원 등 정책을 통해 수급 차 해소를 촉진

. 산업 연계 강화: 기업과 협력하여 현장 실습 및 취업 연계를 강화하고, 재직자 대상 역량 강화 프로그램을 제공

- 지속적 모니터링 및 피드백

. 수급 현황 변화를 주기적으로 모니터링하여 전략의 효과를 평가하고, 변화하는 수요에 맞춰 정책을 지속적으로 조정

3) 기대효과

- 정보보호 인력 수급 차 분석은 산업과 국가의 보안 역량을 강화하고 미래에 대비한 전략적 인재 양성을 위해 필수적임
- 정보보호 인력의 양성과 활용을 체계적으로 개선함으로써 국제적으로 경쟁력 있는 사이버 보안 역량 확보 가능

[제언 2] K-Security Education Framework 개발 및 확산

1) 추진배경 및 목적

- 미국에서는 사이버 보안을 위한 NICE 인력 프레임워크(**NICE Framework**)를 개발하여 개인이나 조직이 사이버 보안 작업을 수행하는 데 필요한 업무, 지식 및 기술을 설명

- 미국의 NICE 프레임워크는 조직 내 사이버보안 위험을 효과적으로 관리하기 위해 특정 사이버 보안 관련 지식과 기술이 필요한 개인이나 조직이 목적에 맞게 사용
  - (고용주) 인력평가를 실시하고 인력격차를 파악하여 직원 교육 및 경력 개발 경로를 제공
  - (대학 및 단과대학) 고용주의 요구를 반영하는 과정 내용을 개발하고 조정
  - (교육자) 학생들이 사이버보안 관련 업무를 탐구하고 미래 학습 방향을 계획하도록 지원
  - (교육 및 인증 제공자) 현재 시장 수요를 반영하는 국가 표준에 맞춰 교육 및 인증 프로그램과 매핑
  - (학생, 구직자, 직장인) 직무 역할과 관련 지식과 기술을 알아보고, 미래 학습과 경력 발전을 위한 경로를 계획
  - (사이버보안 인력 서비스 제공업체) 개발 및 공급되는 제품과 서비스에 NICE 프레임워크를 통합

- 영국에서는 **사이버보안지식체계(CyBOK, Cyber Security Body of Knowledge)**를 통해 사이버 보안의 기본 지식 체계를 수립하여 학습 및 경력 경로, 커리큘럼 및 전문교육 개발을 지원

- 우리나라도 사이버 보안 인력 양성을 위한 표준모델(가칭, K-Security Education Framework)을 개발하여 산업체/대학/교육자/구직자 등이 보안직무별로 공통으로 활용할 수 있는 체계 마련

2) 추진내용

- 사이버보안 업무 역할 및 범주 정의
  - 사이버보안 직무 세분화: 사이버보안 직무를 주요 역할별로 나눔. 예를 들어,
    . 전략 및 관리: 보안 정책, 거버넌스, 리스크 관리
    . 운영 및 대응: 침해사고 대응, 보안 모니터링, 취약점 관리
    . 엔지니어링 및 아키텍처: 네트워크 보안 설계, 시스템 보안 구축

. 평가 및 감사: 보안 감사, 컴플라이언스 확인

. 연구 및 개발: 보안 솔루션 연구, 암호학 개발

- 범주별 직무 정의: 각 역할에 대해 필요한 구체적인 직무를 정의하고, 이를 실행하기 위한 기술 및 역량을 기술

- **직무와 책임 도출**
  - 직무별 책임 정의: 각 업무 범주에 대해 주요 작업내용, 주요 성과 지표(KPI), 협업 필요성(다른 직무와의 상호작용) 등
  - 역할 책임 문서화: 직무 설명서를 작성하여 각 역할의 책임과 기대치를 문서화
- **사이버보안 경력 경로 설계**
  - 초급-중급-고급 경로 정의: 직무별로 경력 발전 경로를 설계. 예를 들어,

    . 초급: SOC 분석가 → 중급: 사고 대응 전문가 → 고급: 보안 운영 관리자

    . 초급: 네트워크 보안 엔지니어 → 중급: 보안 아키텍트 → 고급: CISO
  - 필수 기술과 인증 파악: 각 경로 단계별로 요구되는 기술, 경험, 자격 등을 명시
- **사이버보안 운영 체계 수립**
  - 업무 프로세스 정의: 사이버보안 업무의 표준 운영 절차(SOP)를 설계하여 업무 수행 방식을 체계화
- **역량 평가 및 교육**
  - 역량 평가 체계 도입: 현재 인력의 기술 수준과 역량을 평가하기 위한 도구와 기준을 설정
  - 각 직무와 경력 단계별로 필요한 기술과 지식을 개발하기 위해 맞춤형 교육 프로그램을 운영
- **멘토링 및 코칭 시스템:**
  - 경력 경로를 지원하기 위해 멘토링이나 코칭 시스템을 도입하여 인재 성장지원

3) 기대효과

- **초급에서 고급까지의 경력 경로가 명확히 제시되어, 개인이 자신의 성장 방향을 계획할 수 있음**
- **특정 직무(예: 보안 엔지니어, 사고 대응 전문가 등)에서 요구되는 역량과 인증을 사전에 준비할 수 있음**
- **산업체에서는 직무별 요구 사항에 맞춘 교육 프로그램을 설계할 수 있어, 실무에 바로 투입 가능한 인력을 양성할 수 있음**

[제언 3] 아동 및 청소년부터 정보보호 교육 프로그램 강화

1) 추진배경 및 목적

- **이스라엘에서는 사이버보안 인력을 양성하기 위해 중학생과 고등학생(13학년~17학년)을 대상으로 사이버보안 교육 강화**
  - 청소년에게 기술기반을 제공하고 문제해결 능력과 업계 표준 도구에 대한 이해 능력을 교육
  - 코딩, 프로그래밍 및 기타 기술에 대한 실무 경험을 제공
  - 창의적 사고와 모든 분야에 적용할 수 있는 문제해결 기술을 개발
  - 산업에서 사용되는 최신 도구와 기술을 접하여 경력을 쌓기 위한 좋은 출발점을 제공
  - 이스라엘 정보군에서 중요한 직책을 맡기를 원하는 청소년은 사이버보안에 관한 기본사항을 학습
  - 비슷한 관심사를 가진 또래를 만나고 연결될 수 있는 기회 제공

- **영국에서는 7세~17세의 아동 및 청소년을 위한 프로그램(CyberFirst) 제공**
  - 사이버 보안을 소개하고 장학금, 경쟁대회, 게임 등으로 일찍부터 사이버보안 기술과 경험에 노출
  - **(교육대상)** 7세부터 대학입학을 준비하는 상급학년까지 연령에 따른 사이버 보안 교육을 제공
  - **(교육의 특징)** 저학년을 위한 게임형 교육과 사이버보안을 소개하는 짧은 무료캠프로 구성되어 있으며, 진로를 선택한 중등교육과정 이후(14~15세 이상)에는 사이버보안의 기초과정을 교육
  - **(커리큘럼)** 연령과 학년에 맞춘 다양한 교육내용으로 구성

- **싱가포르에서는 재능 있는 사이버 보안 애호가를 어린 나이부터 육성**
  - **(운영형태)** SG Cyber Talent 이니셔티브는 재능 있는 사이버 보안 애호가를 어린 나이부터 육성하고, 사이버 보안 전문가가 기술을 심화하도록 돕고 있음. SG Cyber Talent는 기존 인재 유치 및 전문 개발 이니셔티브를 기반으로 구축
  - **(과정)** SG 사이버 청소년 오디세이는 SG Cyber Youth를 포함해 다양한 프로그램을 제공, 청소년 사이버 탐험 프로그램(YCEP, Youth Cyber Exploration Programme) 부트 캠프와 학생 자원봉사 및 인정 프로그램, 사이버 보안 경력 멘토링 프로그램 등 제공

- 우리나라도 미래 정보보호 인재 육성 및 보안 분야 진로 탐색 기회를 제공하기 위해서 아동 및 청소년을 대상으로 정보보호 교육 프로그램을 강화하여 학생들에게 사이버보안 분야의 중요성과 흥미를 알릴 필요가 있음

2) 추진내용

- **교육 목표 설정**
  - 기초 디지털 리터러시 향상: 인터넷과 디지털 기기의 올바른 사용 방법, 정보보호, 온라인 안전 습관 형성을 목표로 설정
  - 사이버보안 기본 개념 학습: 해킹, 피싱, 악성코드 등 사이버 위협에 대한 기본 이해와 대응 방법을 지도
  - 진로 탐색 지원: 정보보호 분야의 매력을 보여주고, 관련 진로를 탐색할 기회를 제공
- **맞춤형 교육 콘텐츠 개발**
  - 연령별 맞춤형 콘텐츠 제공: 초등학생은 놀이와 체험 중심의 콘텐츠(예: 보안 퀴즈, 애니메이션, 게임), 중·고등학생은 실습 중심의 콘텐츠(예: 모의 해킹 실습, 가상 사이버훈련장 경험) 제공
  - 실생활 사례 중심 교육: 비밀번호 관리의 중요성, 소셜미디어 사용 시 주의점, 피싱 이메일 구별 방법 등 일상생활과 연결된 내용을 소개
  - 보안 직업 소개: 정보보호 전문가, 화이트 해커 등 보안 분야 직업군과 활동 사례를 소개하여 흥미를 유발
- **교육 방법 다양화**
  - 체험형 학습 도입: 실습과 체험을 통해 직접 문제를 해결하는 방식으로 교육. 예) 가상 훈련장이나 시뮬레이션을 활용
  - 게임화(Gameification): 퀘스트나 포인트 시스템을 활용한 게임 방식으로 학습 동기를 부여
  - 온·오프라인 혼합 학습: 학교나 커뮤니티 센터에서 오프라인 수업을 진행하고, 온라인 플랫폼을 통해 추가 학습과 복습을 지원

3) 기대효과

- 아동과 청소년의 디지털 안전의식 및 보안 기술 이해력 향상
- 정보보호 인재 육성을 위한 기반 확대
- 정보보호 분야에 대한 사회적 관심 및 인식 제고

[제언 4] 비전공자 대상 정보보호 교육로드맵 및 재교육 프로그램 체계화

1) 추진배경

- **정보보호 인력에 대한 수요가 증가하면서 IT전공자·보안 전공자가 아닌 비전공자·일반 구직자들도 정보보호 직무에 대한 관심이 증가함**
  - 그럼에도 불구하고 이들에 대한 체계적인 유입방안이나 교육과정 등은 부족하여 진입장벽이 다소 높은 실정임
  - 정보보호 초·중급 인력수급 해결방안 중 하나로, 비전공자·일반 구직자 중 정보보호 직무를 희망하는 인원에 대한 효과적인 양성책이 필요
- **사설 학원 등을 통한 국비지원 교육 프로그램 등이 존재하나, 체계적인 인력양성에는 다소 부족**
  - 학원 간 경쟁·과도한 교육생 유치활동 등으로 정작 교육의 질(Quality)이나 양성 인력의 경쟁력을 제고하지 못함

2) 추진내용

- **비전공자 중심으로 정보보호 교육 대상과 목표 정의**
  - 교육 대상 설정: 비전공자의 배경에 따라 세부적인 그룹으로 나누어 필요성을 분석, IT 기초 지식이 없는 일반인(취업 준비자, 직장인), IT 지식은 있으나 보안 지식이 부족한 사람(프로그래머, 네트워크 엔지니어 등) 등
  - 교육 목표 명확화: 기본 사이버 보안 이해, 기술 기반 보안 실무 역량 개발(예: 네트워크 보안, 침해 대응), 정보보호 전문 직무로의 진출(예: SOC 분석가, 보안 엔지니어 등)
- **교육 로드맵 설계**
  - 단계별 학습 구조: 초급부터 고급까지 단계별로 학습 목표와 내용을 설정
    . 입문 단계: 정보보호 개념, 사이버 위협 이해, 개인정보 보호
    . 기초 단계: 네트워크, 운영체제, 클라우드 등 IT 기본 개념 학습
    . 중급 단계: 네트워크 보안, 침해 대응, 보안 모니터링
    . 고급 단계: 모의 해킹, 취약점 분석, 클라우드/IoT 보안
  - 커리큘럼 구성: 실습과 이론을 균형 있게 배치
    . 이론 교육: 보안 개념, 법률, 윤리, 기술 개요

. 실습 교육: 가상훈련장 활용, 모의 해킹 실습, 보안 도구 사용

- **맞춤형 교육 콘텐츠 개발**
  - 비전공자 맞춤형 내용 설계: 비전공자도 이해할 수 있도록 IT 기술의 기초부터 설명하며, 전문용어를 쉽게 풀어서 지도
  - 실생활 연계 교육: 비밀번호 관리, 소셜미디어 보안 설정 등 생활 밀접한 사례를 중심으로 시작하여 점차 전문적인 내용으로 지도
- **재교육 프로그램 체계화**
  - 모듈식 학습: 필요한 주제를 선택적으로 학습할 수 있도록 모듈화된 과정 제공

    예) "기초 네트워크 보안", "침해 사고 대응", "보안 정책 관리"
  - 단기 집중 과정: 직장인 등 시간 제약이 있는 사람들을 위한 단기 과정 개설(2주~3개월).
  - 온·오프라인 병행 학습: 온라인/오프라인 워크숍을 결합하여 접근성 제고
- **실습 중심 학습 환경 구축**
  - 가상 사이버훈련장 운영: 비전공자도 쉽게 접근할 수 있도록 시뮬레이션 기반의 사이버훈련장(예: Security-Gym)을 설계
  - 오픈소스 도구 활용: Wireshark, Metasploit 등 보안 도구 사용법 교육
  - 사고 대응 실습: 실제 사례를 기반으로 한 시나리오(예: 랜섬웨어 공격 대응) 실습
- **역량 평가와 인증**
  - 평가 체계 도입: 학습 결과를 평가하기 위해 시험과 프로젝트 기반 평가를 도입
  - 인증 프로그램 운영: 수료 후 자격증 취득을 목표로 한 교육 제공
- **진로 지원 및 커리어 연계**
  - 멘토링 프로그램: 정보보호 전문가와의 멘토링을 통해 직무에 대한 이해와 진로 상담 지원
  - 채용 연계 지원: 산업체 협력하여 교육 이수자를 보안 직무로 연결하는 프로그램 운영
- **교육 프로그램 홍보 및 지속 가능성 확보**
  - 공공 및 민간 협력: 정부와 기업의 지원을 받아 교육 비용을 낮추고 접근성을 확대
  - 커뮤니티 구축: 비전공자들이 학습 경험을 공유하고 네트워크를 형성할 수 있는 커뮤니티 제공

3) 기대효과

- 비전공자도 정보보호 분야로 진출할 수 있는 명확한 경로 제공
- 정보보호 분야 인력 부족 문제 해결, 정보보호 초급수준 인력 수급 개선
- 개인의 사이버 보안 역량 강화로 전반적인 사이버 안전 수준 향상

[제언 5] 정보보호인력에 대한 AI교육 및 보안윤리교육 강화

1) 추진배경

- **AI 기술의 급속한 발전과 사이버보안 연계성**
  - AI 활용 보안 강화 필요성: AI는 침해 사고 탐지, 위협 분석, 이상 징후 감지 등 사이버보안의 핵심 기술로 자리 잡고 있음. 신규 인력이 AI 기술을 이해하고 활용할 수 있어야 최신 보안 위협에 효과적으로 대응할 수 있음
  - AI 기반 공격 증가: 해커들은 AI를 활용한 지능적인 공격(예: AI 생성 피싱 이메일, 악성코드) 기법을 점점 더 사용하고 있음. 이러한 위협에 대비하기 위해 AI 관련 기술 지식이 필수적임
  - 보안 자동화 기술의 필요성: AI 기반 자동화 도구를 활용하면 반복적인 작업을 줄이고 보안 효율성을 높일 수 있음. 신규 인력은 이를 활용할 역량을 갖추어야 함

- **전체 보안사고 가운데 내부자가 원인이 된 경우가 많은 부분을 차지하여 보안윤리 부재의 심각성 부각**
  - 기술이 뛰어난 보안시스템을 갖췄더라도 시스템을 다루는 인력의 도덕적, 윤리적인 문제가 해결되지 않으면 사고는 끊임없이 발생
  - 내부자에 의한 보안사고를 막기 위해 내부자를 대상으로 한 윤리교육의 필요성 제기
  - 보안윤리가 없이 능력만을 강조한 사회적 풍토가 조성돼 보안인력 양성이 악성해커 양성으로 변질될 우려가 높음
  - 정보보호 전문가의 윤리적 책임: 정보보호 인력은 데이터 보호, 프라이버시 유지, 시스템 안정성 등을 보장하는 데 중요한 역할을 함. 윤리적 기준 없이 보안 기술을 사용할 경우 부적절한 행위(예: 개인정보 남용, 불법 감시)가 발생할 수 있음

- **AI와 윤리의 상호 연관성**
  - AI 윤리 문제 해결 필요성: AI가 보안 작업에 도입되면서, AI 시스템의 공정성, 투명성, 책임성이 중요한 문제로 떠오르고 있음. 신규 인력이 이러한 윤리적 문제를 이해하고, AI 시스템이 윤리적으로 설계되고 운영되도록 할 수 있어야 함

2) 추진내용

- **교육 목표 및 대상 정의**
  - 목표 설정:
    . AI 교육: AI 기술 이해 및 보안 활용 능력 향상
    . 윤리 교육: 윤리적 의사결정 능력 강화 및 법적·사회적 책임 의식 고취
  - 대상 설정:
    . 정보보호 분야에 새로 진입한 초급 및 중급 인력
    . 보안 전공자뿐만 아니라 비전공자, 전환 직업자까지 포함.
- **AI 교육 콘텐츠 개발**
  - AI 기초 및 응용 교육:
    . 기초: AI/ML의 기본 개념, 데이터 처리 기초, 알고리즘 이해.
    . 응용: AI 기반 위협 탐지(예: 이상 탐지, 악성코드 분석), 보안 자동화 활용.
  - 실습 중심 학습:
    . 오픈소스 AI 도구 사용법(예: TensorFlow, PyTorch 등).
    . 사이버보안 데이터셋을 활용한 AI 모델 개발 실습.
  - 최신 기술 트렌드 반영:
    . 딥러닝 기반 공격과 방어 기술(예: GAN을 활용한 공격 및 방어).
    . AI가 활용되는 클라우드 보안, IoT 보안, 침해사고 대응 사례.
- **보안 윤리 교육 콘텐츠 개발**
  - 윤리 개념 및 법적 책임: 정보보호 관련 법규 및 규제, 그리고 개인정보 보호, 공정성, 투명성, 책임성 등 핵심 윤리 개념
  - 윤리적 설계 및 프로세스: AI와 보안 기술의 윤리적 설계 원칙과 프로세스 도입(예: 데이터 편향 제거, 결과 검증).

3) 기대효과

- 정보보호 인력이 AI 기술과 보안 윤리에 대한 이해를 통해 최신 위협에 효과적으로 대응
- 조직과 사회의 신뢰를 높이고, 윤리적이고 전문적인 정보보호 생태계 구축
- 신규 인력이 더 나은 보안 환경을 조성하는 데 기여할 수 있는 지속 가능한 교육 체계 마련
- AI와 윤리적 사고가 융합된 정보보호 전문 인력을 양성하는데 기여

[제언 6] 시니어 전문가를 위한 정보보호 감리사 제도 도입

1) 추진배경

- **일본에서는 2003년 4월부터 '정보보안 감사제도'를 도입 운영 중**
  - 정보시스템의 보안뿐만 아니라 감사 대상에서 정보자산에 대한 보안 관리체계 및 관리주기가 구축되어 적절한 조치가 이루어지고 있는지의 관점에서 감사 수행
  - 일본 정보보호감사협회(JASA)에서 감사 자격제도를 운영하여 단계별 인력 양성
    - 정보보안 감사보(CAIS-Assistant), 공인 정보보안 감사사(CAIS-Auditor), 공인 정보보안 주임 감사사(CAIS-Lead Auditor) 등 경력에 따른 자격 부여

- **우리나라에서 정보시스템감리사 등 IT 관련 감리사는 활성화되어 있으나 정보보호 감리 관련 제도는 부재**
  - 잇따른 정보유출 사고 및 사이버테러 위협 증가로 인해 정보시스템의 안전성 확보가 중요한 요소로 부상
  - 정보시스템 감리분야에 포함된 정보보호 감리가 아닌 독자적 전문 분야로서 정보보호감리에 대한 수요 증가

- **정보보호 거버넌스 강화**
  - 보안 수준 검증 및 관리 필요성: 정보보호의 중요성이 증대되면서 보안 체계를 점검하고 운영의 적정성을 검증할 전문가가 필요. 감리사는 조직의 보안 정책, 절차, 기술적 대책이 적절히 구현되고 유지되는지 확인하는 핵심 역할을 수행
  - 위험 관리와 규제 준수: 시니어 전문가가 정보보호 감리사로 활동하면 보안 거버넌스가 강화되고, 규제 준수(GDPR, ISMS 등)에 대한 신뢰도를 높일 수 있음

- **시니어 전문가의 경험 활용**
  - 풍부한 경험과 전문성 적용: 정보보호 감리는 기술적 지식뿐만 아니라 보안 정책, 컴플라이언스, 사고 대응 경험이 필요. 시니어 전문가의 풍부한 경험은 이러한 분야에서 큰 가치를 발휘할 수 있음

2) 추진내용

제도의 목적과 필요성 명확화

- 목적 정의: 정보보호 감리사 제도를 통해 조직의 보안 수준을 체계적으로 검증하고, 시니어 전문가의 경험을 활용하여 보안 사고를 예방하며, 보안 역량을 강화하는 데 목적을 둠
- 필요성 명문화: 제도의 필요성과 기대 효과(예: 보안 사고 감소, 규제 준수 강화, 기업 신뢰도 향상)를 정부, 기업, 공공기관 등 이해관계자들에게 설득력 있게 제시

자격 요건 및 인증 체계 설계

- 감리사 자격 요건 설정:
  . 경력 요건: 정보보호, IT 관리, 감사 분야에서 일정 연수 이상의 실무 경험
  . 학력 및 기술 요건: 정보보호 관련 학위나 주요 자격증 보유 여부
- 인증 체계 개발:
  . 인증 과정: 필기시험, 실무평가, 면접 등 다단계 검증
  . 인증 유지: 지속적인 교육(CPD) 이수, 주기적 재인증
- 국내외 인증(ISMS)과 연계: 글로벌 감리 자격(CISA, ISACA 등)과의 호환성을 검토하여 제도의 국제적 신뢰도 확보

교육 및 훈련 프로그램 마련

- 교육 콘텐츠 개발:
  . 기초 교육: 정보보호 법규, 컴플라이언스, 위험 관리
  . 심화 교육: 보안 감사 방법론, 최신 기술 동향, 감리 보고서 작성
- 실습 중심 훈련:
  . 실제 사례 기반의 워크숍 및 시뮬레이션 훈련 제공
  . 모의 감리 실습을 통해 실무 적응력 강화

3) 기대효과

- 정보보호 수준의 객관적 검증 및 개선
- 시니어 전문가의 경험과 역량 활용 극대화
- 보안 환경의 고도화와 규제 강화 속에서 조직이 효과적으로 대응하고, 지속 가능한 보안 생태계를 구축하는데 기여

P·A·R·T 05

결론

□ 본 연구에서는 글로벌 정보보호 전문인력 양성방안을 조사하여, 해외 우수사례를 발굴하고 국내 현황과의 비교·분석을 통해 향후 국내 정보보호 전문인력 양성 방안 개선과 고도화에 활용하고자 하였음

□ 이를 위해 국가별 정보보호 전문인력 자격제도 조사 및 국내 자격제도와의 비교, 국가별 정보보호 전문인력 양성을 위한 교육 프로그램 조사 및 국내 정보보호 전문인력 양성교육과 비교·분석을 실시하였음

- 먼저, 정보보호 전문인력 자격제도 조사를 위해 국가별로 주요 자격제도의 운영방식 및 사후 관리 관련 사항을 제시하였음. 예를 들어 자격제도 검정내용, 시험시간, 합격기준, 응시료, 시험방식, 응시언어, 자격 유효기간 등을 분석하였음
- 또한 국가별 정보보호 전문인력 자격제도와 국내 자격제도와의 비교를 위해 국내 자격제도의 주요 현황 및 특징과 조사하고, 해외 사례와의 공통점·차이점 등을 분석하였음
- 국가별 정보보호 전문인력 양성을 위한 교육 프로그램 조사를 위해서는 국가별 주요 교육기관 및 교육프로그램의 운영 현황에 대한 사항을 제시하였음. 예를 들어 교육기관 운영 형태 및 주요 설비, 교육 커리큘럼 및 특징, 교육대상 등을 조사하였음
- 또한 국가별 정보보호 전문인력 양성을 위한 교육 프로그램과 국내 정보보호 전문인력 양성 교육과의 비교를 위해서는 국내 정보보호 전문인력 양성 프로그램의 주요 현황 및 특징을 조사하고, 해외사례와의 공통점·차이점 등을 분석하였음

□ 본 연구에서는 국가별 정보보호 전문인력 양성을 위한 교육 프로그램과 국내 정보보호 전문인력 양성교육과 비교·분석을 통해, 그리고 우리 정부가 정보보호 전문인력 양성을 위해 추진하고 있는 “10만 사이버보안 인재 양성 계획”과 비교를 통해 “10만 사이버보안 인재 양성”에 도움이 되고, 국내 정보보호 전문인력 양성에 추가적으로 적용 가능한 6가지 – ▲ 초급, 중급, 고급, 특급 등 수준별 인력 수급차 분석 실시 및 맞춤형 수급차 해소 전략 추진, ▲ K-Security Education Framework 개발 및 확산, ▲ 아동 및 청소년부터 정보보호 교육 프로그램 강화, ▲ 비전공자 대상 정보보호 교육로드맵 수립 및 재교육 프로그램 체계화, ▲ 정보보호인력에 대한 AI 교육 및 보안윤리 교육강화, ▲ 시니어 전문가를 위한 정보보호 감리사 제도 마련 – 정책방안들을 추가로 제언하였음

□ 정보보호 전문인력 양성을 위한 정책이 성공적으로 수행되었을 때 기대되는 효과는 다음과 같음

- 초급부터 특급까지 수준별 수요와 공급 차이를 분석하고 맞춤형 전략을 통해 정보보호 인력 수급 불균형 문제를 해결하며, 산업별 및 직무별 정보보호 요구를 충족할 수 있을 것으로 기대됨
- K-Security Education Framework를 개발하여 국가 차원의 통일된 교육 체계를 구축함으로써 체계적인 인재 양성과 글로벌 표준 연계를 통해 국제적 경쟁력을 확보하고, 일관된 기준으로 운영되는 교육 과정을 통해 정보보호 인력의 역량 격차를 줄일 수 있을 것으로 기대됨
- 아동 및 청소년의 정보보호 교육을 강화하여 정보보호의 중요성과 기초 지식을 조기에 습득하게 함으로써 전문가로 성장할 인재 풀이 확대되고, 안전한 디지털 습관과 보안 윤리를 갖춘 미래 세대를 육성할 수 있을 것으로 기대됨
- 비전공자를 위한 로드맵과 재교육 프로그램을 체계화하여 다양한 배경의 인재가 정보보호 분야로 진출할 수 있도록 지원하고, IT 전공자뿐 아니라 다양한 분야에서 전문인력을 배출하여 인력 풀을 다각화할 수 있을 것으로 기대됨
- AI 교육을 강화하여 최신 사이버 위협에 효과적으로 대응할 인재를 양성하고, 보안 윤리 의식을 고취하여 정보보호 인력이 윤리적 의사결정과 법적 책임을 준수함으로써 최신 기술과 윤리적 기준을 반영한 인재 양성에 기여할 수 있을 것으로 기대됨
- 정보보호 감리사 제도를 마련하여 시니어 전문가의 경험과 지식을 체계적으로 활용해 조직 및 국가 차원의 보안 수준을 강화하고, 시니어 전문가들에게 새로운 경력 기회를 제공함으로써 지속 가능한 보안 생태계를 조성할 수 있을 것으로 기대됨
- 체계적인 정책으로 교육받은 인력이 조직과 산업의 정보보호 수준을 전반적으로 향상시키고, 국가 차원의 사이버보안 경쟁력을 강화할 수 있고, 국제적 표준에 부합하는 전문 인력을 양성하여, 글로벌 사이버보안 시장에서의 리더십을 확보할 수 있을 것으로 기대됨

참고문헌

IITP GT 주간브리프, ‘이스라엘의 사이버 보안 산업 및 정책 현황’, 2020.11.30.

강순희·김안국·박성재·김주섭·김승택·김덕호·정주연·박충렬‘자격제도의 비전과 발전방안’, 한국노동연구원, 2003.

과학기술정보통신부 보도자료, 사이버 10만 인재 양성 방안’발표, 2022.7.13.

아시아투데이, ‘이스라엘 사이버보안 부대, 실리콘밸리 점령’, 2024.09.01.

아주경제, ‘디지털 전환으로 정보보호 인력 수요 증가, KISA 전문인력 3만명 양성한다’, 2022.02.28.

지디넷코리아, ‘"무조건 억대 연봉"…점점 더 '귀한 몸' 될 직업은?’, 2024.08.18.

〈참고 웹사이트〉

http://www.nitic.org

https://atecentral.net/

https://explore.skillbuilder.aws/learn/course/external/view/elearning/17623/aws-cloud-quest-recertify-cloud-practitioner

https://ilabs.eccouncil.org/

https://niccs.cisa.gov/

https://stepaheadcpd.co.uk/

https://www.csa.gov.sg/

https://www.cyber.gov.au/

https://www.cyberseek.org/

https://www.cybok.org/

https://www.gov.uk/government/organisations/ofqual

https://www.gov.uk/government/publications/application-for-recognition-supporting-information/supporting-information-application-for-recognition#the-general-conditions-of-recognition

https://www.improvate.net/

https://www.isaca.org/credentialing/cisa/maintain-cisa-certification

https://www.isc2.org/members/cpe-opportunities

https://www.israelcybercampus.com/

https://www.nationalcyberwatch.org/

https://www.ncsc.gov.uk

https://www.ncsc.gov.uk/collection/cybersprinters/the-game

https://www.ncsc.gov.uk/cyberfirst/overview

https://www.ncyte.net/

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started

https://www.pearsonvue.com/us/en/about.html

https://www.tau.ac.il/

글로벌 정보보호인력양성 사례분석

발 행 일 : 2024년 12월

발 행 처 : 정보보호 인적자원개발위원회
(대표기관 : 한국정보보호산업협회)

주 소 : 서울시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회 사무국

전 화 : (02) 6748-2011

〈비매품〉

※ 본 보고서의 내용은 한국정보보호산업협회의 공식 입장과는 무관합니다.

글로벌 정보보호인력양성 사례분석 연구

Case analysis study on global information security human resources training