2024

정보보호산업 직무변화 모니터링 보고서

2024. 12.

고용노동부

HRDK 한국산업인력공단 Human Resources Development Service of Korea

ISC 정보보호 인적자원개발위원회 Information Security Industrial Skills Council

2024 정보보호산업
직무변화 모니터링 보고서

2024년 12월

연구책임자 : 정보보호ISC 조 연 호 사무총장

참여연구원 : 정보보호ISC 이 보 연 주무팀장

정보보호ISC 이 은 수 주 임

정보보호ISC 김 민 혜 주 임

이용자를 위하여

1. 「2024 정보보호산업 직무변화 모니터링 보고서」는 고용노동부와 한국산업인력공단의 지원을 받아 정보보호 인적자원개발위원회(ISC)에서 작성하였습니다.

2. 정보보호산업 및 직무 현황을 제시할 수 있는 기존 자료를 일부 활용하였으며, 국내 정보보호 직무 종사자를 대상으로 설문조사와 인터뷰를 통해 정보보호산업 내 직무 변화에 대한 모니터링을 실시하였습니다.

3. 본 보고서는 개별 사례를 확인·분석하여 계량화된 자료를 통해 파악하기 어려운 직무 현황과 변화를 전반적으로 파악하는 데에 의의가 있습니다.

4. 보고서의 내용을 대외적으로 활용, 인용할 시에는 관련 참고문헌 및 데이터 출처는 본문의 해당 자료에도 명시하였으니, 반드시 원 출처를 밝혀주시기 바랍니다.

CONTENTS

2024 정보보호산업 직무변화 모니터링 보고서

개 요

PART. 01

1 개 요

1. 사업 필요성 및 목적

사업 필요성

- 다양한 환경변화 요인으로 정보보호ISC 소관 산업의 직무 및 숙련수요가 변화함에 따라 이에 대한 능동적인 대응 필요성 확대
- 효과적이고 활용성 높은 고용·노동 관련 사업 추진을 위해 정보보호인력의 실제 직무를 파악하여 정보보호 분야 직무맵에 반영하고 산업별 역량체계(SQF) 개발 및 활용·확산 등 유관 사업과의 연계 필요

사업 목적

- 정보보호ISC 소관 산업의 유망직무, 신규직무, 소멸직무 등을 파악하여 인적자원 표준화 및 인력수급 체계 수립을 위한 기틀 마련
- 정보보호ISC 소관 산업에 영향을 미치는 주요 환경변화 요인을 살펴보고 직무변화의 선행요인을 파악하여 유효한 대응 방안 제시
- 환경변화에 따른 정보보호ISC 소관 산업 내 직무변화를 살펴보고 이를 토대로 인적자원 관련 정책 제언을 위한 기초자료 마련

2. 추진방법

2024년 정보보호산업 직무변화 모니터링은 ① 산업범위 설정 및 표준직무 도출, ② 주요 직무선정 및 조사, ③ 결과 분석 및 보고서 작성 등 3단계의 절차를 통해 모니터링을 진행하였다.

추진절차	세부내용	방 법
1단계 산업범위 설정 및 표준직무 도출	· ISC 소관 산업분야 중 모니터링 수행 산업범위 설정 · 대상산업의 구체적인 직무 정의 도출	운영위원회, 문헌조사
2단계 주요 직무선정 및 조사	· 정보보호산업 생태계 분석 · 정보보호 분야 직무맵(18개 직무)과 연계하여 직무 정립 · 직무에 대한 산업현장 의견 수렴용 설문지 제작	문헌조사, 전문가 회의
	· 정보보호 직무 종사자를 보유한 사업체(정보보호기업, 일반 기업 모두 포함)를 대상으로 산업현장 의견 수렴	설문조사
	· 설문조사 결과를 기반으로 주요 모니터링 수행 대상 직무 선정	-
	· 세부적인 직무변화 및 선행요인에 대한 전문가 심층 모니터링 (인터뷰) 진행	전문가 FGI
	· 타당성 검증 및 개선 의견 수렴 전문가 회의 개최	전문가 회의
3단계 결과 분석 및 보고서 작성	· 조사 결과에 따른 직무변화 선행요인 및 변화 양상 분석 · 정보보호직무의 생성 및 소멸 직무 전망 · 직무변화 모니터링 결과 및 시사점 도출 · 정보보호 분야 직무맵(안) 마련	보고서 발간

2024 정보보호산업 직무변화 모니터링 보고서

직무변화 모니터링 과정

PART. 02

2 직무변화 모니터링 과정

1. 문헌조사

정보보호 분야의 한국표준산업분류(KSIC), 국가직무능력표준(NCS), 한국고용직업분류, 산업계 선행연구보고서 등 통계자료와 인적자원개발 및 분석을 위해 활용되고 있는 연구자료 등을 통해 문헌조사를 실시하였으며, 이를 참고하여 2024 직무변화 모니터링 대상 산업 범위 설정, 사업 수행에 필요한 직무 분류 및 정의 도출, 정보보호산업 생태계 분석 기초자료 마련 등에 활용하였다.

직무맵

직무맵이란 해당 산업에서 통용되는 직무를 도출하여 표준화하고 수준범위를 설정한 것이다. 직무맵은 아래와 같이 소관분야, 산업분야, 직무, 수준으로 구성되어 있다.

그림 Ⅱ-1 | **직무맵 구성**

* 출처 : 산업별역량체계(SQF) 개발 매뉴얼(고용노동부, 한국산업인력공단)

- **산업분야** : 일반적으로 산업 등의 활동분야, 영역을 의미하는 표현으로 일반적인 노동자의 경력이동이 가능한 범위를 뜻한다. 노동자의 경력이동이 가능하다는 것은 동일한 교육훈련 또는 자격을 통해 습득한 직무역량(지식, 기술 등)을 바탕으로 입직 또는 이직 활동이 이루어지는 것을 의미한다.
- **소관분야** : NCS 분류표상 ISC가 지정된 담당분야 및 실제 산업현장에서 관여하고 있는 모든 NCS 분야를 제시한 것이다.
- **직무** : 업무수행에 필요한 지식, 기술이 유사해 해당 노동시장에서 노동자의 수직적인 경력이동이 일반적으로 이루어지는 업무의 집합을 의미한다.
- **수준** : 업무수행에 필요한 지식 및 기술의 난이도·복잡성에 따라 직무를 '직무수준'으로 구분하는 기준으로, KQF 수준을 기반으로 구성된다.
- **직무 수준범위** : 하나의 직무를 기준으로 입직 시 요구되는 수준부터 승진을 통해 최종으로 도달할 수 있는 수준까지의 범위를 의미한다.

정보보호ISC 소관 산업 중 하나인 정보보호산업의 직무맵은 총 18개의 직무로 구성되어 있으며, 직무별 정의는 다음과 같다.

그림 II-2 | NCS 기반 정보보호 분야 직무맵

수준	직무	정보보호 운영/관리	정보보호 컨설팅	보안사고 대응	정보보호 개발	영상정보 보안	디지털 포렌식	클라우드보안 관리운영	모빌리티 보안	OT보안
8										
7										
6										
5										
4										
3										
2										
1										
	산업분야	정보보호								
	소관분야	정보보호ISC 소관분야								

수준	직무	정보보호 기획	정보보호 엔지니어링	보안 품질관리	기술영업	마케팅/ 홍보	정보보호 교육	보안감사	보안감리	보안 인증평가
8										
7										
6										
5										
4										
3										
2										
1										
	산업분야	정보보호								
	소관분야	정보보호ISC 소관분야								

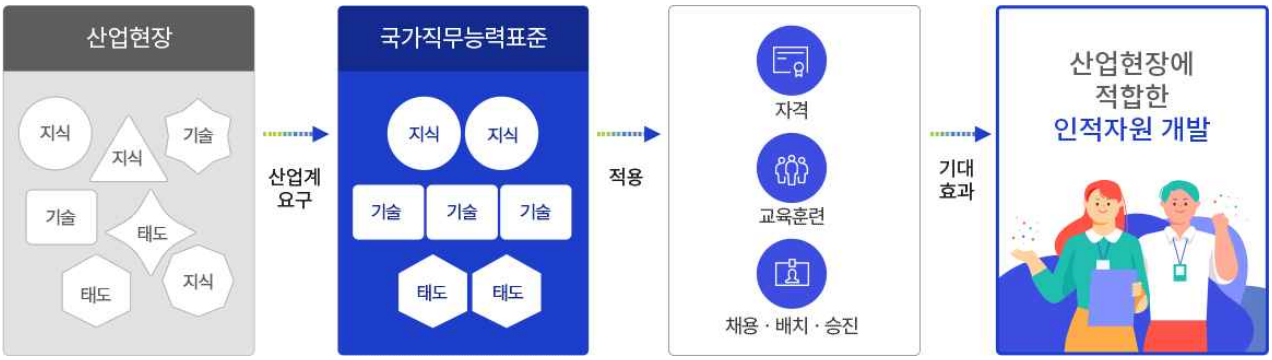
직 무	정 의
정보보호운영/관리	정보 자산을 안전하게 운영하기 위하여 정보보호 제품 및 솔루션을 운영하고, 법제도를 준수하여 보호관리 활동을 수행하며, 도출된 정보보호 대책을 기반으로 관리하는 일이다.
정보보호컨설팅	정보자산을 보호하기 위한 관리적, 물리적, 기술적 영역의 보안 요구사항 및 프로세스를 객관적으로 분석하여 개선 방안을 제안하고, 정보보호 제품의 인증 평가를 수행하는 일이다.
보안사고대응	보안사고의 피해확산 방지를 위해 위협정보를 수집, 탐지 및 분석하여 침해사고에 대응하며 정보시스템을 복구하는 일이다.
정보보호개발	정보보호제품에서 요구되는 요구사항을 분석하여 정보보호제품을 설계하고, 보안 요구사항에 대한 테스트 및 검증하는 일이다.
영상정보보안	영상정보의 수집, 저장, 반출, 파기 등 처리 과정에서 기밀성, 무결성, 가용성을 확보하고 접근통제와 오남용 방지, 영상정보관제, 보안사고 대응 등을 수행하는 일이다.
디지털포렌식	디지털기기에서 발생된 특정 행위의 사실 관계를 규명하고, 추후 법정에서 증거 자료로 인정될 수 있도록 요건을 갖추어 과학적 방법으로 증거물을 수집, 이동, 보존, 분석, 제출, 검증하는 일이다.
클라우드보안관리운영	조직이 클라우드 인프라를 안전하게 활용하기 위하여 정보보호 정책을 기획하며, 이에 따른 보안 운영 업무를 수행하고, 감사를 통해 조직의 클라우드 정보보호 거버넌스를 구현하는 일이다.
모빌리티보안	모빌리티의 안전한 활용을 위해 식별한 보안위험에 대해 조치하고 시험평가를 기반으로 보안성을 검증하여 모빌리티를 관리하고 운영하는 일이다.
OT보안	OT환경의 시스템 및 네트워크에 대한 사이버 안전성을 확보하기 위하여 OT보안 체계를 구축하기 위한 개발, 운영, 평가와 위협 및 사고대응 업무를 수행하는 일이다.
정보보호기획	조직의 목표 달성과 정보자산의 보호를 위해 정보보호 전략, 거버넌스, 운영정책, 정보보호 제품 및 솔루션을 기획하는 일이다.
정보보호엔지니어링	정보서비스의 보안 요구사항에 따라 정보보안 시스템 설치를 위한 설계, 구축, 유지보수를 수행하는 일이다.

직 무	정 의
보안품질관리	정보보호 품질관리를 위하여 전사적인 보안대책을 수립하고 제품 등의 품질보증을 위한 시험 분석, 테스트케이스 작성, 시험 수행 및 보고서를 작성하는 일이다.
기술영업	정보보호 지식을 바탕으로 고객 관리 및 영업 전략 수립과 사업기회를 창출하고 요구사항에 적합한 솔루션제안으로 협약, 계약, 판매, 사후관리를 수행하는 일이다.
마케팅/홍보	브랜드 인지도와 시장 경쟁력 강화에 기여하기 위한정보보호 솔루션 마케팅전략을 설계하고 대내외 소통을 통한고객 유지관리와 신규시장을 개척하는 일이다.
정보보호교육	정보보호 분야의 기술교육을 수행하기 위하여 교육 환경을 조성하며, 교육과정 개발 및 성과 평가를 수행하는 일이다.
보안감사	정보보호를 위한 관련 법, 제도, 정책, 역할, 가이드라인, 규범, 기술표준 등을 준수하도록 지속적으로 통제하고 관리하는 일이다.
보안감리	정보보호의 효율성과 효과성을 향상시키고 안전성을 확보하기 위하여 제3자의 관점에서 정보보호의 정책 및 기획, 정보시스템 구축 및 운영 등에 관한 사항을 종합적으로 점검하고 문제점이 개선 되도록 시정조치사항을 도출하고 확인하는 일이다.
보안인증평가	정보보호 제품에 대한 신뢰성 확보와 제품경쟁력 강화를 위하여 정보보호 제품에 대한 보안 요구사항과 보증 요구사항의 적합성 여부를 인증하거나 인증취득을 준비하는 일이다.

국가직무능력표준(NCS)

국가직무능력표준(NCS, National Competency Standards)란 산업 현장의 직무를 수행하기 위해 필요한 능력(지식, 기술, 태도)을 국가적 차원에서 표준화 한 것으로 능력단위 또는 능력단위의 집합을 의미한다.

그림 Ⅱ-3 | NCS 개념도



* 출처 : NCS 홈페이지(https://ncs.go.kr/)

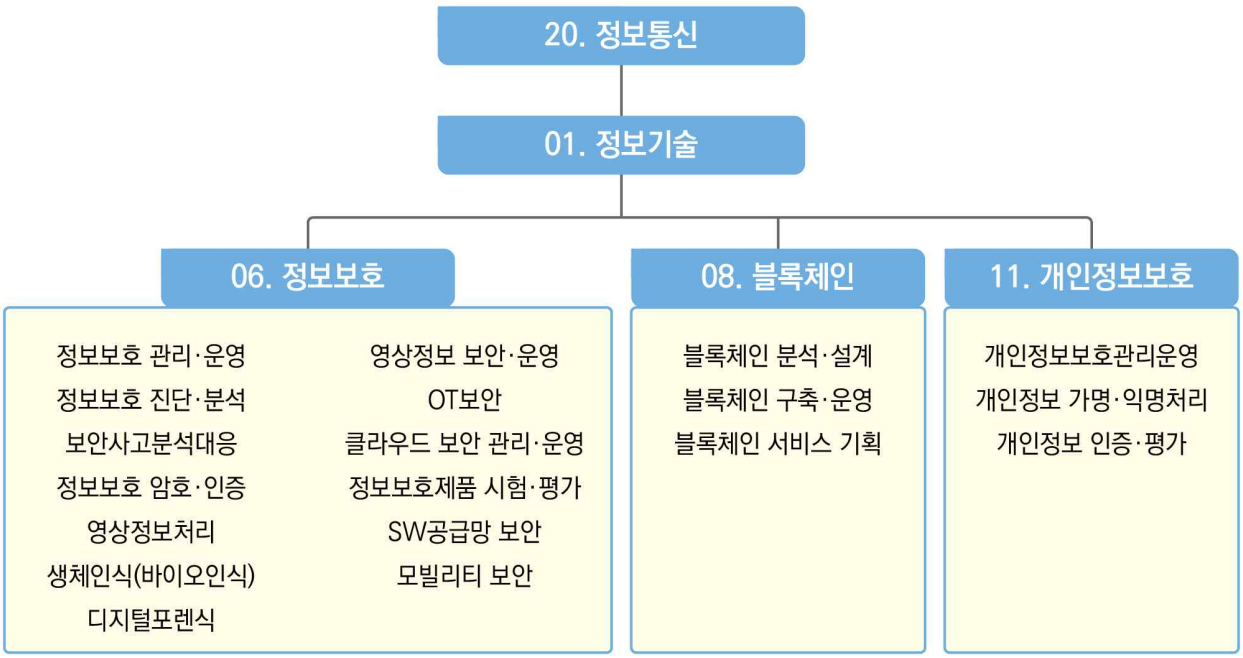
능력단위는 NCS의 기본 구성 요소로 복수의 능력단위요소, 적용 범위 및 작업 상황, 평가지침, 직업기초능력 등의 정보로 구성되며, 능력단위요소는 수행준거, 지식·기술·태도로 구성된다.

그림 Ⅱ-4 | NCS 구성

* 출처 : NCS 홈페이지(https://ncs.go.kr/)

정보보호ISC 소관 분야의 NCS는 정보통신(대분류) - 정보기술(중분류) - 정보보호, 블록체인, 개인정보보호(소분류)로 다음과 같이 구성되어 있다.

그림 II-5 | 정보보호ISC 소관 NCS



정보보호 소분류 내 13개의 세분류는 다음과 같이 정의하고 있다.

세분류	정 의
01. 정보보호관리·운영	정보보호관리·운영은 조직의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략과 정책을 수립하고, 법령 준수, 보호관리 활동을 수행하며, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 일이다.
02. 정보보호진단·분석	정보보호진단·분석은 주요 정보자산을 보호하기 위하여 보안진단과 위험평가를 수행하고 정보보호 대책, 관리체계 설계, 보안전략을 수립·자문하는 일이다.
03. 보안사고분석대응	보안사고 분석대응은 보안사고에 대한 정보의 확보·분석을 통하여 시스템 복구와 재발 방지 대책을 수립하는 일이다.
04. 정보보호암호·인증	정보보호암호·인증은 정보의 기밀성과 무결성, 신뢰성을 보장하기 위한 암호 및 인증 기술을 개발, 관리, 검증하고 해당 시스템을 운영하는 일이다.

세분류	정 의
05. 영상정보처리	영상정보처리는 영상정보처리 알고리즘을 개발하고 영상정보처리시스템 구축과 영상관제 업무관리를 수행하는 일이다.
06. 생체인식(바이오인식)	생체인식(바이오인식)은 개인의 고유한 생리학적 또는 행동학적 특징을 획득 및 추출한 정보로 신원을 식별하거나 인증하기 위하여 생체인식 시스템을 개발 및 평가를 수행하는 일이다.
08. 디지털포렌식	디지털포렌식은 디지털 기기에서 발생된 특정 행위의 사실 관계를 규명하고, 추후 법정에서 증거 자료로 인정될 수 있도록 요건을 갖추어 과학적 방법으로 증거물을 수집, 이동, 보존, 분석, 제출, 검증하는 일이다.
09. 영상정보보안·운영	영상정보보안·운영은 영상정보의 수집, 저장, 반출, 파기 등 처리 과정에서 기밀성, 무결성, 가용성을 확보하고 접근통제와 오남용 방지, 영상정보관제, 보안사고대응 등을 수행하는 일이다.
11. OT보안	OT(Operation Technology, 운영기술)보안은 OT환경의 시스템 및 네트워크에 대한 사이버 안전성을 확보하기 위하여 OT보안 체계를 구축하기 위한 개발, 운영, 평가와 위협 및 사고대응 업무를 수행하는 일이다.
12. 클라우드 보안 관리·운영	클라우드 보안 관리·운영은 조직이 클라우드 인프라를 안전하게 활용하기 위하여 정보보호 정책을 기획하며, 이에 따른 보안 운영 업무를 수행하고, 감사를 통해 조직의 클라우드 정보보호 거버넌스를 구현하는 일이다.
14. 정보보호제품시험·평가	정보보호제품 시험·평가는 사용자가 정보보호제품을 안전하게 사용할 수 있도록 정보보호제품에 구현된 보안기능의 안전성과 신뢰성을 검증받는 일이다.
15. SW공급망 보안	SW공급망 보안은 안전한 개발 환경을 구축하고 SW 구성명세서(SBOM)와 취약점을 관리하여 SW 개발, 도입, 운영까지 SW공급망을 안전하게 보호하는 일이다.
16. 모빌리티 보안	모빌리티 보안은 모빌리티의 안정성을 확보하기 위하여 보안 조직구성, 전략과 정책 수립, 법령을 준수하고, 생명주기 전 단계에 걸쳐 보안위협과 위험을 식별하고 보안성 검증 활동과 대응방안을 수립, 적용, 평가, 인증하는 일이다.

국내 정보보호산업 실태조사

매년 정기적으로 시행되는 '국내 정보보호산업 실태조사'(국가승인통계 승인번호 제127013호)에서는 정보보호산업을 다음과 같이 분류하고 있다.

구 분	대분류	중분류
정보보안	정보보안 제품(솔루션)	네트워크보안 솔루션
		엔드포인트보안 솔루션
		플랫폼보안/보안관리 솔루션
		클라우드보안 솔루션
		컨텐츠/데이터 보안 솔루션
		공통인프라보안 솔루션
	정보보안 관련 서비스	보안 컨설팅
		보안시스템 유지관리/보안성 지속 서비스
		보안관제 서비스
		보안교육 및 훈련 서비스
		보안인증 서비스
	정보보안 기타	기타
물리보안	물리보안 제품(솔루션)	보안용 카메라
		보안용 저장장치
		보안장비 부품
		물리보안 솔루션
		물리보안 주변장비
		출입통제 장비
		생체인식 보안시스템
		경보/감시 장비
		기타 제품
	물리보안 관련 서비스	출동보안 서비스
		영상보안 서비스
		클라우드 서비스
		기타 보안 서비스

* 출처 : 2024년 국내 정보보호산업 실태조사(과학기술정보통신부, 한국정보보호산업협회)

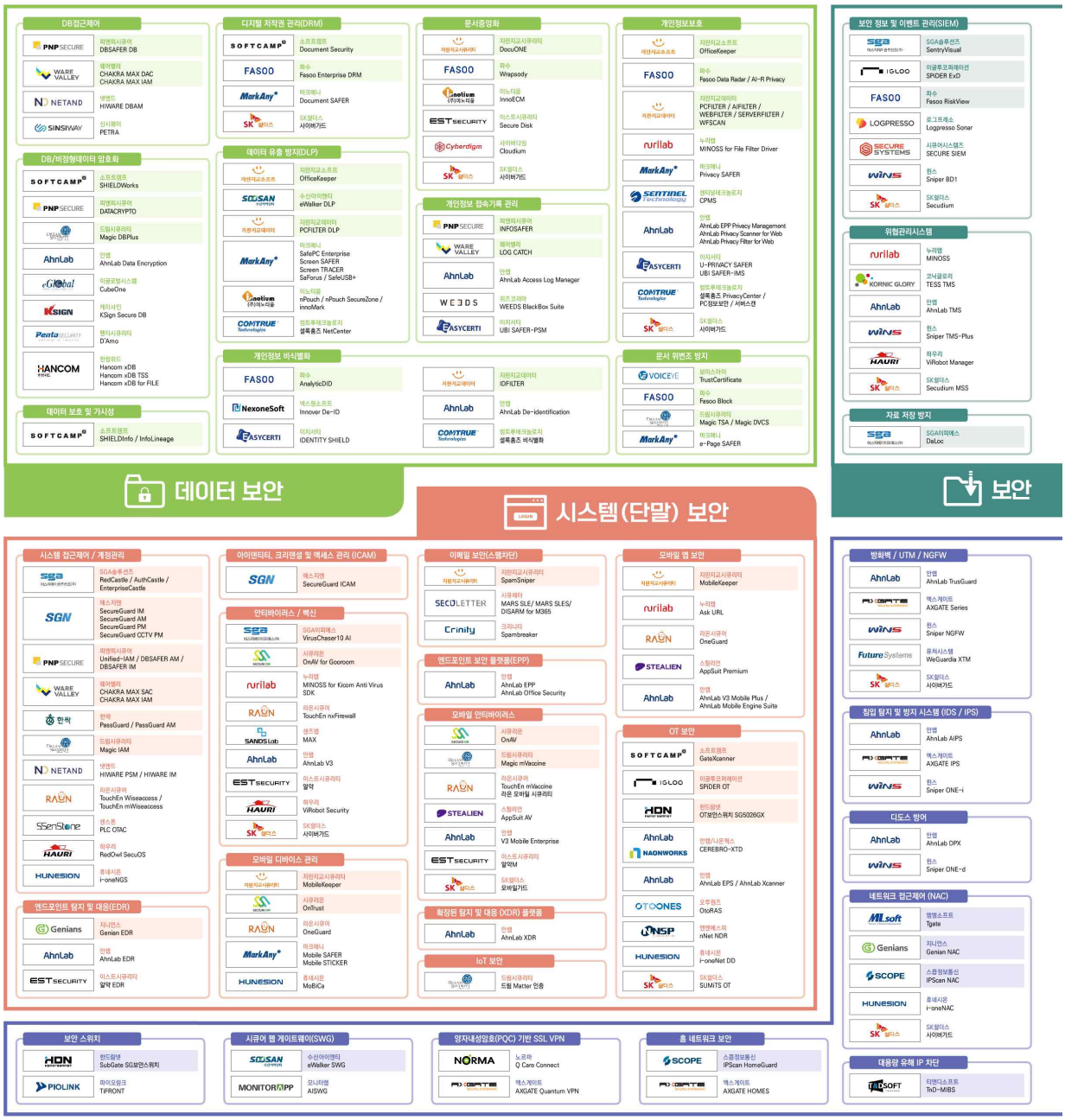
실태조사 내 인력 관련 문항에서는 정보보호산업의 인력을 다음과 같이 분류하고 있다.

구 분		세부분류	세부 직종 예시
정보보안	정보보안 연구 및 개발	시스템 및 네트워크 기술, 암호 및 인증, 기술응용기술 및 서비스	· 컴퓨터시스템 분석 및 설계 전문가 · 네트워크 분석 및 설계 전문가 · 관련 연구소 및 산업체의 연구원 · 컴퓨터 악성프로그램 분석가
	엔지니어	정보시스템 관리	· 데이터베이스 관리자(DB운영) · OS 운영자 · 리눅스 전문가 · 전산관리 전문가 · 시스템 엔지니어 · 클라우드 엔지니어 등
	정보보안 관리	정보보안 컨설팅	· 정보보안 컨설턴트 · 진단 및 모의해킹 · 정보보호평가인증(ISO, ISMS 등)
		정보보안 관제	· 정보보안 관제
		정보보안 관리자	· CIO/CSO/CISO/CPO
	정보보안 영업	정보보안 마케팅	· 정보보안제품 마케팅, 국내외 판로확보
	기타 정보보안 관련직	정보시스템 감리 및 인증, 정보보안 교육, 기타	· 정보시스템 감사사 · 관련 학과를 개설한 대학의 교수 · 관련 사설교육기관의 강사 · 기타 정보보안 업무 관련자
물리보안	제품 개발	하드웨어	· PCB 및 전자 회로 등 제품의 Hardware 관련 개발
		응용 소프트웨어	· Window, Linux, RTOS 기반의 응용 Program 개발
	기술 지원	설계/시공 및 감리	· SI 영업을 위한 설계 및 제안서 작성 관련 업무 · 현장 감리 및 시공 관련 업무
	운용	IT 운용	· OS 운용, 보안 솔루션 운용 등
	생산	생산기술/품질 관리	· 생산 시스템 운영 전반에 관련된 전문 업무 · 품질 관리 및 품질 시스템 운영에 필요한 업무
	영업	국내 외 영업	· 국내외 고객을 대상으로 한 마케팅, 영업 기술 지원 등
	관리 및 기타	시설 관리 경비	· 시설 관리 경비 · 출동 경비 요원
		관리, 기타	· 내부 관리 업무 · 기타 명시되지 않은 업무

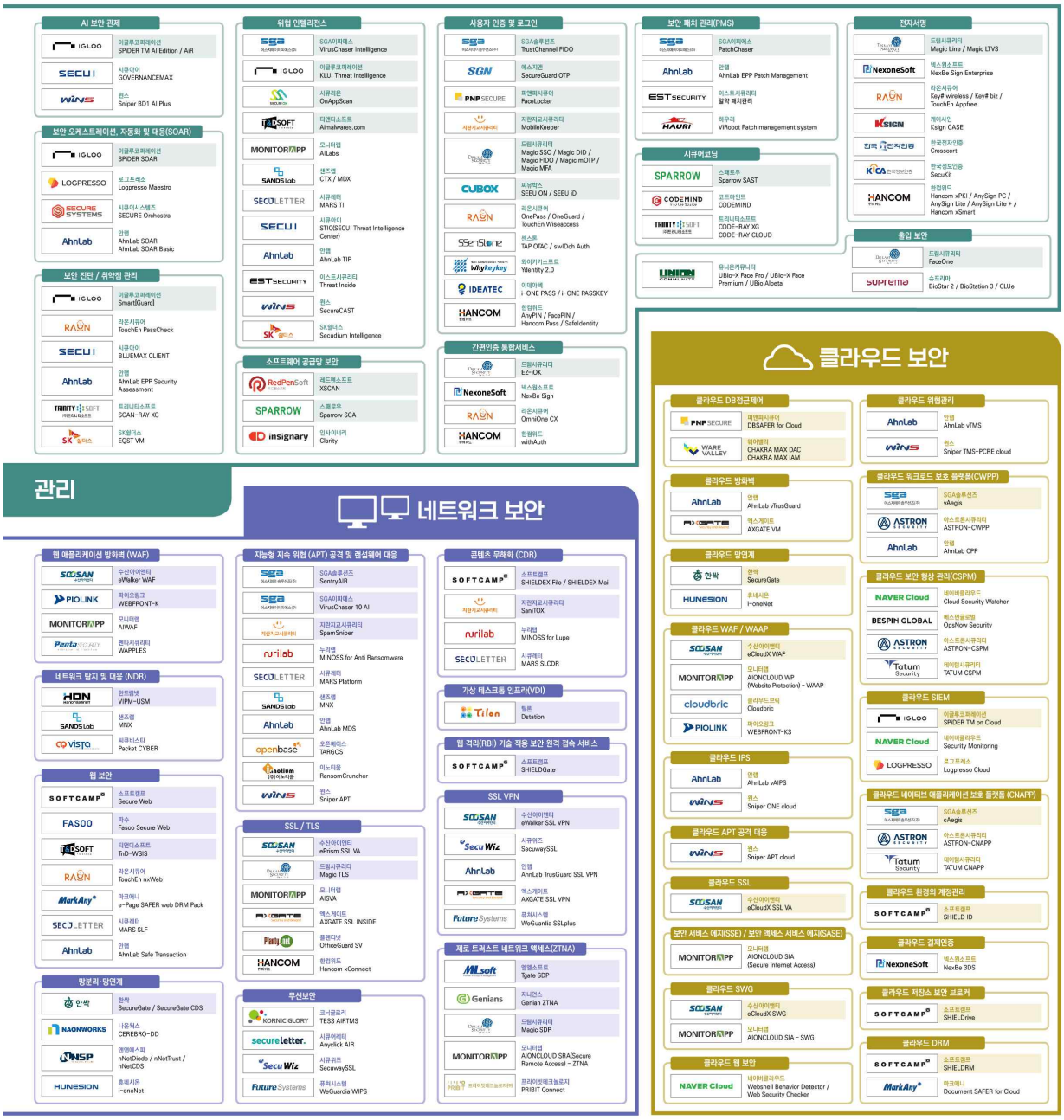
* 출처 : 2024년 국내 정보보호산업 실태조사(과학기술정보통신부, 한국정보보호산업협회)

국산 정보보호 솔루션 구성도

IT 전문 언론사에서 매년 국내 정보보호기업의 제품(솔루션)을 분류하여 배포하고 있다.



* 출처 : 아이티데일리 홈페이지(http://www.itdaily.kr/), 컴퓨터월드 홈페이지(https://www.comworld.co.kr/)


AI 보안 관제
이글루코퍼레이션 SPIDER TM AI Edition / AiR
시큐아이 GOVERNANCEMAX
윈스 Sniper BD1 AI Plus
보안 오케스트레이션, 자동화 및 대응(SOAR)
이글루코퍼레이션 SPIDER SOAR
로그프레소 Logpresso Maestro
시큐아이랩스 SECURE Orchestra
안랩 AhnLab SOAR AhnLab SOAR Basic
보안 진단 / 취약점 관리
이글루코퍼레이션 Smart[Guard]
라온시큐어 TouchEn PassCheck
시큐아이 BLUEMAX CLIENT
안랩 AhnLab EPP Security Assessment
트리니티소프트 SCAN-RAY XG
SK쉴더스 EQST VM
위협 인텔리전스
SGA이피에스 VirusChaser Intelligence
이글루코퍼레이션 KLU: Threat Intelligence
시큐레온 OnAppScan
타겐티소프트 Aimalwares.com
모니터랩 AILabs
샌즈랩 CTX / MDX
시큐레터 MARS TI
시큐아이 STIC(SECUI Threat Intelligence Center)
안랩 AhnLab TIP
이스트시큐리티 Threat Inside
윈스 SecureCAST
SK쉴더스 Secudium Intelligence
소프트웨어 공급망 보안
레드펜소프트 XSCAN
스패로우 SPARROW SCA
인사이너리 Clarity
사용자 인증 및 로그인
SGA솔루션즈 TrustChannel FIDO
엑스지엔 SecureGuard OTP
파멘피시큐어 FaceLocker
지란지교시큐리티 MobileKeeper
드림시큐리티 Magic SSO / Magic DID / Magic FIDO / Magic mOTP / Magic MFA
씨박스 SEEU ON / SEEU iD
라온시큐어 OnePass / OneGuard / TouchEn Wiseaccess
센스톤 TAP OTAC / swIDch Auth
와이키키소프트 Ydentity 2.0
이데아텍 i-ONE PASS / i-ONE PASSKEY
한컴위드 AnyPIN / FacePIN / Hancom Pass / SafeIdentity
간편인증 통합서비스
드림시큐리티 EZ-iOK
넥슨원소프트 NexBe Sign
라온시큐어 OmniOne CX
한컴위드 withAuth
보안 패치 관리(PMS)
SGA이피에스 PatchCheser
안랩 AhnLab EPP Patch Management
이스트시큐리티 알약 패치관리
하우리 ViRobot Patch management system
시큐어코딩
스패로우 Sparrow SAST
코드마인드 CODEMIND
트리니티소프트 CODE-RAY XG CODE-RAY CLOUD
유니온커뮤니티 UBio-X Face Pro / UBic-X Face Premium / UBio Alpeta
전자서명
드림시큐리티 Magic Line / Magic LTVS
넥슨원소프트 NexBe Sign Enterprise
라온시큐어 Key# wireless / Key# biz / TouchEn Appfree
케이사인 Ksign CASE
한국전자인증 Crosscert
한국정보인증 SecuKit
한컴위드 Hancom xPKI / AnySign PC / AnySign Lite / AnySign Lite + / Hancom xSmart
출입 보안
드림시큐리티 FaceOne
슈프리마 BioStar 2 / BioStation 3 / CLUe
클라우드 보안
클라우드 DB접근제어
지란지교시큐어 DBSAFER for Cloud
웨어밸리 CHAKRA MAX DAC CHAKRA MAX IAM
클라우드 방화벽
안랩 AhnLab vTrusGuard
엑스게이트 AXGATE VM
클라우드 망연계
한싹 SecureGate
휴네시온 i-oneNet
클라우드 WAF / WAAP
수산아이엔티 eCloudX WAF
모니터랩 AIONCLOUD WP (Website Protection) - WAAP
클라우드브릭 Cloudbric
파이오링크 WEBFRONT-KS
클라우드 IPS
안랩 AhnLab vAIPS
윈스 Sniper ONE cloud
클라우드 APT 공격 대응
윈스 Sniper APT cloud
클라우드 SSL
수산아이엔티 eCloudX SSL VA
보안 서비스 에지(SSE) / 보안 액세스 서비스 에지(SASE)
모니터랩 AIONCLOUD SIA (Secure Internet Access)
클라우드 SWG
수산아이엔티 eCloudX SWG
모니터랩 AIONCLOUD SIA - SWG
클라우드 웹 보안
네이버클라우드 Webshell Behavior Detector / Web Security Checker
클라우드 워크로드 보호 플랫폼(CWPP)
SGA솔루션즈 vAegis
아스트로시큐리티 ASTRON-CWPP
안랩 AhnLab CPP
클라우드 보안 형상 관리(CSPM)
네이버클라우드 Cloud Security Watcher
벤스글로벌 OpsNow Security
아스트로시큐리티 ASTRON-CSPM
테이텀시큐리티 TATUM CSPM
클라우드 SIEM
이글루코퍼레이션 SPIDER TM on Cloud
네이버클라우드 Security Monitoring
로그프레소 Logpresso Cloud
클라우드 네이티브 애플리케이션 보호 플랫폼 (CNAPP)
SGA솔루션즈 oAegis
아스트로시큐리티 ASTRON-CNAPP
테이텀시큐리티 TATUM CNAPP
클라우드 환경의 계정관리
소프트캠프 SHIELD ID
클라우드 겁제인증
넥슨원소프트 NexBe 3DS
클라우드 저장소 보안 브로커
소프트캠프 SHIELDrive
클라우드 DRM
소프트캠프 SHIELDRM
마크애니 Document SAFER for Cloud
관리
네트워크 보안
웹 애플리케이션 방화벽 (WAF)
수산아이엔티 eWalker WAF
파이오링크 WEBFRONT-K
모니터랩 AIWAF
펜타시큐리티 WAPPLES
네트워크 탐지 및 대응 (NDR)
한드림넷 VIPM-USM
샌즈랩 MNX
씨크릿 Packet CYBER
웹 보안
소프트캠프 Secure Web
파수 Fasoo Secure Web
타겐티소프트 TnD-WSiS
라온시큐어 TouchEn nxWeb
마크애니 e-Page SAFER web DRM Pack
시큐레터 MARS SLF
안랩 AhnLab Safe Transaction
망분리·망연계
한싹 SecureGate / SecureGate CDS
나온웍스 CEREBRO-DD
엔피넥스 nNetDiode / nNetTrust / nNetCDS
휴네시온 i-oneNet
지능형 지속 위협 (APT) 공격 및 랜섬웨어 대응
SGA솔루션즈 SentryAiR
SGA이피에스 VirusChaser 10 AI
지란지교시큐리티 SpamSniper
누리랩 MINOSS for Anti Ransomware
시큐레터 MARS Platform
샌즈랩 MNX
안랩 AhnLab MDS
오픈베이스 TARGOS
이노지움 RansomCruncher
윈스 Sniper APT
SSL / TLS
수산아이엔티 ePrism SSL VA
드림시큐리티 Magic TLS
모니터랩 AISWA
엑스게이트 AXGATE SSL INSIDE
플랜다운 OfficeGuard SV
한컴위드 Hancom xConnect
무선보안
코닉글로리 TESS AIRTMS
시큐어레터 Anyclick AIR
시큐위즈 SecuwaySSL
퓨처시스템 WeGuardia WIPS
콘텐츠 무해화 (CDR)
소프트캠프 SHIELDEX File / SHIELDEX Mail
지란지교시큐리티 SaniTOX
누리랩 MINOSS for Lupe
시큐레터 MARS SLCDR
가상 데스크톱 인프라(VDI)
틸론 Dstation
웹 격리(RBI) 기술 적용 보안 원격 접속 서비스
소프트캠프 SHIELDGate
SSL VPN
수산아이엔티 eWalker SSL VPN
시큐위즈 SecuwaySSL
안랩 AhnLab TrusGuard SSL VPN
엑스게이트 AXGATE SSL VPN
퓨처시스템 WeGuardia SSLplus
제로 트러스트 네트워크 액세스(ZTNA)
엠엘소프트 Tgate SDP
지니언스 Genian ZTNA
드림시큐리티 Magic SDP
모니터랩 AIONCLOUD SRA(Secure Remote Access) - ZTNA
프라이빗테크놀로지 PRIBIT Connect

2. 전문가 회의

설문조사 및 보고서의 완성도를 높이기 위한 정보보호 산업계 및 학계 전문가와의 회의를 통해 현안을 검토하고 사업 수행 관련 개선 의견을 수렴하였다.

회의내용	일 시	참석자	회의결과
모니터링 대상 산업 설정	2024년 4월	ISC 참여기관·기업 기관장 및 대표이사, 정보보호ISC 사무국	정보보호ISC 소관 산업 중 2024년도 직무변화 모니터링 대상 산업으로 '정보보호산업' 설정
직무 분석 및 설문문항 설계	2024년 5월	정보보호 산업계 및 학계 전문가, 정보보호ISC 사무국	직무정의 보완 및 설문문항 추가 등
산업 생태계 분석 자문	2024년 7월	정보보호 학계 전문가, 정보보호ISC 사무국	2024년도 산업 생태계 분석 범위 설정 및 향후 직무변화 모니터링 사업의 전반적인 운영 방향 논의
정보보호산업 생태계 분석	2024년 8월 ~ 2024년 10월 (총 3회)	정보보호 학계 전문가, 정보보호ISC 사무국	정보보호산업 생태계 구조 도출 및 분석
직무변화 모니터링 사업 및 보고서 자문	2024년 12월 (총 4회)	정보보호 산업계 및 학계 전문가, 정보보호ISC 사무국	전반적인 직무변화에 대한 추가 자문 및 최종 보고서 검토

3. 산업체 의견수렴 및 검증

정보보호 분야 직무맵을 기반으로 총 19개의 직무 및 정의를 도출하였으며, 응답률 향상 및 설문 응답자의 이해도를 제고시키기 위해 직무를 특성에 따라 총 6개의 분야로 재분류하여 설문조사와 심층 인터뷰를 진행하였다.

설문조사

정보보호 기업 및 일반기업의 정보보호 업무를 수행하고 있는 인사 또는 직무 담당자를 대상으로 설문조사를 진행하여 직무변화에 대한 의견을 수렴하였다.

- 기 간 : 2024년 7월 ~ 2024년 10월
- 대상자 : 총 30개 정보보호 유관 기업의 인사 및 직무 담당자
- 방 법 : 서면 및 대면 설문조사

심층 인터뷰

○ 전문가 FGI

설문조사에서 도출된 데이터를 기반으로, 정보보호산업에 많은 영향을 미치고 직무변화가 큰 직무를 선정하여 포커스 그룹 인터뷰(FGI)를 진행하였다.

해당 직무와 관련하여 다수 기업의 의견을 수렴하고 전반적인 변화양상을 파악하기 위해 기업의 규모와 사업영역을 고려하여 인터뷰 대상 기업 및 전문가를 선정하였다.

직 무	일 시	대상 기업 특성
정보보호개발	2024년 10월	· 총 8개 기업 - 설립 : 1997년 ~ 2018년 / 7년차 ~ 26년차 - 규모 : 30억 대 ~ 400억 대 - 사원수 : 10명 대 ~ 400명 대 - 사업영역 : 응용소프트웨어 개발 및 공급, 네트워크 보안, 클라우드 보안, 엔드포인트 보안, 취약점 분석, 블록체인 등
클라우드보안관리운영	2024년 11월	· 총 3개 기업 - 설립 : 1981년 ~ 2022년 / 3년차 ~ 44년차 - 규모 : 6,000억 대 ~ 18조 대 - 사원수 : 600명 대 ~ 18,000명 대 - 사업영역 : 클라우드 컴퓨팅 서비스, 소프트웨어 개발, 네트워크 관리, 인터넷 및 전자상거래 등

전문가 인터뷰

이후 모든 분야에 대해 전반적인 직무변화 현황을 보다 상세히 파악하기 위해 분야별 대표 직무를 선정하여 2024년 11월 관련 산업계 전문가를 대상으로 심층 인터뷰를 진행하였다.

분 야	직 무	주요 질의 내용
연구·개발	정보보호개발	1) 정보보호산업의 전반적인 변화 및 요인 ・정보보호산업 직무변화에 영향을 주는 요인 ・해당 요인으로 인해 가장 크게 변화한 요소 ・정보보호 분야 직무구분 및 수준의 적절성(직무맵) ・직무별 인력양성 및 교육훈련 수요 2) 담당 직무 관련 세부 변화 및 요인 ・직무 수행에 필요한 기술 및 역량 ・직무에서 가장 많이 변화된 요소 ・직무의 변화에 가장 큰 영향을 미치는 요인 ・직무의 인력 수준 분포 ・직무의 변화 속도 및 예상 변화 ・해당 직무가 정보보호산업에 미치는 영향 ・직무변화에 따른 사내 대응 방안
운영·관리	정보보호엔지니어링	
조사·대응	보안관제, 디지털포렌식	
진단·평가	정보보호컨설팅	
신기술보안	모빌리티 보안	
기타	기술영업	

정보보호산업 생태계 분석

PART. 03

3 정보보호산업 생태계 분석

1. 정보보호산업 개요

정보보호산업은 '정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업(정보보호산업법 제2조)'으로 진화하는 보안 위협에 대한 대응과 우수한 제품 개발을 위해 지속적인 R&D와 더불어 암호·인증·인식·감시 등의 보안 분야 학문 외 인문학, 공학 등 多학제적인 인재가 필요하다는 특성을 가지고 있다.

기술의 적용영역, 제품의 특성 등에 따라 정보보안, 물리보안, 융합보안(정보보안+물리보안, 정보보안+他산업)으로 산업의 범위를 분류하기도 한다. 이는 크게 컴퓨터 또는 네트워크상 정보 유출·훼손 등을 방지하기 위한 정보보안, 재난·재해, 범죄 등을 방지하기 위한 물리보안, 자동차나 항공·해상 보안 등의 융합보안으로 구분된다.

구분	정보보안	물리보안	융합보안
특성	컴퓨터 또는 네트워크상 정보 유출과 훼손 등을 방지	재난, 재해, 범죄 등을 방지	정보보안+물리보안 또는 정보보안+他산업과의 결합
예시	해킹 및 침입탐지 등	영상감시, 바이오인식, 무인전자경비 등	운송(자동차, 항공 등) ·의료·건설·국방보안 등

주요 산업품목은 하드웨어·소프트웨어·서비스로 구분하여 왔으나 정보보호산업의 특성상 제품과 서비스의 통합화 및 융합화가 매우 빠르게 진행되고 있어 위 세 개 분야의 구분이 점차 모호해지고 있다.

오늘날 정보보호산업은 지능화된 보안위협 및 제조업 등 타 분야에서의 신규 보안이슈 확대로 향후 시장이 더 커질 것으로 전망되는 성장 발전 가능성이 높은 신성장 산업이자 개인의 안전과 재산을 지켜주는 보안 산업인 동시에 각종 사이버 테러 등 보이지 않는 전쟁으로부터 국가의 안위를 지켜주는 방위 산업이기도 하다.

2. 정보보호산업 특성

정보보호산업은 IT 기술의 발전에 따라 중요성과 필요성이 대두되는 산업이다. 1980년대 개인용 컴퓨터의 보급이 본격화되고, 1990년대 PC 통신을 시작으로 인터넷이 대중화되면서 국내 정보보호산업 생태계가 형성되었다.

1986년 최초의 PC 바이러스인 브레인 바이러스[1]를 치료하기 위해 백신 개발이 진행되면서 1990년대에 본격적으로 백신 업체들이 등장하게 되었다. 또한, 1997년 IMF로 인해 비용 절감과 구조조정 등으로 금융 서비스가 온라인화 되면서, 온라인 거래에 대한 보안 요구 증가로 공인 인증서, 키보드 보안, PC 방화벽 등 다양한 보안 솔루션들이 등장하게 되었다.

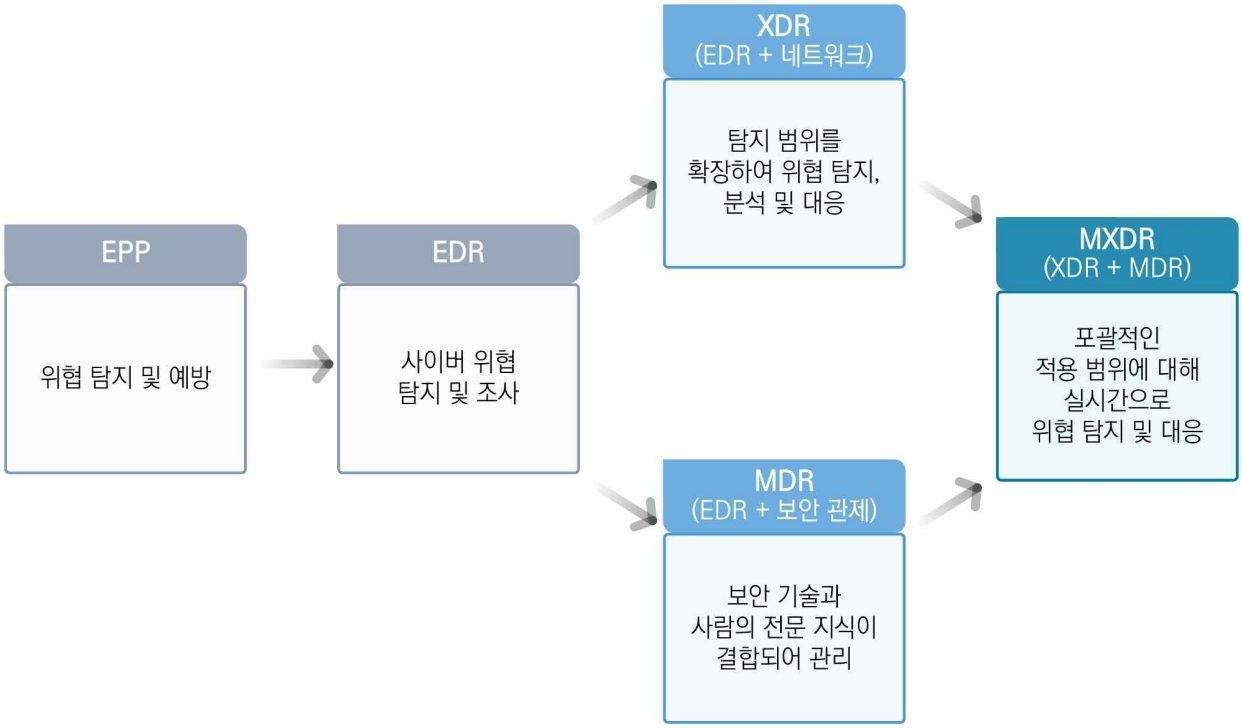
특히, 정보보호산업 생태계가 형성되는 초기에는 1999년 CIH 바이러스[2]와 2001년 슬래머 웜[3]과 관련된 백신을 중심으로 한 정보보호 기업들이 급속히 성장하는 계기가 되었다.

2000년대까지의 정보보호산업은 주로 산업 도메인별로 독립적인 정보보호 솔루션들이 존재하였다. 그러나 2010년대 이후부터는 엔드포인트 보안, 네트워크 보안, 보안관제와 같은 영역들로 통합되기 시작하였으며, 통합 플랫폼 내에서도 다시 세분화되는 경향도 보였다. 2020년 이후 부터는 이러한 영역들이 경계가 모호해지면서 다시 통합되는 양상을 보인다.

예를 들어, 엔드포인트 보안의 경우에는 기존의 백신 기능이 EPP로 발전하면서 다양한 PC 보안 기술을 통합하였다. 이후 EPP는 엔드포인트 보안 영역의 중심축이 되면서 EDR로 진화했다가 최근에는 XDR로 발전하였다. XDR은 엔드포인트와 네트워크 보안을 통합하여 위협을 확장 탐지하는 개념으로 등장했으며, MDR은 EDR과 보안관제를 통합하여 더욱 고도화된 형태로 발전하고 있다.

1) 브레인 바이러스 : 360KB 용량의 플로피 디스켓을 감염시켜 3개의 불량 섹터를 생성하는 부트 바이러스
2) CIH 바이러스 : 인터넷 컴퓨터파일 등 여러 경로를 통해 컴퓨터에 상주해 있다가 매년 4월 26일 작동하며, 기본입출력 장치인 바이오스(BIOS)와 하드디스크의 모든 내용을 손상시켜 PC를 뇌사 상태로 만드는 바이러스
3) 슬래머 웜 : 마이크로소프트(Microsoft)의 데이터베이스 관리시스템인 SQL 서버의 허점을 이용하여 MS SQL server를 공격하는 컴퓨터 웜바이러스

그림 Ⅲ-1 | 엔드포인트 보안 고도화 과정



또한, 랜섬웨어 대응 솔루션은 초기에는 백신의 일부 기능으로 포함되었다가 별도의 자동화 기반 분석 장비로 발전하였으며, 시큐어 코딩 솔루션은 취약점 관리와 공급망 보안으로 발전하며 기업 보안에서의 중요한 축이 되었다.

COVID-19 이후 IT 투자가 급격히 확대되고 디지털 트랜스포메이션이 가속화되면서 대부분의 오프라인 비즈니스가 온라인화 되었다. 이로 인해, 기업의 IT 환경이 복잡해지고 대규모화되면서 정보보호의 중요성은 더욱 부각되었다.

특히, 재택근무와 스마트 오피스 확산으로 인해 망분리 규제가 완화되면서, 기업의 보안 요구는 기존의 엔드포인트, 네트워크, 보안관제를 넘어 종합적인 리스크 관리에 중점을 두고 있으며, 제로트러스트(Zero Trust)와 같은 새로운 보안 모델로 이어지고 있다.

연도별 국내 정보보호산업의 특징은 다음과 같다.

그림 Ⅲ-2 | 국내 정보보호산업 트렌드 변화

1986~2000	⇒	2001~2010	⇒	2011~2020	⇒	2021~현재
PC 보안		인터넷 보안		통합 보안		AI 융합 보안
· 백신(안티바이러스) · 접근제어/계정관리 · 보안관제 · 방화벽 · SSL / TLS · 인증		· DB보안 · DRM / DLP · 이메일 보안 · 모바일 디바이스 관리 · 통합위협관리(UTM) · IDS / IPS · 웹보안/WAF · 보안 Switch / Gateway · NAC / 망분리 / 망연계 / VDI · SSL VPN · 네트워크 분석 · 침해사고대응(CERT) · 정보보호컨설팅 · 모의해킹 · 인증 평가 - 정보보호제품 인증		· 엔드포인트 보안 - EPP - PMS - 개인정보보호 · 모바일 앱 보안 · 네트워크 보안 - NGFW - APT 방어 - 랜섬웨어 대응 - DDoS 방어 · 데이터 보안 - 문서 중앙화 - 인증 / 간편 인증 · 보안관제 - SIEM / SOAR · 침해사고대응(CERT) - 침해사고 분석 - RED / BLUE / PURPLE - TI		· AI 기술 개발 · 엔드포인트 보안 - EDR / XDR - CDR · 보안관제 - MDR / MXDR · 침해사고대응(CERT) - ASM - 취약점 관리 - 공급망 보안 · 네트워크 보안 - 무선 보안 · 융합보안 - IoT 보안 - OT 보안 - 홈 네트워크 보안 - 차량 보안 · 클라우드 보안 - CWPP - CSPM - CNAPP - CASB - ZTNA

참고

용어 풀이

연번	용 어	설 명
1	SSL	보안 소켓 계층 / Secure Sockets Layer · 월드 와이드 웹 브라우저(www)와 웹 서버 간에 데이터를 안전하게 주고받기 위한 표준 프로토콜
2	TLS	전송 계층 보안 / Transport Layer Security · 인터넷상에서 데이터의 도청이나 변조를 막기 위해 사용되는 SSL보다 보안성이 강화된 프로토콜
3	DRM	디지털 저작권 관리 / Digital Rights Management · 디지털 콘텐츠에 비인가자가 접근할 수 없도록 보호하고, 불법으로 복제되어 사용되는 것을 방지하는 기술
4	DLP	데이터 유출 방지 / Data Loss Prevention · 주요 데이터를 보호하고, 데이터가 비인가자에게 노출되거나 외부로 유출되지 않도록 보호하는 기술
5	UTM	통합 위험 관리 / Unified Threat Management · 침입 차단 시스템, 가상 사설망 등 다양한 보안 솔루션 기능을 하나로 통합한 보안 솔루션
6	IDS	침임 탐지 시스템 / Intrusion Detection System · 네트워크 트래픽 또는 시스템 활동을 모니터링하여 비정상적인 패턴이나 이상 행위를 감지하는 솔루션
7	IPS	침입 방지 시스템 / Intrusion Prevention System · 침입 탐지 후 이를 차단하여 대응까지 수행하는 솔루션
8	WAF	웹 애플리케이션 방화벽 / Web Application Firewall · HTTP 프로토콜 이지 기능을 갖춘 프록시 서버
9	NAC	네트워크 접근제어 / Network Access Control · 네트워크에 접속하는 장치에 대해 접속 가능 여부를 확인하여 인가된 장치만이 접속할 수 있도록 제한하는 기술
10	VDI	데스크톱 가상화 / Virtual Desktop Infrastructure · 물리적으로 존재하지는 않지만 실제 작동하는 컴퓨터 안에서 작동하는 하나의 컴퓨터를 만드는 기술
11	SSL VPN	보안 소켓 계층 가상 사설망 / Secure Sockets Layer Virtual Private Network · 장소나 단말의 종류와 관계없이 내부 네트워크에 접속할 수 있는 SSL 기반의 가상 사설망

연번	용 어	설 명
12	CERT	침해사고대응 / Computer Emergency Response Team · 정보통신망 및 정보시스템에 대한 침해사고 예방과 대응을 위해 조직된 기관 내 또는 기업 내 비상대응팀
13	EPP	엔드포인트 통합보안 플랫폼 / Endpoint Protection Platform · 엔드포인트 수준에서 위협을 탐지하고 예방하도록 설계된 보안 솔루션
14	PMS	패치 관리 시스템 / Patch Management System · PC의 패치 상태를 직접 확인하고, 사용자의 필요에 따라 패치를 간편하게 설치, 관리할 수 있게 하는 시스템
15	NGFW	차세대 방화벽 / Next Generation Firewall · 3세대 방화벽 기술의 일부로, 기존 방화벽과 인라인 딥 패킷 검사(DPI)를 사용하는 애플리케이션 방화벽, 침입 방지 시스템(IPS)과 같은 다른 네트워크 장치 필터링 기능을 결합하는 방화벽
16	APT	지능형 지속 공격 / Advanced Persistent Threat · 실시간으로 해킹 공격을 시도하는 것이 아니라 미리 악성코드를 숨겨 놓았다가 시간이 지난 뒤 동시에 작동시키는 해킹 방식
17	DDoS	분산 서비스 거부 공격 / Distributed Denial of Service Attack · 감염된 대량의 숙주 컴퓨터를 이용해 특정 시스템을 마비시키는 사이버 공격
18	SIEM	보안 정보 및 이벤트 관리 / Security Information & Event Management · 다양한 보안 장비와 서버, 네트워크 장비 등으로부터 보안 로그와 이벤트 정보를 수집한 후 정보들 간의 연관성을 분석하여 위협 상황을 인지하고, 침해사고에 신속하게 대응하는 보안관제 솔루션
19	SOAR	보안 오케스트레이션, 자동화 및 대응 / Security Orchestration, Automation & Response · 보안 도구를 통합 및 조정하고 반복적인 작업을 자동화하며 위협 대응 과정을 간소화할 수 있도록 지원하는 소프트웨어 솔루션
20	RED / BLUE / PURPLE	· RED팀 : 공격 기반의 보안팀으로, 침투테스트와 같이 실제 공격자의 행동과 TTPs 재현 등을 통한 보안 업무 수행 · BLUE팀 : 방어 기반의 보안팀으로 보안관제 및 취약성 평가 등을 통한 사이버 공격으로부터 방어하는 보안 업무 수행 · PURPLE팀 : 방어 및 공격 기반의 보안팀으로, RED팀과 BLUE팀의 업무를 통합하여 보안 업무 수행
21	TI	위협 인텔리전스 / Threat Intelligence · 네트워크, 디바이스, 애플리케이션, 데이터 등 보안 위협에 대한 증거 기반 정보

연번	용 어	설 명
22	EDR	엔드포인트 위협 탐지 및 대응 / Endpoint Detection & Response · PC, 랩탑 또는 서버와 같은 엔드포인트 디바이스에서 사이버 위협을 탐지하고 조사하도록 설계된 솔루션
23	XDR	확장된 탐지 및 대응 / eXtended Detection & Response · 탐지 범위를 엔드포인트 너머로 확장하여 여러 데이터 소스에서 탐지, 분석 및 대응을 제공하는 솔루션
24	CDR	콘텐츠 악성코드 무해화 / Content Disarm & Reconstruction · 파일에서 잠재적으로 악성 코드를 제거하기 위한 컴퓨터 보안 기술
25	MDR	관리형 탐지 및 대응 / Managed Detection & Response · 보안 기술과 사람의 전문 지식이 결합되어 관리되는 위협 탐지 및 대응 서비스
26	MXDR	관리형 확장 탐지 및 대응 / Managed eXtended Detection & Response · MDR과 XDR이 통합된 솔루션으로, 엔드포인트를 넘어 포괄적인 적용 범위에 대해 실시간으로 모니터링하는 위협 탐지 및 대응 서비스
27	ASM	공격 표면 관리 / Attack Surface Management · 조직의 공격 표면에 대한 해커의 관점과 접근 방식을 취하는 프로세스 및 기술
28	CWPP	클라우드 워크로드 보안 / Cloud Workload Protection Platform · 클라우드 환경에서 실행되는 애플리케이션(워크로드)을 보호하는 보안 솔루션
29	CSPM	클라우드 보안 형상관리 / Cloud Security Posture Management · 클라우드 환경의 보안 설정을 자동으로 관리하고 오류를 감지하는 기술
30	CNAPP	Cloud Native Application Protection Platform · 단일 사용자 인터페이스에서 여러 클라우드 보안 솔루션을 통합하여 조직에서 전체 클라우드 애플리케이션 공간을 보다 쉽게 보호하는 플랫폼
31	CASB	클라우드 접근 보안 중개 서비스 / Cloud Access Security Broker · 클라우드 서비스를 이용하는 사용자 단말기와 다수의 클라우드 서버 사이에서 클라우드 보안 기능을 제공하는 서비스
32	ZTNA	Zero Trust Network Access · 네트워크 내부와 외부에 모두 보안 위협이 존재한다고 가정하는 'Zero Trust' 보안 모델을 구현할 수 있게 해주는 기술

1986년 ~ 2000년도

- IBM PC 출시로 PC 중심의 기업 업무 환경 변화
- 1986년 브레인 바이러스 등장으로 무료 백신 개발
- 1990년대 인터넷 보급과 1997년 IMF로 인한 온라인 금융 서비스 구축과 IT 투자 확대로 인한 인증 및 암호 요구 증가
- 1999년 CIH 바이러스 이후 백신에 대한 요구 증가 및 Y2K 문제로 인한 IT 투자 확대로 정보보호 업체들의 급성장

2001년 ~ 2010년도

- 2001년 슬래머 웜 등장으로 전세계 인터넷 마비
- 닷컴 기업 Boom-up으로 인터넷 서비스 증가, 2000년대 중반 Web2.0 트렌드 등장에 따른 SNS, 블로그 등 모바일 중심 서비스 급증, 온라인 게임 활성화로 인한 아이템 거래 등장, 인터넷 뱅킹 대중화 등으로 인한 계정정보 유출 사고 증가
- 인터넷 서비스 중심의 보안 요구 증가로 서비스 도메인별 차별화된 보안 솔루션 등장 (키보드 보안, PC 방화벽, 인증, 데이터암호화 등)

2011년 ~ 2020년도

- 7.7 DDoS, 3.4 DDoS 이후 네트워크 보안 요구 증가, DDoS 보안 장비 출시
- 2010년도 초반 APT로 대변되는 개인정보 유출 및 침해사고 급증으로 APT 보안 장비 출시 및 글로벌 기업들의 적극적인 국내 진출
- 2011년 개인정보보호법 발효 이후, 개인정보 암호화 솔루션 및 DB 보안 솔루션 도입 증가
- 엔드포인트 보안, 네트워크 보안, 보안관제를 중심으로 통합 보안 기업 등장
- 2017년 WannaCry 이후 랜섬웨어 피해 급증에 따른 랜섬웨어 대응 솔루션에 대한 요구 및 수요 증가

- 2010년도 후반 클라우드와 AI의 대중화로 인한 클라우드 보안 개념 정립 및 Unknown / Abnormal Detection에 대한 AI 기술 요구 증가
- 위협 정보 공유와 예측, AI 기반 서비스를 위한 CTI(Cyber Threat Intelligence) 플랫폼 등장으로 정보보호산업의 기술적 진화 요구 증가

2021년 ~ 현재

- COVID-19 이후 IT 투자 확대와 급속한 디지털 트랜스포메이션으로 인한 IT 환경의 복잡도 증가와 대규모화 진행
- 재택근무, 스마트 오피스 활성화, 망분리 규제 완화, 물리보안 등 사이버 보안 영역 확대
- CTI와 AI 기술의 발전으로 기존 진단 / 대응 관점 체계에서 이기종 솔루션들의 통합과 리스크 관리에 초점을 둔 XDR 제품 및 MXDR 서비스 등장
- 클라우드 대중화로 제로트러스트 보안과 멀티 클라우드 보안 솔루션 요구 증가
- 5G/IoT 에 대한 보안 중요성 부각
- 취약점 관리를 통한 침해사고 대응과 융합 보안의 요구가 증가하면서 SBOM (Software Biill Of Material) 개념이 등장하고, OT보안과 공급망 보안의 중요성 부각

이를 통해 정보보호산업에는 다음과 같은 변화가 예상된다.

○ 국내 정보보호산업 성장 및 경쟁 심화

- 국내 정보보호산업의 성장은 엔드포인트 보안 솔루션과 같이 지역적 특성에 의존도가 높은 영역[4]이 주도하고 있으며, 해당 솔루션은 글로벌 시장 보다는 국내에 최적화 되어 있다.
- 보안관제는 매출이 성장할수록 비용도 증가하는 구조적 한계[5]를 가지고 있어 수익 구조 변화에 대한 요구가 증가할 것으로 예상된다.
- 보안 대응 비용(엔진 업데이트, 사고 분석 등)에 대한 현실화가 되지 않는 상태에서의 시장 성장은 수익률 문제로 이어질 수 있어서, 가격 정책 변화에 대한 요구가 증가할 것으로 예상된다.
- 국내 시장의 성장과 더불어 글로벌 제품과의 경쟁이 심화할 것으로 예상된다.

○ 클라우드 서비스로의 전환

- 하이브리드 클라우드[6]와 멀티 클라우드[7] 트렌드와 달리, 실제 기업 환경의 변화는 더디게 진행되며, 기존 전통적인 보안 솔루션과 장비는 지속적으로 성장할 것으로 예상된다.
- MS, AWS 등 글로벌 클라우드 플랫폼 기업들이 주도하고 있어 국내 정보보호 기업은 기업별로 특화된 서비스에 집중하는 경향을 보일 것으로 예상된다.
- ZTNA, SASE(Secure Access Service Edge) 등 새로운 보안 아키텍처에 대한 도입 요구가 증가할 것으로 예상된다.

4) 과거에는 글로벌하게 광범위한 악성코드가 많았으나, 최근에는 APT와 같이 특정 기업이나 기관을 대상으로 하는 타겟형 악성코드가 주를 이루고 있음. 또한, 지역마다 IT 업무 환경의 차이로 인한 특성이 있음. 예를 들어, 아래한글이나 인터넷 뱅킹과 같은 비즈니스 환경은 국내에서만 사용하고 있음

5) 현재의 보안관제는 사업수주에 따라 인력을 채용하는 인건비 중심의 사업 영역으로, 보안업체에서는 계약이 만료되면 기존 인력을 유지하는 데에 어려움을 겪고 있음. 따라서 보안업체 입장에서는 고객사가 선호하는 석사급 고급 인원을 확보하기 위해 인건비가 증가하고 있는 상황임

6) 하이브리드 클라우드 : 온프레미스(또는 프라이빗 클라우드)와 퍼블릭 클라우드를 결합하여 사용하는 것을 의미함. 퍼블릭 클라우드로 모든 서비스를 이전하기 보다는, 기존 인프라를 활용하여 비용을 최소화하고 컴플라이언스가 중요한 환경에서 온프레미스로 주요 데이터를 관리할 목적으로 활용함

7) 멀티 클라우드 : 2개 이상의 퍼블릭 클라우드(AWS, Azure, Google Cloud, Naver Cloud 등)를 사용하는 것을 의미함. 특정 서비스에 적합한 클라우드를 선택하여 특정 클라우드 사업자에 종속되지 않도록 하고, 서비스의 최적화가 목적임

AI 기술 확보를 위한 움직임

- 중견 정보보호 기업에서는 AI 기반의 보안 스타트업을 발굴하고 투자 규모가 확대될 것으로 기대되며, 스타트업 인수 합병도 적극적으로 이루어 질 것으로 예상된다.
- 머신러닝을 활용한 위협 탐지(Threat Detection), 이상 행동 탐지(Abnormal Detection), 자동화된 대응 기술 경쟁력 확보에 지속적 투자가 증가할 것으로 예상된다.
- AI 기반 SOAR 도입과 자동화 구축을 통한 보안관제 비용 최소화를 위한 지속적인 투자가 예상된다.

글로벌 진출 다각화

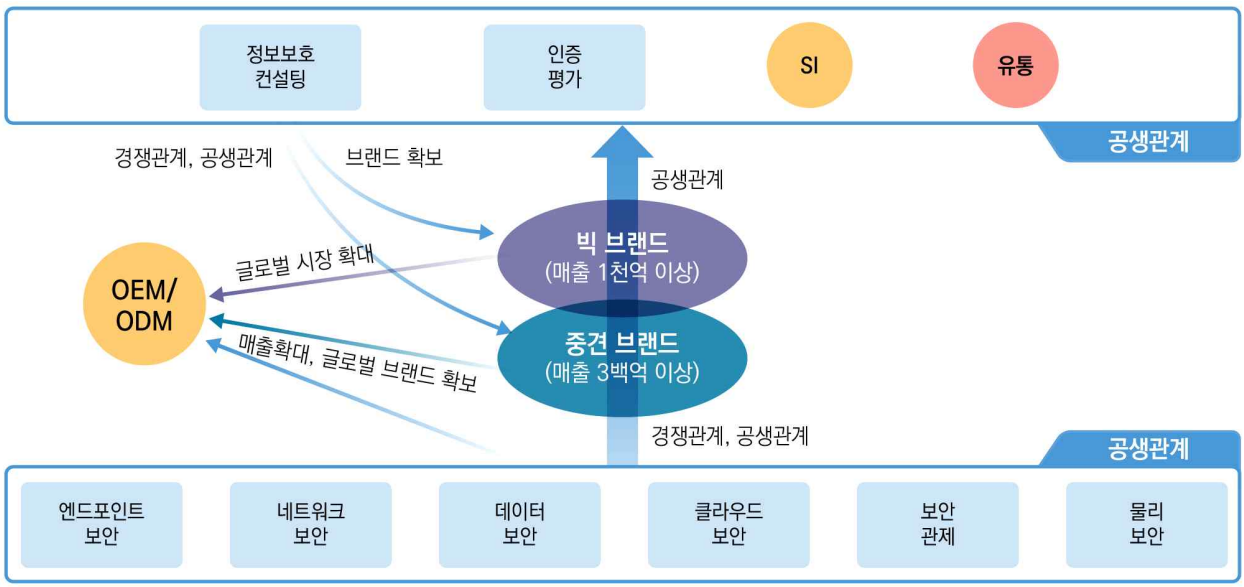
- 지역적 특성 의존도가 높은 분야는 솔루션 수출보다는 현지 기업과의 JV(Joint Venture) 설립을 통한 글로벌 진출이 증가할 것으로 예상된다.
- 클라우드 SaaS형 솔루션들이 지속적으로 등장할 것으로 예상되나, 네임드 브랜드가 아닌 경우에는 실질적인 매출 성장이 더딜 것으로 예상된다.
- 글로벌 기업 또는 현지 기업과의 OEM/ODM을 통한 글로벌 진출 증가가 예상되며, 클라우드 SaaS형 솔루션도 네임드 브랜드와의 OEM/ODM이 활발하게 진행될 것으로 예상된다.
- 글로벌 시장에서 안정적으로 사업을 영위 중인 국내 기업을 통한 글로벌 진출은 기존처럼 지속적으로 유지될 것으로 예상된다.

종합해보면, 정보보호산업의 시장 규모는 IT 환경의 변화와 투자 규모에 따라 지속적으로 성장하는 경향을 보인다. IT 기술에 대한 의존도가 높아질수록 정보보호에 대한 요구는 증가할 수밖에 없으며, 클라우드·IoT·AI와 같은 기술이 발전할수록 정보보호는 필수적인 요소로 자리 잡게 될 것이다. 이러한 점에서 정보보호산업은 지속적으로 성장할 것으로 예상된다.

3. 정보보호산업 생태계 구조

정보보호산업 생태계는 사업영역에 따라 8개의 정보보호 전문기업(엔드포인트 보안, 네트워크 보안, 데이터 보안, 클라우드 보안, 보안관제, 물리보안, 정보보호컨설팅, 인증평가)과 3개의 유관 사업 영위기업(SI, OEM/ODM, 유통)으로 기업군을 분류할 수 있다.

그림 Ⅲ-3 | 정보보호산업 생태계 구조



이 중 사업영역으로 인증평가 분야를 영위하는 기업은 보안성을 평가·인증할 수 있는 기관이 별도로 지정되어 있다는 특수성으로 인해 대부분 해당 분야만 특화한 기업 활동을 전개하는 경우가 대다수이다. 그러나 그 외 영역은 기업의 특성에 따라 다양한 영역을 종합하여 영위하는 사례가 다수 존재한다.

이에 따라 본 보고서에서는 '빅브랜드'를 세 개 이상의 사업분야를 영위하고 매출액이 1천억 이상인 기업으로, '중견브랜드'는 두 개 이상의 사업을 영위하고 매출액이 3백억 이상인 기업으로 정의하였다.

정보보호산업 생태계를 리딩하는 빅브랜드의 경우, OEM/ODM 업체에 자사의 모듈을 판매하여 글로벌 시장 확대를 추진하고 있으며, 중견브랜드는 OEM/ODM 업체를 통해 매출 및 글로벌 브랜드를 확보해나가고 있다.

2023년 이후 매출이 1천억 이상인 정보보호기업이 급격히 증가하는 것으로 보아 정보보호산업은 그 규모와 더불어 생태계의 일원인 기업의 경쟁력도 점차 성장하고 있음을 알 수 있다. 11개 영역의 기업들은 서로 경쟁하면서도 동시에 공생하며 정보보호 생태계를 구성하고 정보보호산업의 성장을 도모하고 있다.

엔드포인트 보안

엔드포인트란 네트워크와 연결된 최종적 IT기기 및 단말을 말한다. 엔드포인트 보안은 이러한 엔드포인트, 즉 컴퓨터, 노트북, 스마트폰, IoT기기 등 네트워크와 연결되는 개별 단말(디바이스)의 보안 수준을 향상시킴으로써 외부 공격에 대응하기 위한 솔루션이다. 최근에는 확장된 개념의 XDR 솔루션이 출시되어 새로운 트랜드를 주도하고 있다.

* 예) 엔드포인트 위협 탐지 및 대응(EDR), 악성코드/랜섬웨어 대응, 지능형 지속 공격(APT) 대응, 모바일 단말 보안, 콘텐츠 악성코드 무해화 기술(CDR) 등

네트워크 보안

인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스, 네트워크상의 정보를 보호하는 정보보호 활동을 총칭하며, 암호화, 전자서명, 접근통제, 데이터 무결성, 인증 교환 등의 보안 메커니즘을 활용한 정보보안 시스템이다.

* 예) 웹 애플리케이션 방화벽(WAF), 방화벽, 침입 방지 시스템(IPS), DDoS 대응, 가상사설망(VPN), 네트워크 접근제어(NAC), 무선 네트워크(Wireless Network) 보안, 네트워크 위협 탐지 및 대응(NDR), 망분리, 데스크톱 가상화 등

데이터 보안

디지털콘텐츠 불법 복제 및 유통 방지를 위한 기술적, 관리적 수단이나, 내부 기밀정보의 유출을 탐지하고 차단하는 기능을 제공하는 정보보안 시스템이다.

* 예) 네트워크 데이터유출방지(DLP), 디지털저작권관리(DRM), 보안USB, DB보안/DB암호, 인쇄물 보안, 메일 보안, 개인정보 비식별화 솔루션, 문서중앙화 솔루션 등

클라우드 보안

클라우드 시스템 자체를 보호하기 위한 각종 기술 및 관리적 수단, 솔루션 등을 포함하는 정보보안 시스템이다.

* 예) 클라우드 워크로드 보안(CWPP), 클라우드 보안 형상관리(CSPM), CASB, SASE, 가상화 관리 등

보안관제

고객의 IT자원 및 보안시스템에 대한 운영 및 관리를 전문적으로 아웃소싱(outsourcing)하거나 원격관제를 통해 각종 침입에 대체 중앙관제센터에서 365일 24시간 실시간으로 감시 및 분석, 대응하는 서비스이다. 대부분 SIEM, SOAR 등을 자체 개발하여 운영하며, 최근에는 솔루션으로 출시하여 판매하기도 한다. 최근에는 MDR, MXDR 서비스가 출시되면서 새로운 시장을 개척하고 있다.

* 예) 원격관제 서비스, 파견관제 서비스, TI 서비스, SIEM, SOAR 등

정보보호컨설팅

조직의 목적을 달성하는데 있어 전산시스템과 네트워크 등 모든 IT 자산과 조직에 일어날 수 있는 위험을 분석하고 이에 대한 대책을 수립함으로써 관리자와 조직이 그 대책을 실현할 수 있도록 지원하는 독립적인 전문자문 서비스이다.

* 예) 정보감사, 개인정보보호컨설팅, 기반시설보호컨설팅 등

인증평가

조직이 수립 및 운영하는 관리체계가 정보보호 측면에서 적합한지를 판단하는 제도로 인증을 통해 정보보호 관리에 대한 인식을 제고해 보호해야할 정보통신망 및 정보자산의 안전성과 신뢰성을 향상시키는 것이 목적이다.

* 예) ISO, ISMS, CC 등

물리보안

조직의 시설, 장비, 데이터 등을 물리적인 위협으로부터 보호하기 위한 보안 대책을 수립하고 실행하는 것을 의미하며, 침입, 도난, 화재, 자연재해 등 물리적 사고로 인한 자산의 손실을 예방하는 데 중점을 둔다. 이를 통해 조직의 자산 보호 및 안전한 업무 환경을 유지하는 것이 목적이다.

* 예) 출입통제시스템, CCTV, 생체인식 시스템, 보안 게이트 등

SI

보안 솔루션 및 인프라를 구축하는 서비스를 의미하며, 정보보호제품을 개발 후 인증평가를 받아 SI 업체와 함께 시스템을 통해 구축하여 유통(영업)한다.

유통

정보보호 솔루션과 서비스를 최종 사용자에게 제공하는 채널 구조를 말한다. 일반적으로 제조사가 직접 유통하는 직판 구조와 총판, 파트너, 대리점(리셀러) 구조를 가지며, 총판과 파트너는 판매와 기술지원이 모두 가능하다. 이를 통해 고객의 산업군에 맞는 적합한 판매 정책과 기술지원 서비스를 제공하는 것이 목적이다.

OEM/ODM

주로 해외 업체로 구성되어 있다. 정보보호 솔루션 및 장비를 국내 기업들이 설계 및 제조하여 글로벌 네임드 브랜드에 공급하는 비즈니스 모델로, 국내 제조사들이 고도의 기술력을 바탕으로 글로벌 시장에서 경쟁력을 확보하고 있다. OEM(Original Equipment Manufacturing)은 글로벌 브랜드의 요구에 맞춰 제품을 제조하여 공급하는 방식이며, ODM(Original Design Manufacturing)은 제품 설계부터 제조까지 포함한 서비스를 제공한다. 이를 통해 국내 기업들은 기술력을 인정받아 세계적인 브랜드와 협력하고, 글로벌 시장에 진출할 수 있는 기회를 확대하고 있다.

참고

2024년 국내 정보보호산업 실태조사

정보보호산업 기업 현황

2023년 국내 소재 정보보호 기업은 정보보안 814개, 물리보안 894개로 총 1,708개로 조사됨

최근 3년 국내 정보보호산업 기업 현황

단위 : 개

구 분	정보보안	물리보안	합 계
2021	669	848	1,517
2022	737	857	1,594
2023	814	894	1,708

정보보호산업 기업 형태

2023년 정보보호 기업의 형태는 대기업이 112개(6.6%), 중기업이 678개(39.7%), 소기업이 918개(53.7%)인 것으로 나타남

2023년 정보보호 기업 형태별 현황

단위 : 개, %

구 분	기업수	비 율
대기업	112	6.6
중기업	678	39.7
소기업	918	53.7
합계	1,708	100

정보보호산업 매출 현황

2023년 정보보호산업 매출액은 총 16,831,047백만 원으로 2022년 대비 4.0% 증가한 것으로 조사되었으며, 2016년 9,042,811백만 원에서 연평균 9.3%씩 지속적으로 성장하고 있음

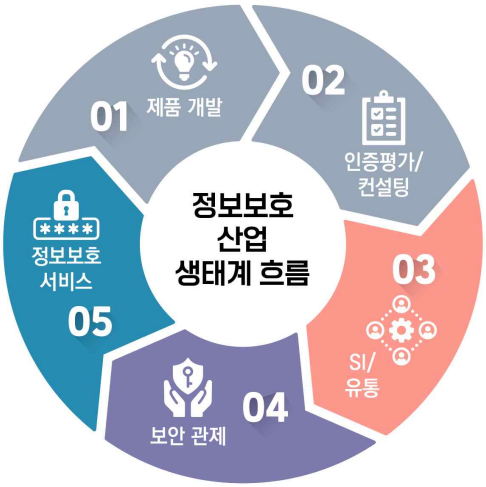
최근 3년 국내 정보보호산업 매출 현황

단위 : 백만 원, %

구 분	정보보안		물리보안		합 계	
	매출액	성장률	매출액	성장률	매출액	성장률
2021	4,549,734	+16.0	9,311,446	+12.1	13,861,180	+13.4
2022	5,615,295	+23.4	10,563,226	+13.4	16,178,521	+16.7
2023	6,145,479	+9.4	10,685,568	+1.2	16,831,047	+4.0

이러한 정보보호산업의 생태계는 제품 개발, 인증평가/컨설팅, SI/유통, 보안관제, 정보보호서비스 순으로 밸류체인이 구성되며, 제품이 업데이트 됨에 따라 이 사이클은 계속 순환되는 구조를 형성한다.

그림 Ⅲ-4 | 정보보호산업 생태계 사이클



○ 제품 개발(개발사)

- 개발사에서 제품을 기획, 설계 디자인 진행하여 소프트웨어 개발, 펌웨어, PCB 제작, 외형 제작 이후 조립을 통해 제품을 완성하고 QA를 통해 솔루션이나 서비스가 출시된다.
- 엔드포인트 보안, 네트워크 보안, 데이터 보안, 클라우드 보안 사업을 영위하는 기업이 제품 개발에 포함된다.
- 이 과정에서 데이터, 외주 모듈, 외주 개발, 부품 및 센서를 공급하는 외주 업체들이 중간 과정을 제공하기도 한다.

○ 인증평가 / 컨설팅

- 공공기관에 개발된 제품을 납품하기 위해서는 CC, GS, 신속확인제, 보안적합성 검증, CSAP, ISMS, ISMS-P 등 다양한 인증을 받아야 한다.
- 기업에서 직접 진행하기도 하지만 컨설팅 업체에서 이 과정을 수행하며, 이 과정에서 모의해킹과 취약점 분석을 같이 진행한다.

SI / 유통

- SI는 보안 제품을 어떤 제품으로 구축할지 선정하고 고객의 요구에 맞게 커스터마이징 하거나, 제품을 운영하기 위한 부가적인 서비스도 같이 개발한다.
- 정보보호 기업은 유통 관리를 위해 세일즈 마케팅을 진행하며, 보통 총판과 대리점, 리셀러 형태로 운영된다.

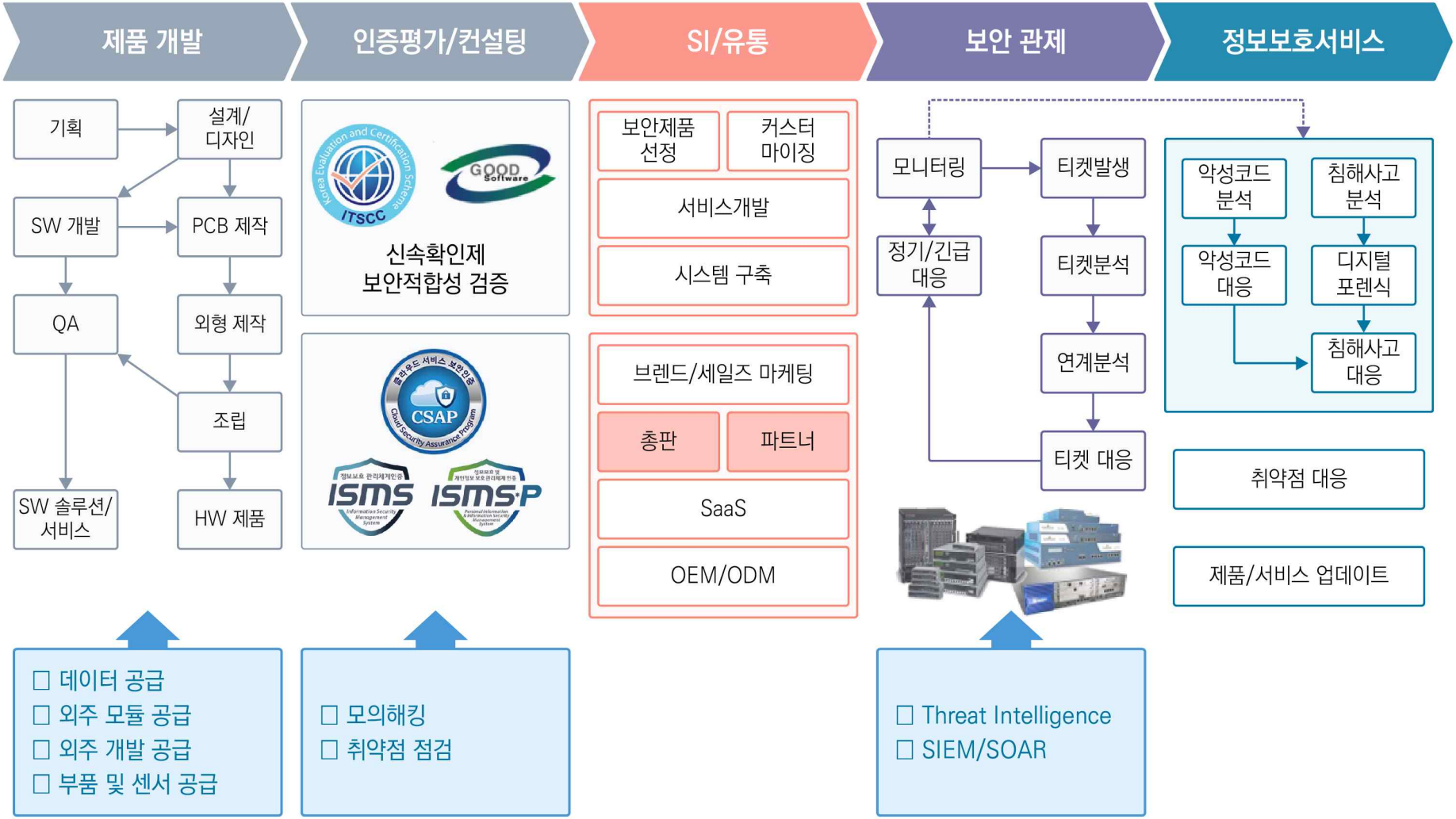
보안관제

- 제품이 구축되면 보안관제를 통해 모니터링을 진행하며, 모니터링 도중 네트워크에서 이상 오류가 발생할 경우 이를 분석하고 관련된 추가 데이터를 연계 분석하여 대응한다.
- 최근에는 TI, SIEM, SOAR 등을 자체 개발하여 운영하며, 솔루션 형태로 출시하여 매출 증대를 목표로 하고 있다.

정보보호서비스

- 이후 제공한 정보보호 제품에 대해 주기적인 분석 및 대응 등 다양한 서비스를 제공하게 된다. 악성코드, 침해사고, 취약점 등을 분석하여 이에 대한 대응, 제품에 대한 오류 해결 및 기능 개선 등 꾸준한 업데이트를 제공한다.
- 다수의 엔드포인트 보안, 네트워크 보안, 데이터 보안, 클라우드 보안 사업을 영위하는 기업이 해당 제품에 대한 정보보호서비스도 같이 제공하고 있으며, 보안관제나 정보보호컨설팅 사업을 영위하는 기업도 정보보호서비스에 포함된다.
- 현재에는 규모가 큰 기업을 중심으로 물리보안 서비스가 제공되고 있으며, 향후에는 물리보안 분야와 관련된 정보보호서비스의 범위가 점차 확장될 것으로 예상된다.

그림 Ⅲ-5 | 정보보호산업 생태계 밸류체인



직무변화 모니터링 결과

PART. 04

4 직무변화 모니터링 결과

정보보호 분야 직무맵에 기반하여 설정한 총 19개의 직무를 6개 분야로 분류하고 설문조사를 진행하였다.

이후 설문조사 결과에 따라 가장 많은 변화가 발생한 2개의 주요 직무를 대상으로 전문가 FGI를 실시하여 세부적인 직무변화 내용을 도출하였으며, 정량 연구 수행을 위해 그 외 6개의 분야별 대표 직무에 대해서도 심층 인터뷰를 실시하여 직무변화를 추가적으로 파악하였다.

- FGI : 정보보호개발, 클라우드보안관리운영
- 인터뷰 : 연구·개발(정보보호개발), 운영·관리(정보보호엔지니어링), 조사·대응(보안관제, 디지털포렌식), 진단·평가(정보보호컨설팅), 신기술보안(모빌리티보안), 기타(기술영업)

정보보호 분야 직무 구분

구분	직 무	정 의
연구·개발	정보보호기획	조직의 목표 달성과 정보자산의 보호를 위해 정보보호 전략, 거버넌스, 운영정책, 정보보호 제품 및 솔루션을 기획하는 일이다.
	정보보호개발	정보보호제품에서 요구되는 요구사항을 분석하여 정보보호제품을 설계하고, 보안 요구사항에 대한 테스트 및 검증하는 일이다.
	정보보호운영/관리	정보 자산을 안전하게 운영하기 위하여 정보보호 제품 및 솔루션을 운영하고, 법제도를 준수하여 보호관리 활동을 수행하며, 도출된 정보보호 대책을 기반으로 관리하는 일이다.
운영·관리	정보보호엔지니어링	정보서비스의 보안 요구사항에 따라 정보보안 시스템 설치를 위한 설계, 구축, 유지보수를 수행하는 일이다.
	보안품질관리	정보보호 품질관리를 위하여 전사적인 보안대책을 수립하고 제품 등의 품질보증을 위한 시험 분석, 테스트케이스 작성, 시험 수행 및 보고서를 작성하는 일이다.
	영상정보보안	영상정보의 수집, 저장, 반출, 파기 등 처리 과정에서 기밀성, 무결성, 가용성을 확보하고 접근통제와 오남용 방지, 영상정보관제, 보안사고 대응 등을 수행하는 일이다.

구분	직 무	정 의
조사·대응	보안사고대응	보안사고의 피해확산 방지를 위해 위협정보를 수집, 탐지 및 분석하여 침해사고에 대응하며 정보시스템을 복구하는 일이다.
	보안관제	원격이나 파견 통합 보안관제센터의 시스템, 조직, 역할을 설계하고, 사업목적에 따라 침해사고를 예방하고 대응하는 보안관제센터(SOC)를 구축, 운영, 관리하는 일이다.
	디지털포렌식	디지털기기에서 발생된 특정 행위의 사실 관계를 규명하고, 추후 법정에서 증거자료로 인정될 수 있도록 요건을 갖추어 과학적 방법으로 증거물을 수집, 이동, 보존, 분석, 제출, 검증하는 일이다.
진단·평가	정보보호컨설팅	정보자산을 보호하기 위한 관리적, 물리적, 기술적 영역의 보안 요구사항 및 프로세스를 객관적으로 분석하여 모의해킹, 취약점 점검 등을 통해 개선 방안을 제안하는 일이다.
	보안감사	정보보호를 위한 관련 법, 제도, 정책, 역할, 가이드라인, 규범, 기술표준 등을 준수하도록 지속적으로 통제하고 관리하는 일이다.
	보안감리	정보보호의 효율성과 효과성을 향상시키고 안전성을 확보하기 위하여 제3자의 관점에서 정보보호의 정책 및 기획, 정보시스템 구축 및 운영 등에 관한 사항을 종합적으로 점검하고 문제점이 개선 되도록 시정조치사항을 도출하고 확인하는 일이다.
	보안인증평가	정보보호 제품에 대한 신뢰성 확보와 제품경쟁력 강화를 위하여 정보보호 제품에 대한 보안 요구사항과 보증 요구사항의 적합성 여부를 인증하거나 인증취득을 준비하는 일이다.
신기술보안	클라우드보안관리운영	조직이 클라우드 인프라를 안전하게 활용하기 위하여 정보보호 정책을 기획하며, 이에 따른 보안 운영 업무를 수행하고, 감사를 통해 조직의 클라우드 정보보호 거버넌스를 구현하는 일이다.
	모빌리티보안	모빌리티의 안전한 활용을 위하여 모빌리티 생명주기 전 단계에 걸쳐 보안위협과 위험을 식별하고, 정보보호 조직 구성, 전략과 정책 수립, 법령 준수, 보안성 검증 활동과 대응방안의 수립, 적용, 평가, 인증을 통하여, 모빌리티의 안정성을 확보하는 일이다.
	OT보안	OT환경의 시스템 및 네트워크에 대한 사이버 안전성을 확보하기 위하여 OT보안 체계를 구축하기 위한 개발, 운영, 평가와 위협 및 사고대응 업무를 수행하는 일이다.
기타	기술영업	정보보호 지식을 바탕으로 고객 관리 및 영업 전략 수립과 사업기회를 창출하고 요구사항에 적합한 솔루션제안으로 협약, 계약, 판매, 사후관리를 수행하는 일이다.
	마케팅/홍보	브랜드 인지도와 시장 경쟁력 강화에 기여하기 위한 정보보호 솔루션 마케팅전략을 설계하고 대내외 소통을 통한고객 유지관리와 신규시장을 개척하는 일이다.
	정보보호교육	정보보호 분야의 기술교육을 수행하기 위하여 교육 환경을 조성하며, 교육과정 개발 및 성과 평가를 수행하는 일이다.

직무변화 모니터링 설문 및 심층 인터뷰의 주요 내용은 다음과 같이 요약할 수 있다.

직무변화 모니터링 설문 및 심층 인터뷰 결과(요약)

구 분	직 무	직무수준	직무변화 선행요인	직무변화	역량변화
연구·개발	정보보호기획 정보보호개발	4~6수준	시장환경변화	· 클라우드 서비스로의 전환 · AI를 활용한 업무 수행 · 보안통합 및 오케스트레이션	· 개발 관련 세부 지식 변화 · 설계문서 작성의 중요성 증가 · 표준 및 인증 해석 적용 능력 필요 · 문해력 및 커뮤니케이션 능력 · 신기술에 대한 이해 및 적용
운영·관리	정보보호운영/관리 정보보호엔지니어링 보안품질관리 영상정보보안	3~5수준	시장환경변화	· 보안 기술 통합에 따른 협업 증가 · 업무 강도의 지속적인 증가	· 기술 발전에 따른 요구 수준 증가
조사·대응	보안사고대응 보안관제 디지털포렌식	4~6수준	법·제도변화	· 자동화를 적용한 솔루션 도입	· 업무 수행 범위 확대에 따른 역량 향상
진단·평가	정보보호컨설팅 보안감사 보안감리 보안인증평가	4~6수준	법·제도변화	· 인식 변화로 인한 유입 인원 감소 · 업무 수행 방향 변화	· 법제도 제·개정에 따른 적용 · 사용 도구 변화 및 방법론에 대한 이해
신기술보안	클라우드보안관리운영 모빌리티보안 OT보안	3~6수준	시장환경변화	· 세분화된 부서 운영 · AI 활용의 확대 · 전문성 확장 · 타산업과의 융합으로 인한 높은 수요	· 다양한 클라우드 서비스 활용 경험 요구 · 클라우드 관련 부가서비스 증가 · 임베디드 시스템 및 보안 지식 요구 · 주기적인 법률 모니터링 및 자문 능력
기타	기술영업 마케팅/홍보 정보보호교육	4~6수준	시장환경변화	· 시장 변화에 대한 주기적인 모니터링	· 주기적인 트렌드 파악 능력 · 업무 수행을 위한 작성 문서 증가

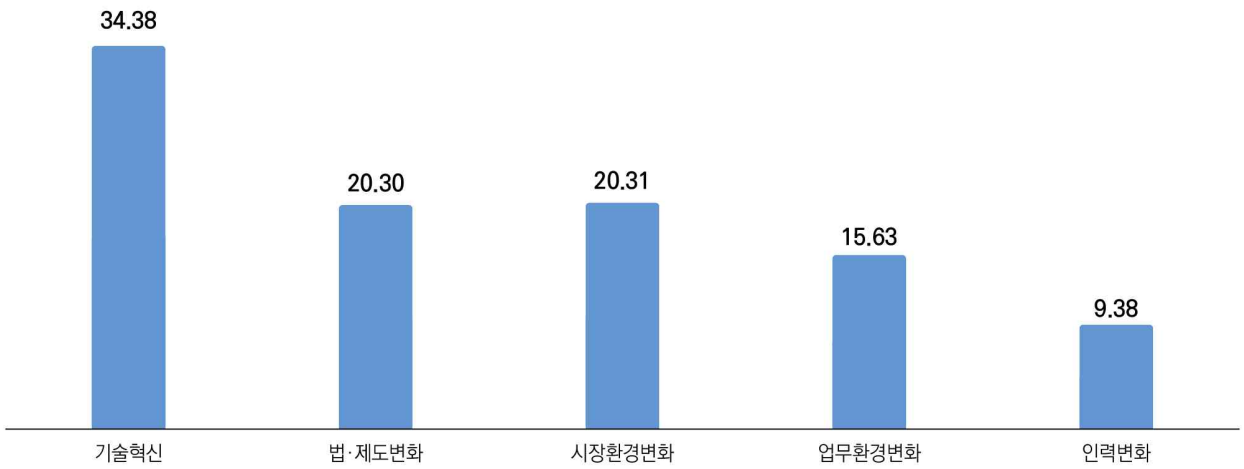
1. 설문조사

정보보호산업 변화 선행요인

최근 정보보호산업의 직무나 일하는 과정의 변화를 초래하는 요인을 살펴보면, 기술혁신 34.38%, 법·제도변화 20.30%, 시장환경변화 20.31%, 업무환경변화 15.63%, 인력변화 9.38%로 나타났다.

그림 Ⅳ-1 | 정보보호산업 변화 선행요인

단위 : %



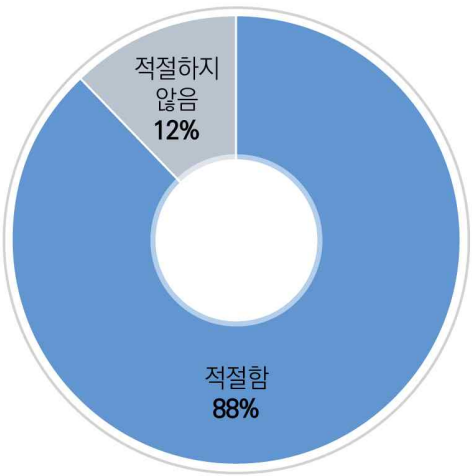
순 위	선행요인	비중(%)
1	기술혁신(인공지능, 자동화 등)	34.38
2	시장환경변화(시장수요, 경쟁, 등)	20.31
3	법·제도변화	20.30
4	업무환경변화(재택근무, 스마트오피스 등)	15.63
5	인력변화(인구감소, 처우·급여 등 개인욕구변화 등)	9.38
합 계		100

구체적인 의견으로는 ▲ 사이버위협 증가 및 해킹 수준의 고도화, ▲ 법적 규제의 변화에 따른 내규 및 업무 절차의 변화, ▲ 최신기술에 대한 이해 및 전문성 요구, ▲ 글로벌 기업 증가에 따른 국가별 규제 준수 필요, ▲ 기술융합이나 타사와의 협업, ▲ 개인중심으로의 삶의 인식 전환, ▲ 경쟁 심화로 인한 잦은 이직 등이 있다.

직무구분의 적절성

정보보호 직무맵을 기준으로 정보보호산업의 직무구분의 적절성을 살펴보면, 적절하다는 의견의 88%, 적절하지 않다는 의견이 12%로 나타났다.

그림 Ⅳ-2 | 직무구분의 적절성



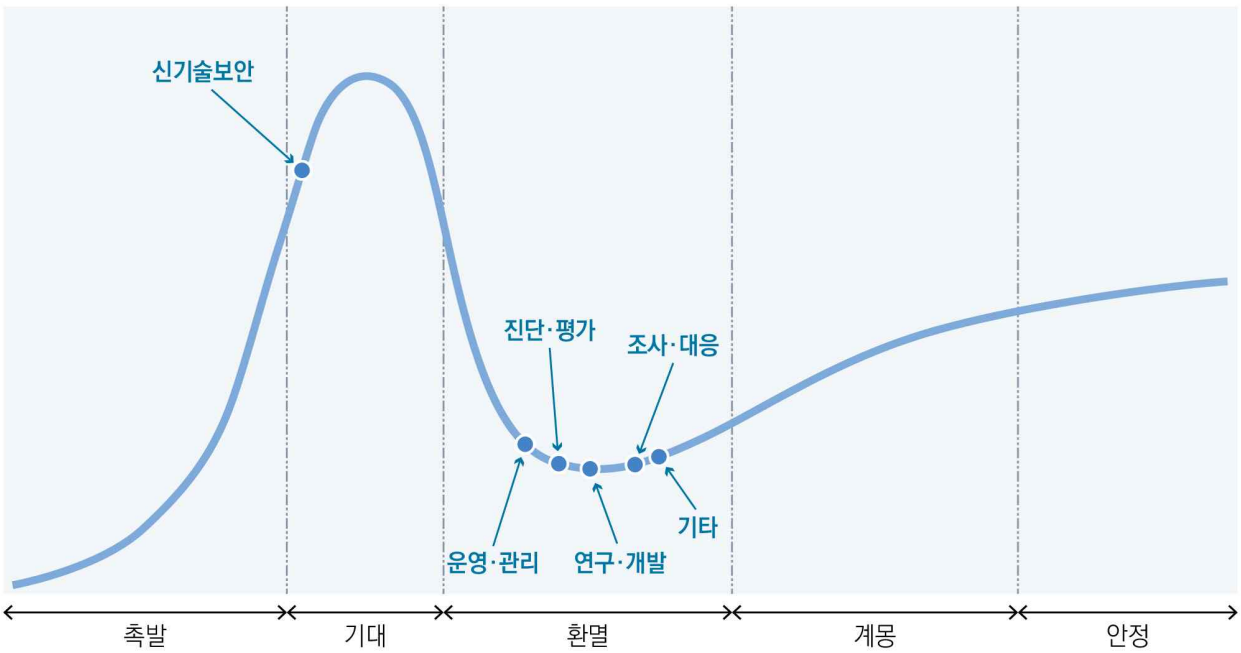
* 5점 척도 기준으로 응답 (1 ~ 2 : 적절함 / 3 ~ 5 : 적절하지 않음)

적절하지 않다고 생각한 이유로는 ▲ 직무 단위가 대기업 중심으로 되어 있다, ▲ 직무 내용이 통합이 되어 있다 등의 의견이 있다. 구체적으로 모의해킹이 '정보보호컨설팅' 하위의 역량이 아닌 '보안진단'등 별도 직무로 분리되는 것이 좋을 것 같다는 의견이 있었다.

직무별 성숙도

가트너(Gartner)의 하이프 사이클(Hype Cycle)에 기반하여 국내 정보보호산업의 직무별 성숙도를 5단계로 나누어 설문을 진행한 결과 기타(3.75), 조사·대응(3.71), 연구·개발(3.50), 진단·평가(3.44), 운영·관리(3.29) 분야는 '환멸' 단계로, 신기술보안(2.12) 분야는 '기대' 단계로 나타났다.

그림 Ⅳ-3 | 국내 정보보호산업 직무별 성숙도



순 위	구 분	직 무				성숙도(평균)
1	기타	기술영업	마케팅/홍보	정보보호교육		3.75
2	조사·대응	보안사고대응	보안관제	디지털포렌식		3.71
3	연구·개발	정보보호기획	정보보호개발			3.50
4	진단·평가	정보보호컨설팅	보안감사	보안감리	보안인증평가	3.44
5	운영·관리	정보보호운영/관리	정보보호엔지니어링	보안품질관리	영상정보보안	3.29
6	신기술보안	클라우드보안관리운영	모빌리티보안	OT보안		2.12

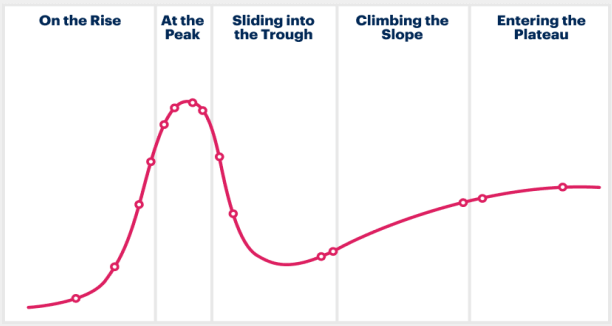
* 5점 척도 기준 (1 : 촉발 / 2: 기대 / 3 : 환멸 / 4 : 계몽 / 5 : 안정)

참고

가트너의 하이프 사이클

- **가트너(Gartner)** 주식회사는 전 세계 85개국에 고객사를 두고 있는 미국의 정보 기술 연구 및 자문회사로, 시장 분석 결과의 시각화 도구로 하이프 사이클 및 매직 쿼드런트를 개발하여 사용하고 있다.
- **하이프 사이클(Hype Cycle)**은 기술의 성숙도를 표현하기 위한 시각적 도구로 성장 주기에 따라 5개의 단계로 이루어진다.

그림 Ⅳ-5 | 하이프 사이클 구조



* 출처 : Gartner(https://www.gartner.com/)

정보보호산업의 직무별 성숙도를 파악하기 위해 하이프 사이클 구조를 참고하여 5개의 단계를 구분하였으며, 각 단계별 특징을 다음과 같이 정의하여 설문조사를 진행하였다.

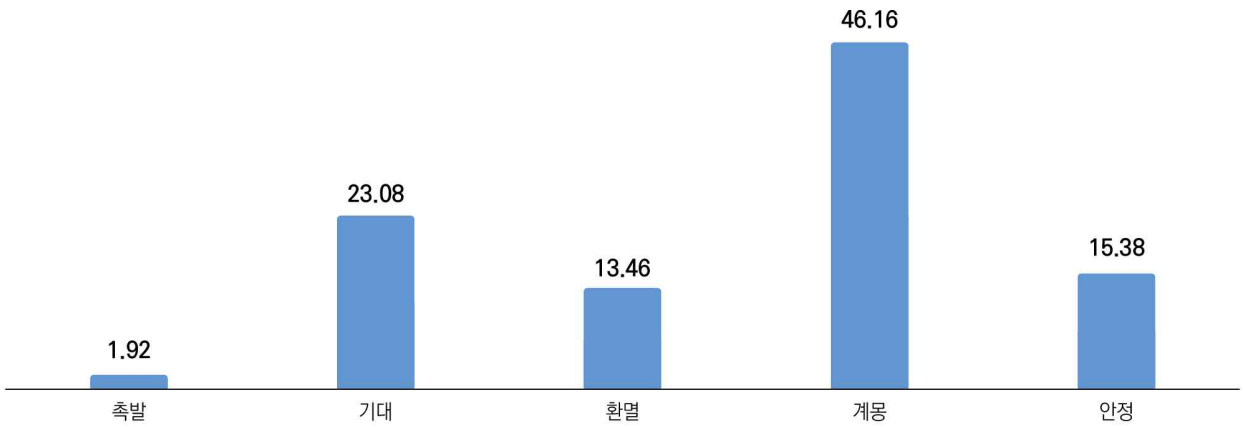
단 계		특 징
1	촉발	· 잠재적 기술이 관심을 받기 시작하는 시기이며, 초기 단계의 개념적 모델과 미디어의 관심이 대중의 관심을 불러일으킨다. · 상용화된 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다.
		→ 해당 업무에 대한 관심이 높아지기 시작하여, 직무의 수요가 예상되는 단계
2	기대	· 초기의 대중성이 일부의 성공적 사례와 다수의 실패 사례를 양산해 낸다. · 일부 기업이 실제 사업에 착수하지만, 대부분의 기업들은 관망한다.
		→ 해당 업무에 대한 관심이 매우 높아져, 직무 종사자가 나타나기 시작하는 단계
3	환멸	· 실험 및 구현이 결과물을 내놓지만 실패함에 따라 관심이 시들해진다. · 제품화를 시도한 주체들은 포기하거나 실패한다. · 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속된다.
		→ 해당 업무에 대한 관심이 시들해짐에 따라, 일부 회사에서만 직무 담당자를 지정하는 단계
4	계몽	· 기술의 수익 모델을 보여 주는 좋은 사례들이 늘어나고 더 잘 이해되기 시작한다. · 2-3세대 제품들이 출시된다. · 더 많은 기업들이 사업에 투자하기 시작한다. · 보수적인 기업들은 여전히 유보적인 입장을 취한다.
		→ 해당 업무가 인정받기 시작하여, 다수의 회사에서 직무 담당자를 보유하기 시작하는 단계
5	안정	· 기술이 시장의 주류로 자리 잡기 시작한다. · 사업자의 생존 가능성을 평가하기 위한 기준이 명확해진다. · 시장에서 성과를 거두기 시작한다.
		→ 해당 업무가 자리 잡기 시작함에 따라, 다수의 회사에서 직무 담당자를 안정적으로 보유하는 단계

○ 연구·개발

연구·개발 분야 직무의 산업 내 성숙도는 촉발 1.92%, 기대 23.08%, 환멸 13.46%, 계몽 46.16%, 안정 15.38%로 나타났다.

그림 Ⅳ-6 | 연구·개발 분야 산업 내 성숙도

단위 : %

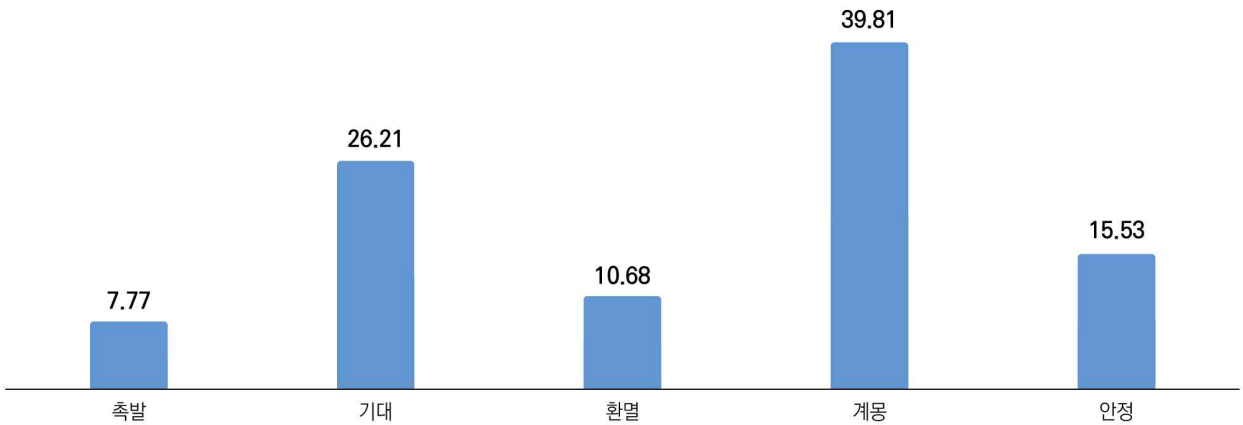


○ 운영·관리

운영·관리 분야 직무의 산업 내 성숙도는 촉발 7.77%, 기대 26.21%, 환멸 10.68%, 계몽 39.81%, 안정 15.53%로 나타났다.

그림 Ⅳ-7 | 운영·관리 분야 산업 내 성숙도

단위 : %

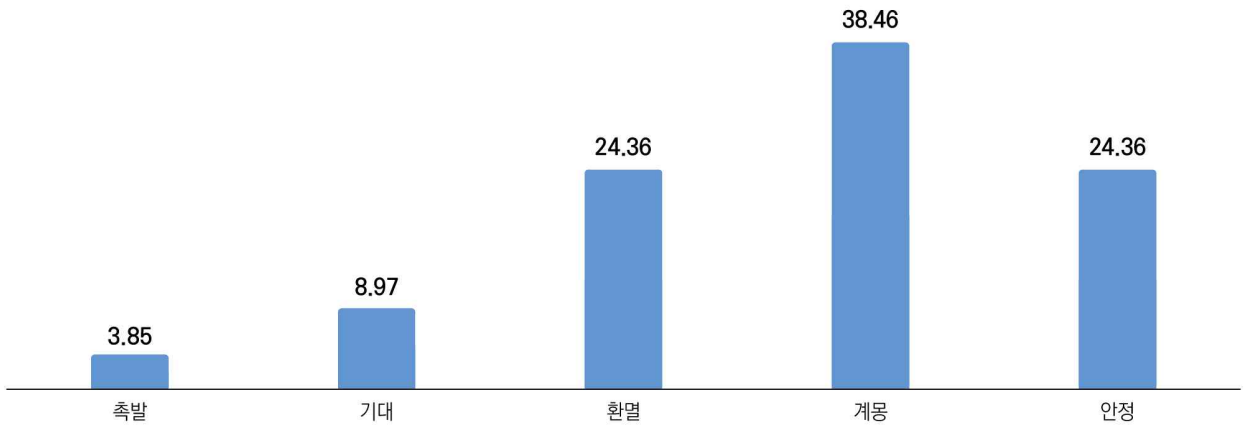


○ 조사·대응

조사·대응 분야 직무의 산업 내 성숙도는 촉발 3.85%, 기대 8.97%, 환멸 24.36%, 계몽 38.46%, 안정 24.36%로 나타났다.

그림 Ⅳ-8 | 조사·대응 분야 산업 내 성숙도

단위 : %

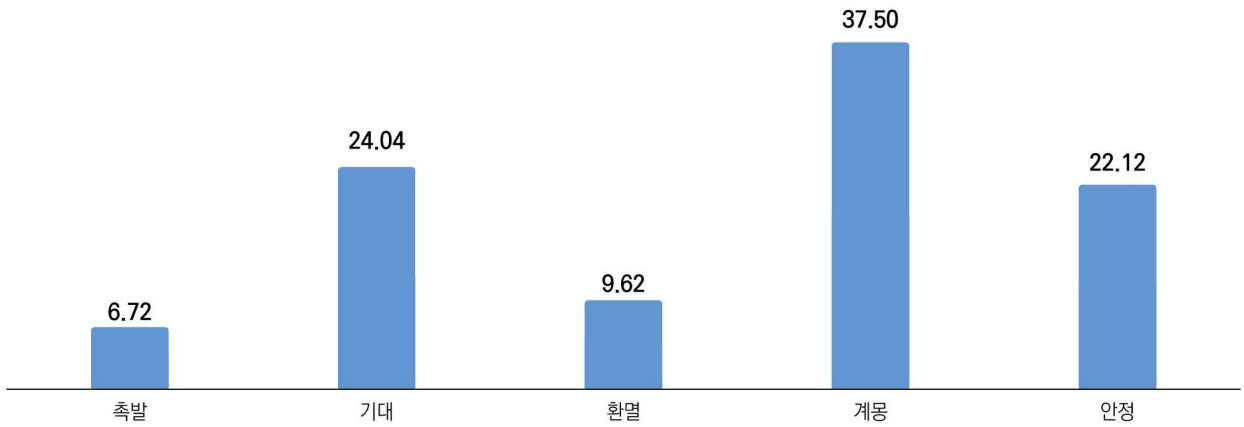


○ 진단·평가

진단·평가 분야 직무의 산업 내 성숙도는 촉발 6.72%, 기대 24.04%, 환멸 9.62%, 계몽 37.50%, 안정 22.12%로 나타났다.

그림 Ⅳ-9 | 진단·평가 분야 산업 내 성숙도

단위 : %

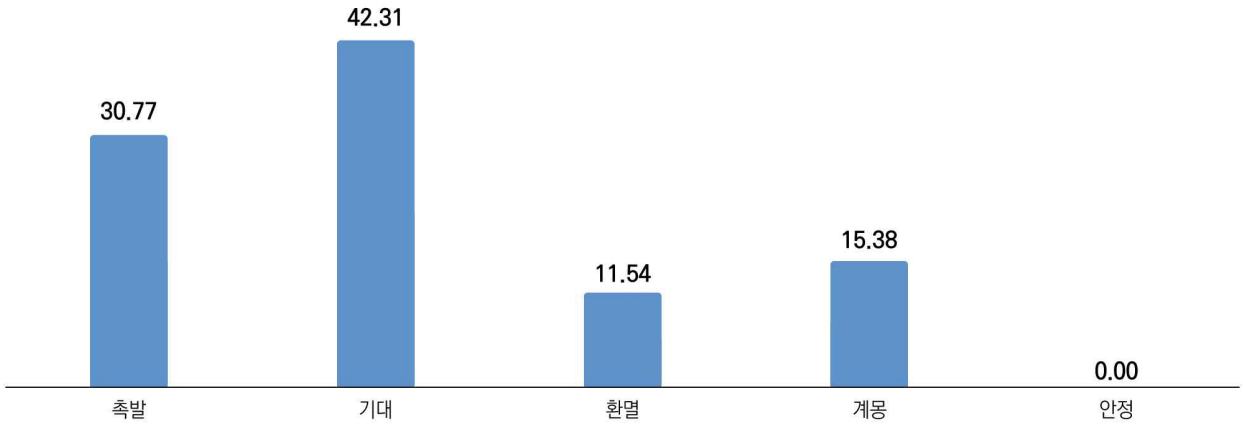


신기술보안

신기술보안 분야 직무의 산업 내 성숙도는 촉발 30.77%, 기대 42.31%, 환멸 11.54%, 계몽 15.38%, 안정 0.00%로 나타났다.

그림 Ⅳ-10 | 신기술보안 분야 산업 내 성숙도

단위 : %

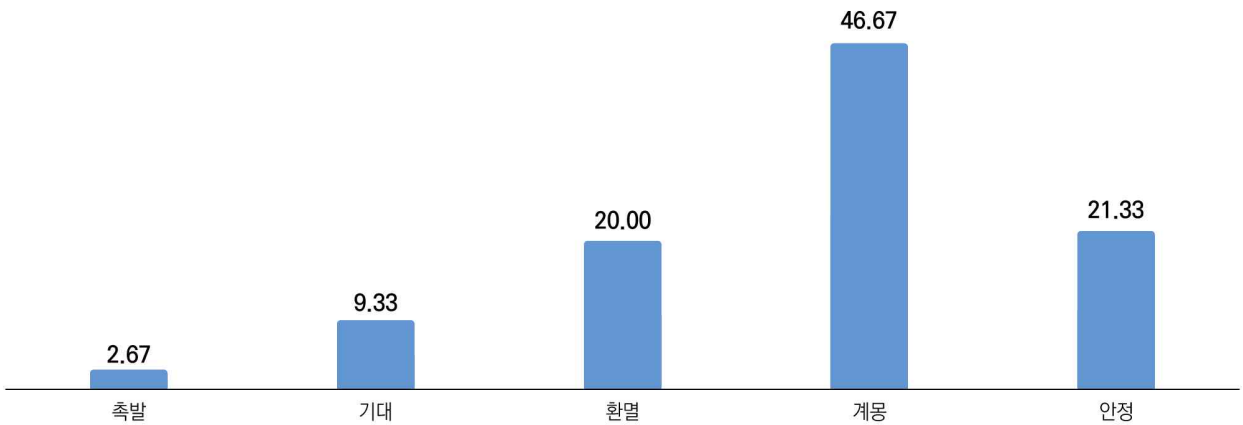


기타

기타 분야 직무의 산업 내 성숙도는 촉발 2.67%, 기대 9.33%, 환멸 20.00%, 계몽 46.67%, 안정 21.33%로 나타났다.

그림 Ⅳ-11 | 기타 분야 산업 내 성숙도

단위 : %

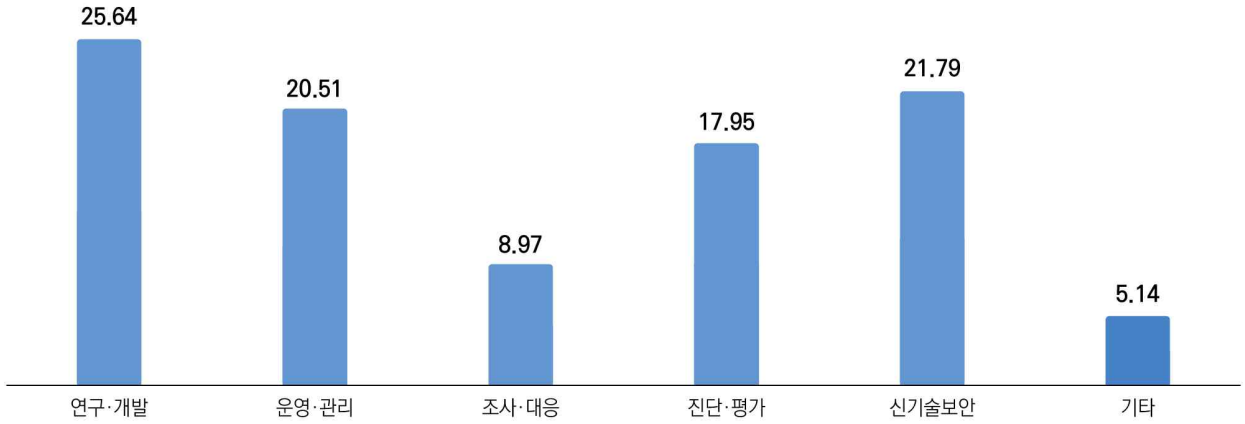


영향력

정보보호산업 성장에 전반적으로 많은 영향력을 미치는 직무를 살펴보면, 연구·개발 25.64%, 운영·관리 20.51%, 조사·대응 8.97%, 진단·평가 17.95%, 신기술보안 21.79%, 기타 5.14%로 나타났다.

그림 Ⅳ-12 | 정보보호산업 성장에 영향을 미치는 직무(1+2+3순위)

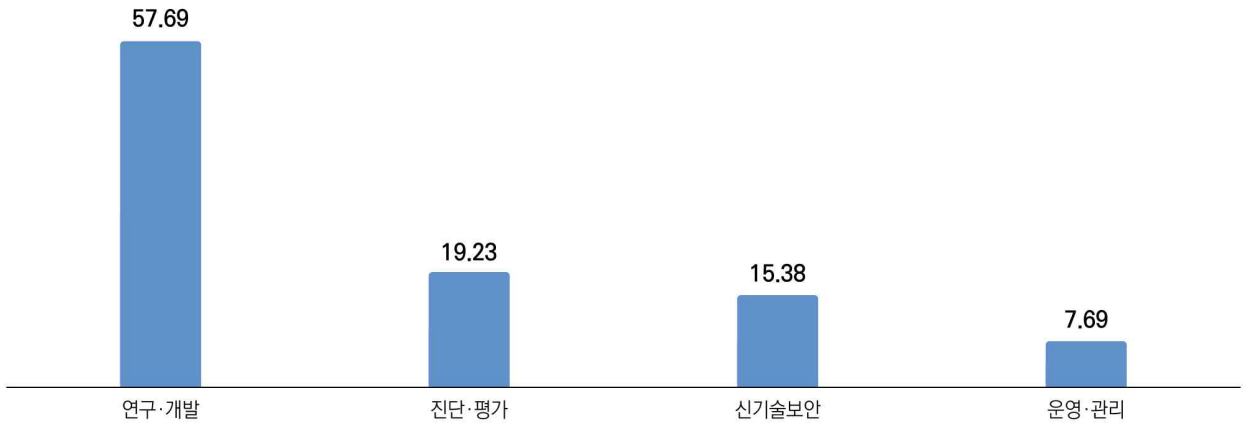
단위 : %



이 중 가장 큰 영향력을 미치는 직무 1순위는 연구·개발 57.69%, 진단·평가 19.23%, 신기술보안 15.38%, 운영·관리 7.69%로 조사되었다.

그림 Ⅳ-13 | 정보보호산업 성장에 영향을 미치는 직무(1순위)

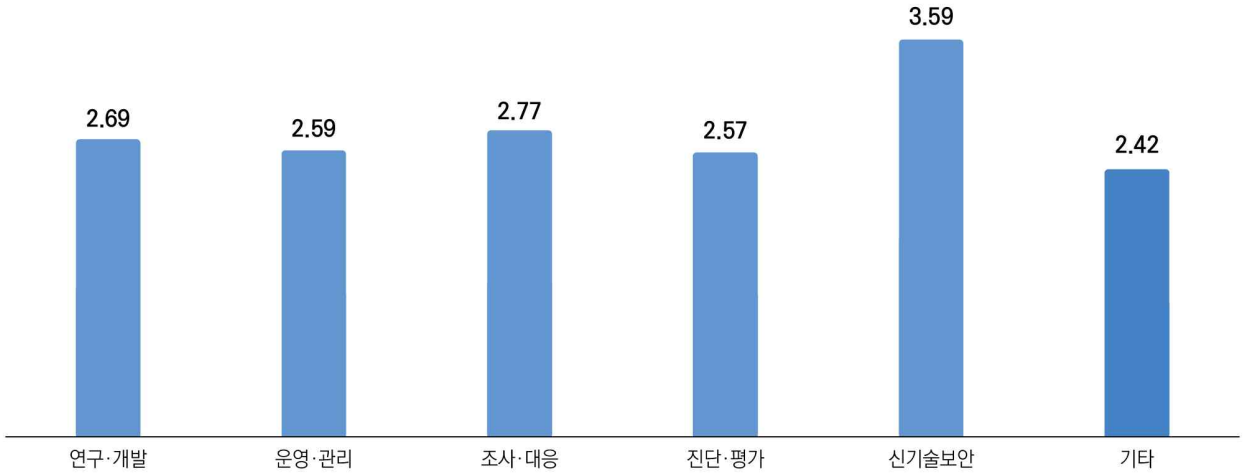
단위 : %



직무변화

지난 3년간 직무별 변화도의 평균을 살펴보면, 연구·개발 2.69, 운영·관리 2.59, 조사·대응 2.77, 진단·평가 2.57, 신기술보안 3.59, 기타 2.42로 나타났다.

그림 Ⅳ-14 | 정보보호산업 직무변화도 평균



직무변화 정도 응답 중 '많이 변화함' 비율이 가장 높은 분야는 신기술보안(60.26%), 연구·개발(30.77%), 조사·대응(26.92%), 진단·평가(22.12%), 운영·관리(20.19%), 기타(19.23%) 순으로 나타났다.

순위	구 분	직 무				응답률(%)
1	신기술보안	클라우드보안관리운영	모빌리티보안	OT보안		60.26
2	연구·개발	정보보호기획	정보보호개발			30.77
3	조사·대응	보안사고대응	보안관제	디지털포렌식		26.92
4	진단·평가	정보보호컨설팅	보안감사	보안감리	보안인증평가	22.12
5	운영·관리	정보보호운영/관리	정보보호엔지니어링	보안품질관리	영상정보보안	20.19
6	기타	기술영업	마케팅/홍보	정보보호교육		19.23

* 많이 변화함 : 5점 척도 기준 (1 : 전혀 달라지지 않음 ~ 5 : 완전히 달라짐) 4 ~ 5 응답

○ 연구·개발

연구·개발 분야의 직무변화 정도는 변화없음 17.31%, 변화함 51.92%, 많이 변화함 30.77%로 나타났다.

그림 Ⅳ-15 | 연구·개발 분야 직무변화 정도

단위 : %

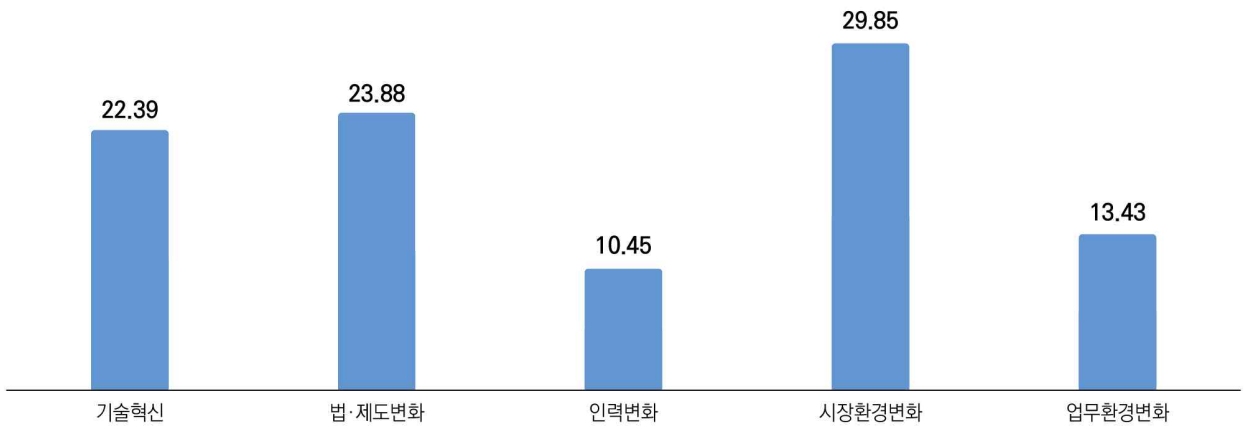
* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

연구·개발 분야 직무의 주요 변화요인은 기술혁신 22.39%, 법·제도변화 23.88%, 인력변화 10.45%, 시장환경변화 29.85%, 업무환경변화 13.43%로 나타났다.

* 기타 요인으로는 AI를 활용한 보안솔루션 개발 등의 의견이 있다.

그림 Ⅳ-16 | 연구·개발 분야 변화요인(복수 응답)

단위 : %



운영·관리

운영·관리 분야의 직무변화 정도는 변화없음 20.19%, 변화함 59.62%, 많이 변화함 20.19%로 나타났다.

그림 Ⅳ-17 | 운영·관리 분야 직무변화 정도

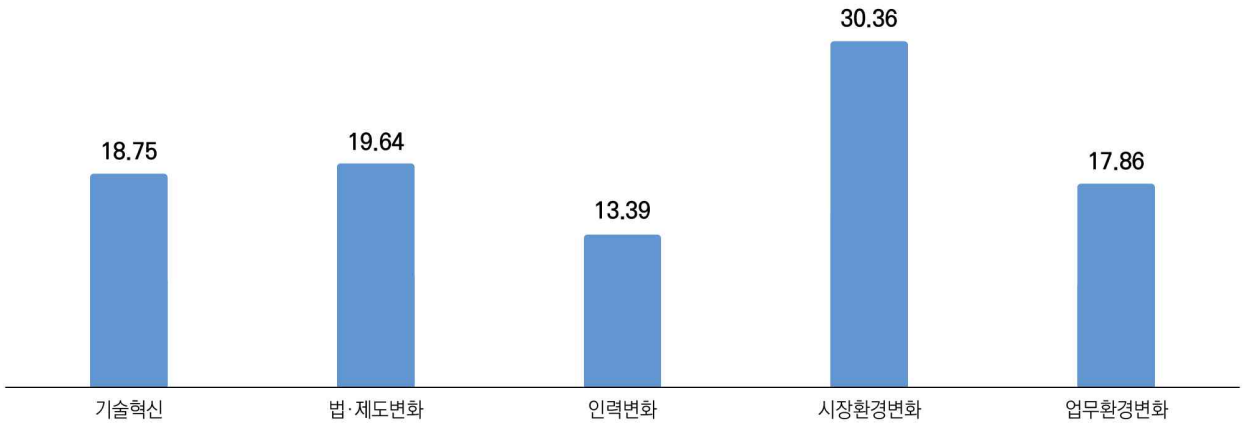
단위 : %

* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

운영·관리 분야 직무의 주요 변화요인은 기술혁신 18.75%, 법·제도변화 19.64%, 인력변화 13.39%, 시장환경변화 30.36%, 업무환경변화 17.86%로 나타났다.

그림 Ⅳ-18 | 운영·관리 분야 변화요인(복수 응답)

단위 : %



○ 조사·대응

조사·대응 분야의 직무변화 정도는 변화없음 12.82%, 변화함 60.26%, 많이 변화함 26.92%로 나타났다.

그림 Ⅳ-19 | 조사·대응 분야 직무변화 정도

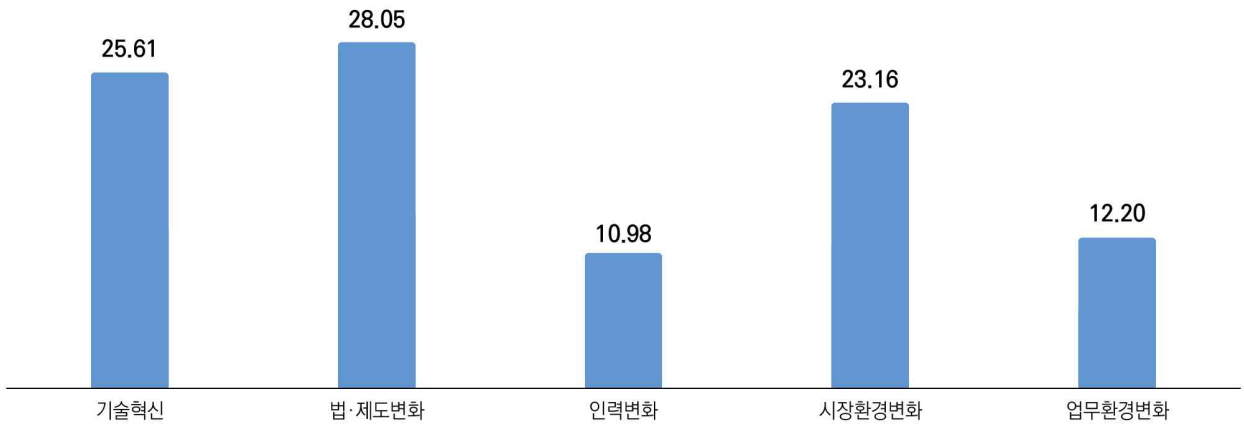
단위 : %

* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

조사·대응 분야 직무의 주요 변화요인은 기술혁신 25.61%, 법·제도변화 28.05%, 인력변화 10.98%, 시장환경변화 23.16%, 업무환경변화 12.20%로 나타났다.

그림 Ⅳ-20 | 조사·대응 분야 변화요인(복수 응답)

단위 : %



진단·평가

진단·평가 분야의 직무변화 정도는 변화없음 15.38%, 변화함 62.50%, 많이 변화함 22.12%로 나타났다.

그림 Ⅳ-21 | 진단·평가 분야 직무변화 정도

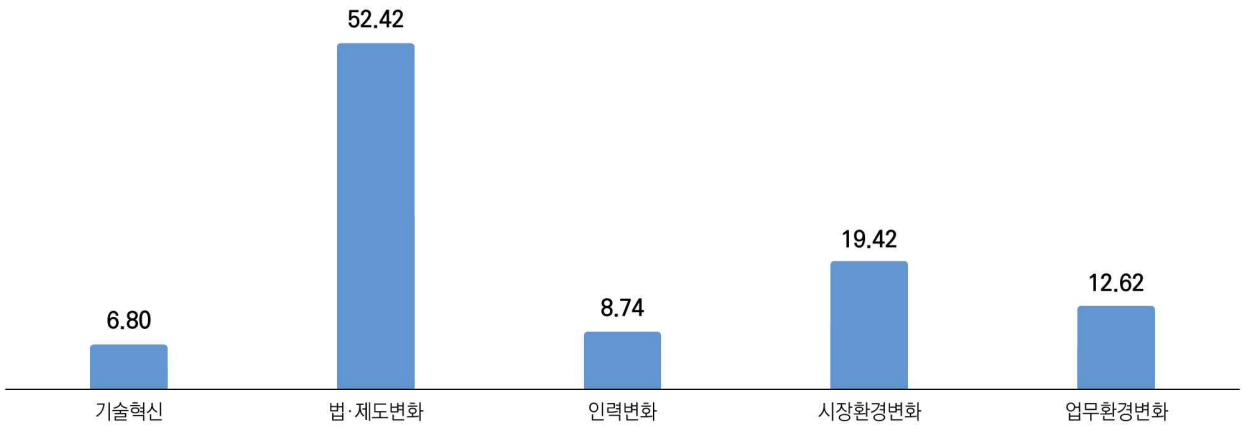
단위 : %

* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

진단·평가 분야 직무의 주요 변화요인은 기술혁신 6.80%, 법·제도변화 52.42%, 인력변화 8.74%, 시장환경변화 19.42%, 업무환경변화 12.62%로 나타났다.

그림 Ⅳ-22 | 진단·평가 분야 변화요인(복수 응답)

단위 : %

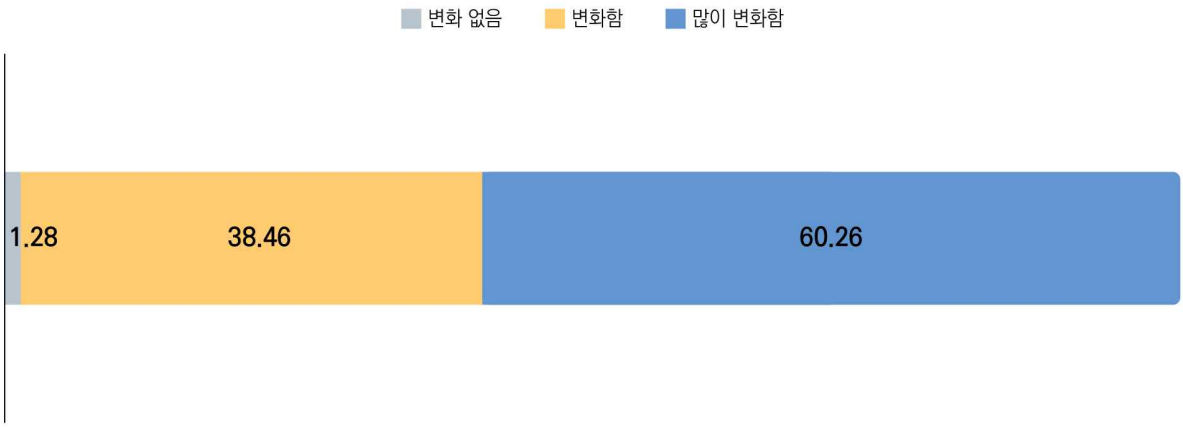


○ 신기술보안

신기술보안 분야의 직무변화 정도는 변화없음 1.28%, 변화함 38.46%, 많이 변화함 60.26%로 나타났다.

그림 Ⅳ-23 | 신기술보안 분야 직무변화 정도

단위 : %



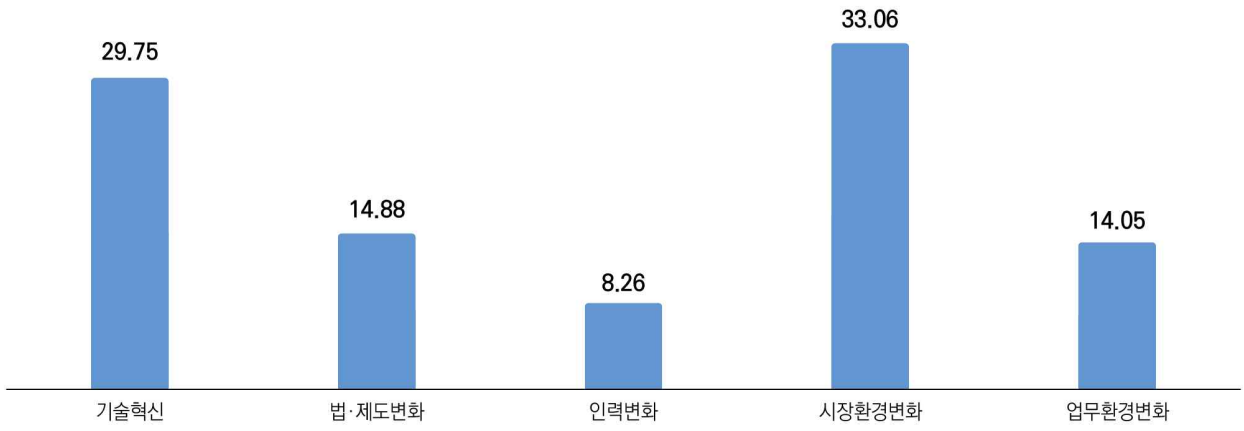
* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

신기술보안 분야 직무의 주요 변화요인은 기술혁신 29.75%, 법·제도변화 14.88%, 인력변화 8.26%, 시장환경변화 33.06%, 업무환경변화 14.05%로 나타났다.

* 기타 요인으로는 내부 데이터 중요도에 따른 관리 방침 변화 등의 의견이 있다.

그림 Ⅳ-24 | 신기술보안 분야 변화요인(복수 응답)

단위 : %

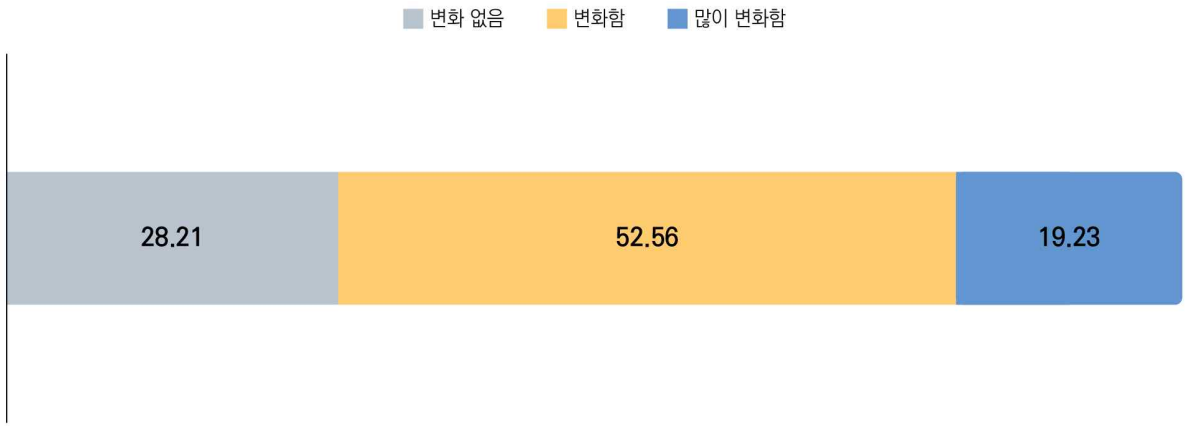


○ 기타

기타 분야의 직무변화 정도는 변화없음 28.21%, 변화함 52.56%, 많이 변화함 19.23%로 나타나, 타 직무 대비 변화정도가 가장 낮은 것으로 조사되었다.

그림 Ⅳ-25 | 기타 분야 직무변화 정도

단위 : %

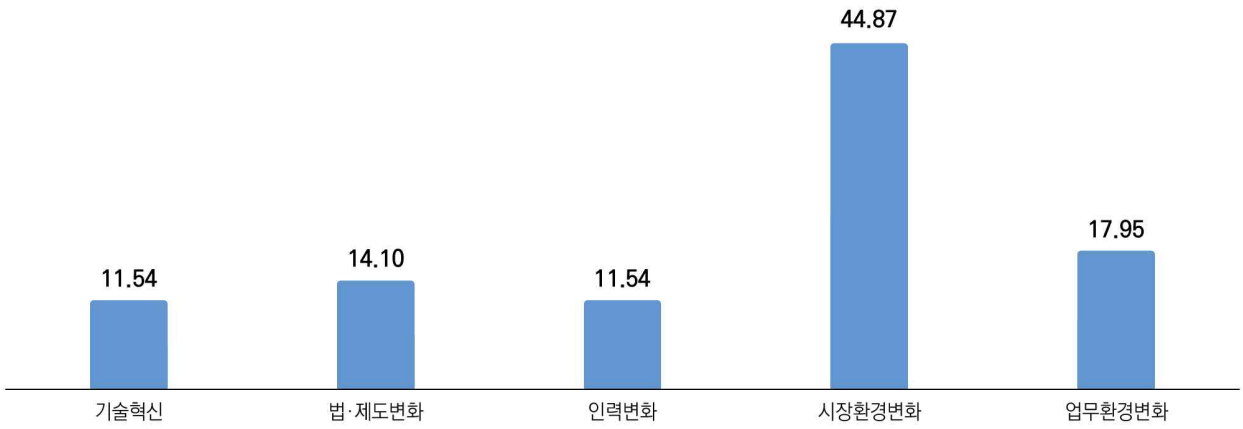


* 5점 척도 기준으로 응답 (1 : 변화 없음 / 2 ~ 3 : 변화함 / 4 ~ 5 : 많이 변화함)

기타 분야 직무의 주요 변화요인은 기술혁신 11.54%, 법·제도변화 14.10%, 인력변화 11.54%, 시장환경변화 44.87%, 업무환경변화 17.95%로 나타났다.

그림 Ⅳ-26 | 기타 분야 변화요인(복수 응답)

단위 : %



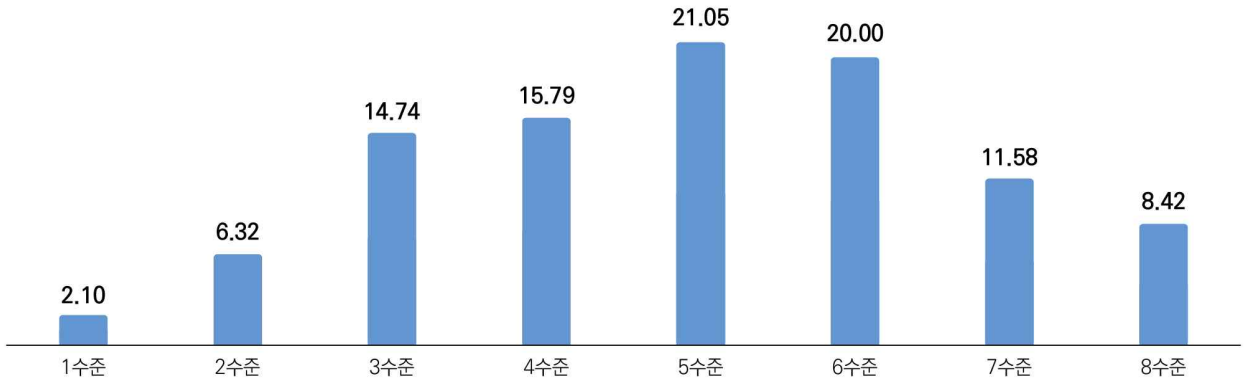
인력수준

○ 연구·개발

연구·개발 분야 직무의 인력수준은 1수준 2.10%, 2수준 6.32%, 3수준 14.74%, 4수준 15.79%, 5수준 21.05%, 6수준 20.00%, 7수준 11.58%, 8수준 8.42%로 분포된 것으로 나타났다.

그림 Ⅳ-27 | 연구·개발 분야 인력수준

단위 : %

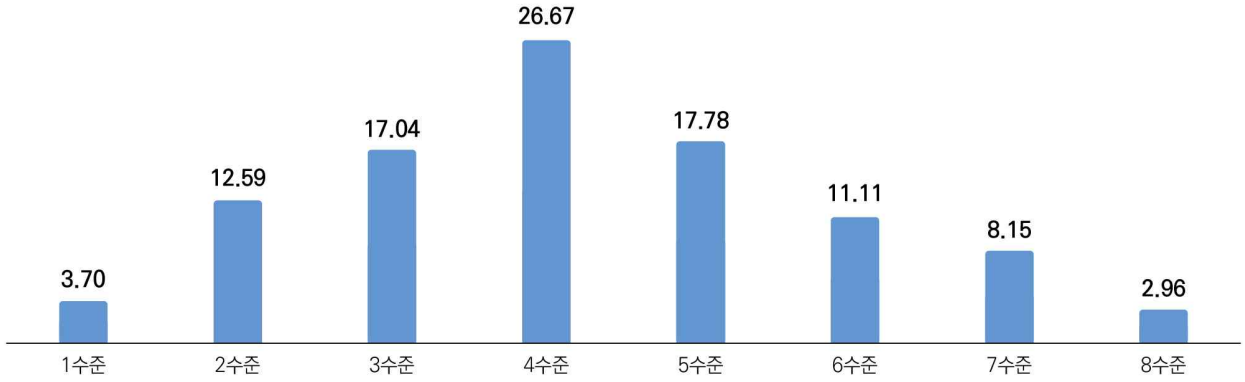


○ 운영·관리

운영·관리 분야 직무의 인력수준은 1수준 3.70%, 2수준 12.59%, 3수준 17.04%, 4수준 26.67%, 5수준 17.78%, 6수준 11.11%, 7수준 8.15%, 8수준 2.96%로 분포된 것으로 나타났다.

그림 Ⅳ-28 | 운영·관리 분야 인력수준

단위 : %

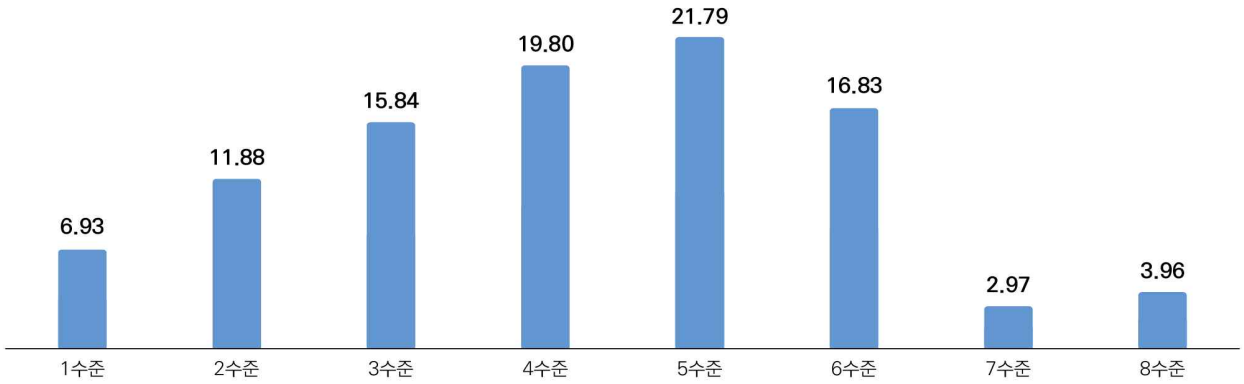


조사·대응

조사·대응 분야 직무의 인력수준은 1수준 6.93%, 2수준 11.88%, 3수준 15.84%, 4수준 19.80%, 5수준 21.79%, 6수준 16.83%, 7수준 2.97%, 8수준 3.96%로 분포된 것으로 나타났다.

그림 Ⅳ-29 | 조사·대응 분야 인력수준

단위 : %

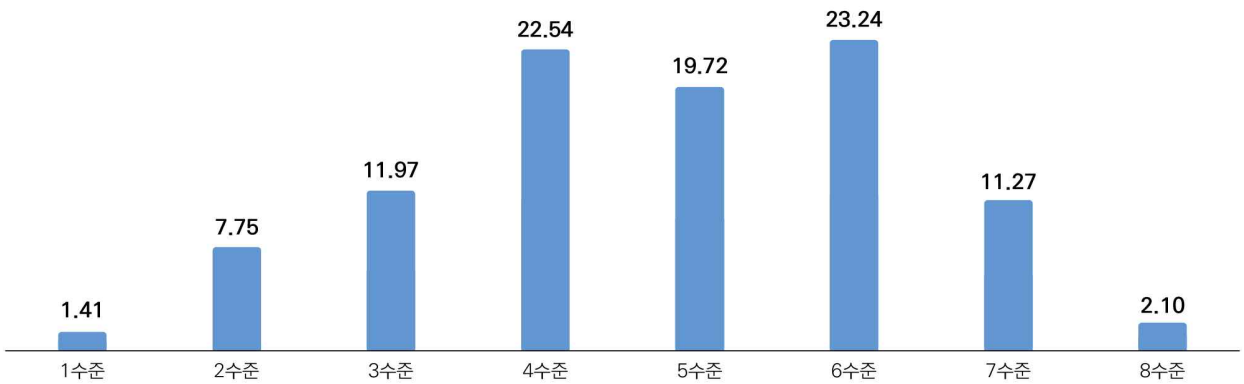


진단·평가

진단·평가 분야 직무의 인력수준은 1수준 1.41%, 2수준 7.75%, 3수준 11.97%, 4수준 22.54%, 5수준 19.72%, 6수준 23.24%, 7수준 11.27%, 8수준 2.10%로 분포된 것으로 나타났다.

그림 Ⅳ-30 | 진단·평가 분야 인력수준

단위 : %

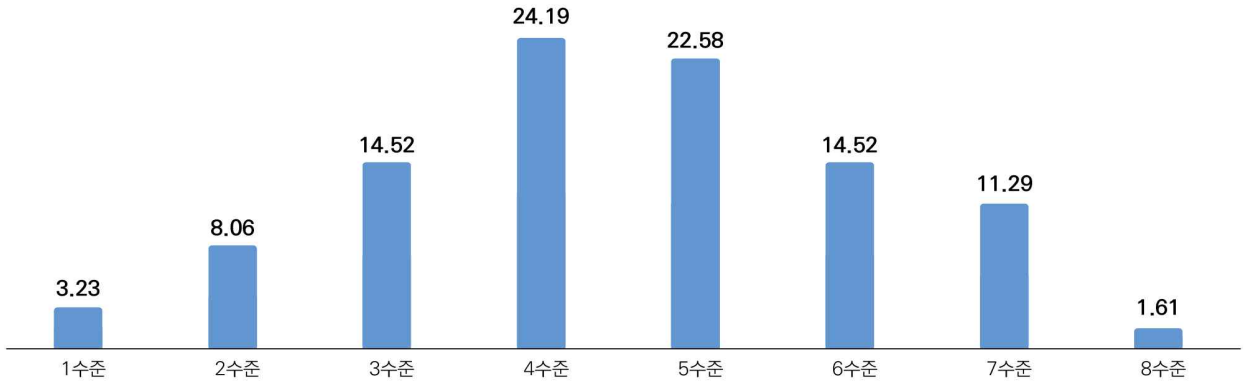


○ 신기술보안

신기술보안 분야 직무의 인력수준은 1수준 3.23%, 2수준 8.06%, 3수준 14.52%, 4수준 24.19%, 5수준 22.58%, 6수준 14.52%, 7수준 11.29%, 8수준 1.61%로 분포된 것으로 나타났다.

그림 Ⅳ-31 | 신기술보안 분야 인력수준

단위 : %

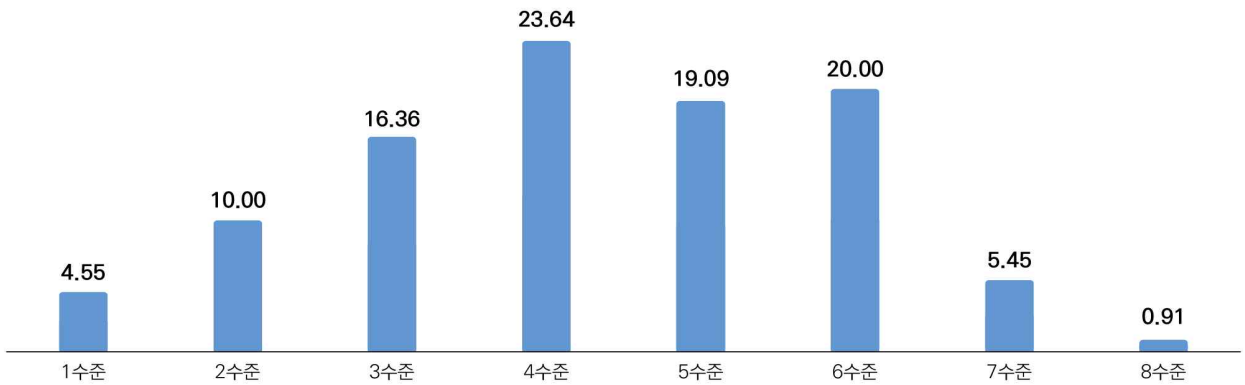


○ 기타

기타 분야 직무의 인력수준은 1수준 4.55%, 2수준 10.00%, 3수준 16.36%, 4수준 23.64%, 5수준 19.09%, 6수준 20.00%, 7수준 5.45%, 8수준 0.91%로 분포된 것으로 나타났다.

그림 Ⅳ-32 | 기타 분야 인력수준

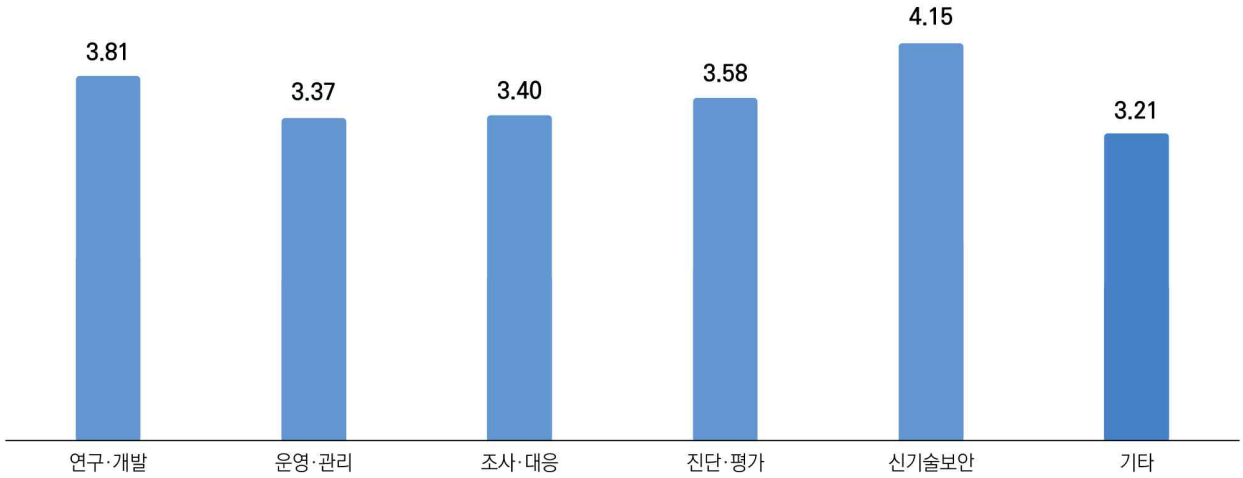
단위 : %



직무전망

향후 3년 이내 직무별 유망도의 평균을 살펴보면, 연구·개발 3.81, 운영·관리 3.37, 조사·대응 3.40, 진단·평가 3.58, 신기술보안 4.15, 기타 3.21로 나타났다.

그림 Ⅳ-33 | 정보보호산업 직무유망도 평균



순 위	구 분	직 무				유망도(평균)
1	신기술보안	클라우드보안관리운영	모빌리티보안	OT보안		4.15
2	연구·개발	정보보호기획	정보보호개발			3.81
3	진단·평가	정보보호컨설팅	보안감사	보안감리	보안인증평가	3.58
4	조사·대응	보안사고대응	보안관제	디지털포렌식		3.40
5	운영·관리	정보보호운영/관리	정보보호엔지니어링	보안품질관리	영상정보보안	3.37
6	기타	기술영업	마케팅/홍보	정보보호교육		3.21

* 5점 척도 기준 (1 : 매우 비유망 ~ 5 : 매우 유망)

또한, 다양한 직무변화에 따라 현재 구분된 직무 외에 새롭게 생겨난 직무(신생직무)나 사라진 직무(소멸직무), 통합·분할 등 대체되고 있는 직무(대체직무)를 등 기존의 직무구분을 다음과 같이 전망하였다.

변화양상	직 무	
신생직무	빅데이터	· 빅데이터 관리 보안
	인공지능(AI)	· AI 보안 전문가 (AI 관리 보안, AI 데이터 보안 분석 등)
	자동화	· 보안 업무 자동화 대응 및 운영
	기타	· 위협 인텔리전스 수집/분석 및 대응
소멸직무	시스템 및 네트워크	· 단순 시스템 관리자
		· 일반적인 네트워크 및 서버 관리자
	취약점 진단	· 자동화 솔루션 개발로 인한 기술적 취약점 진단 업무
대체직무	대체	· 종이문서 출력보안이 디지털 전자문서보안으로 대체
	통합	· 보안 컨설턴트와 보안 엔지니어의 통합
기타	분리 및 세분화	· 모의해킹(정보보호컨설팅과 분리) · 악성코드 분석(정보보호엔지니어링과 분리) · 정보보호운영/관리 직무 세분화 - 네트워크 정보보호 운영/관리 - 엔드포인트 정보보호 운영/관리 - 법/관리적(법/규제/효율성 등) 정보보호 운영/관리 등

기타의견

이외에도 설문조사를 진행하면서 정보보호 분야 직무 및 변화양상, 모니터링 사업에 대한 의견 등 정보보호산업과 직무 전반에 대한 전문가들의 다양한 생각을 확인할 수 있었다.

직무변화에 대한 의견

연번	내 용
1	· 정보보호 직무 변화의 요인 및 양상은 크게 법적 규제의 변화와 IT기업의 환경변화가 가장 큰 요인이며, MZ세대들의 보안에 대한 인식 및 이해가 중요한 직무 변화의 요인이라고 생각함
2	· 기업에 따라 명명되지 않은 직무가 잔존하고 있으나, 큰 틀에서는 변화가 없을 것 같음
3	· 정보보호 분야의 직무구분 변화와 관련하여 특별히 새로운 직무가 발생할 수도 있으리라 생각하며, 모든 직무에 정보보호 분야의 업무가 포함되어(녹아 들어가 있는 상태) 수행하게 될 것이라고 생각함
4	· NCS의 정보보호 직무가 다양한 IT 신기술/환경의 등장으로 현재 정의된 직무에 시장 또는 환경 변화를 잘 반영하고 있는지 정의, 능력, 수행역할 등에 대한 지속적인 검토와 확인이 필요해 보임
5	· AI가 활성화 되면, 보안관제 부분의 인력이 많이 효율화 되어 필요인력이 감소될 것으로 판단됨
6	· CISO의 의무와 책임이 강화됨 · 더 많은 업종에서 정보보안사고 이슈가 부각됨에 따라 더 많은 인력수요를 필요로 하게 됨 · 인공지능, 자동화 등에 기인한 더 많은 윤리적 이슈와 각종 사건사고 등에 대한 대응능력이 필요함
7	· 현재 정보보호 직무는 사이버위협대응, 보안관제, 보안컨설팅 등으로 정확히 업무가 분류되기보다는 다양한 위협에 대응하기 위하여 통합되고 있음 · 이에 따라 전문성에 더하여 다양한 직무를 처리할 수 있는 능력이 필요로 하고 있음
8	· 빠르게 변화하고 있는 정보보호 환경과 산업 환경에 따라, 명확한 직무 구분에 따른 업무만 수행하기는 어려운 상황이 되고 있음 · 기술 인력이 정보보호 컨설팅과 함께 기술 영업을 진행할 수도 있고, 마케팅/홍보 인력도 정보보호 교육과 함께 Co-Work 하기도 함
9	· 직무변화의 주요 요인은 규제강화, 산업환경 변화, 사회적 인식 변화라고 생각됨 – 규제강화 : 개인정보보호법 등 관련 법규가 강화되면서 보안 요구사항 강화 – 산업환경 변화 : 디지털전환이 가속화되면서 기업의 정보자산이 증가하고, 이에 대한 보호 필요성 확대 – 사회적 인식 변화 : 사이버공격의 심각성이 증가하면서 정보보호에 대한 사회적 인식 증대 – 지속적인 학습 : 새로운 기술을 학습하는 것이 필요함

○ 정보보호산업 변화에 대한 의견

연번	내 용
1	· 연구원, 컨설턴트의 경우 우수한 인원의 해외 진출 등으로 국가적 인력손실이 발생하고 있어, 시장 상황에 부합하는 가치평가와 대가산정 등의 대응이 필요할 것임
2	· 시시각각 변하는 법/제도적 변화 및 기술혁신 등에 정보보안업계는 항상 대응체계를 마련하고, 길라잡이의 역할을 해야 할 것으로 보임
3	· 정보기술의 발달에 따라 정보보호의 수준 및 기술적 난이도가 점점 높아져가고 있음 · 양자암호를 비롯하여 향후에도 새로운 신기술의 등장으로 인해 정보보호의 높은 수준을 지속적으로 요구하게 될 뿐만 아니라 정보전달 체계 및 디바이스의 발달과 생체 정보이용 등 관리해야 할 정보의 범위 증가로 더욱 복잡하고 정교한 정보보호 요구가 발생할 것으로 예상됨

○ 기타 직무변화 모니터링 사업 전반에 대한 의견

연번	내 용
1	· 금번 직무변화 모니터링의 직무 구분 및 정의, 직무변화 요인, 직무변화 양상의 데이터가 좋은 초석이 되어 정보보안 업계의 인력 발굴 및 양성에 좋은 보탬이 되었으면 하는 바람임
2	· 해당 직무 조사가 변화하는 사항을 지속적으로 반영할 수 있었으면 좋겠음

2. 심층 인터뷰

전문가 FGI

설문조사를 기반으로 직무변화가 큰 두 개 직무를 선정하여 전문가 FGI를 실시하였다. FGI는 해당 직무를 영위하는 기업의 규모 및 재직인원을 고려하여 대상 기업을 선정하였으며, 두 개 직무의 세부적인 특징과 변화를 도출하였다.

○ 연구·개발 (정보보호개발 직무)

① 필요 역량 및 변화

1) 개발 관련 기본 지식

보안 제품 개발을 위한 운영 시스템(OS)과 시스템 네트워크 관련 지식은 필수이며 C, C++, Java, JavaScript, Python, TypeScript 등 기초적인 프로그래밍 언어 능력이 요구된다.

보안기술을 적용하기 위해 대칭키, 공개키 기반구조(PKI), 알고리즘을 활용하는 방법 등 암호학 관련 기초지식도 필요하다. 또한, 이러한 지식을 활용하여 제품 개발에 필요한 요구사항을 제시하기 위한 PoC[8]를 코드로 생성하는 능력도 요구된다.

실제 일부 기업에서는 이러한 과정에 대해 개발 역량 및 연차에 따라 조직을 나누어 운영하기도 한다.

구 분	업무내용
기반기술	상세 프로토콜이나 문서 해석을 통해 사전 준비를 위한 기본적인 파일럿 코딩 수행
설계	아키텍처 전반에 대한 프로세스나 시퀀스 제작, 보통 고연차의 재직자가 많음
일반개발	실제 제품 개발, 보통 저연차의 재직자가 많음

2) 설계문서 작성 능력

정보보호개발 담당자는 제품 개발 과정에서 이해관계자들이 보안 준수사항을 고려하여 제품을 개발할 수 있도록 보안 관련 내용을 포함한 설계과정을 소프트웨어 공학적으로 문서화하여 담당자에게 공유하는 능력이 필요하다.

8) PoC(Proof of Concept) : 기존 시장에 없던 기술을 도입하기 전, 이를 검증하기 위해 사용하는 것을 의미함

이를 통해, 이해관계자들과 소통하거나 업무 분업 및 협업, 인수인계가 쉽게 이루어지며, 개발 관련 아웃소싱을 진행하는 과정에서도 설계문서가 매우 중요하게 활용된다.

따라서 정보보호개발 담당자를 대상으로 일반 개발 뿐 아니라 여러 솔루션에 대한 설계문서 작성, 평가, 검증 등 설계과정에 대한 교육훈련이 필요하다.

3) 표준 및 인증 해석 능력

개발 과정에서 작성하는 모든 문서에는 ISO/IEC 등 준수해야 하는 표준 및 인증이 존재하나, 다수의 제품 개발자는 이러한 표준 및 인증 문서를 해석하는 데에 어려움을 겪고 있다.

과거에 비해 현재에는 글로벌 경쟁을 위한 컴플라이언스나 UN에서 제시하는 규제가 굉장히 중요해졌다. 이에 따라, 앞으로는 규제가 더 획일화되고 강화될 것으로 예상되어 개발 능력 외에도 표준에 대한 이해 및 적용 능력이 요구될 것이다.

또한, OT보안, 스마트카 보안 등 특정 산업군에서 보안기술의 필요성이 대두되면서, 일반적인 보안 관련 인증서와 다른 특정 산업군에서 사용하는 인증서의 표준을 준수하는 것도 중요하다. 최근에는 정부에서 강조하는 ESG 인증 등 보안 트렌드에 따른 인증 및 표준을 확인하여 준수하는 능력도 요구된다.

따라서 국제 및 국내 표준 문서의 구조나 해석법, 적용 가능한 표준을 선택하는 방법, 최소한 이러한 표준 문서를 검색할 수 있는 프로세스를 정립하는 능력이 필요하다.

이에 따라, 사내에서는 SOP와 같이 SW프로세스 품질인증 제도에서 인증받기 위해 사용했던 내부 자체 표준 문서를 기반으로 하여 설계자들이 서로 소통할 수 있도록 문서를 제작하기도 한다.

4) 문해력 및 커뮤니케이션 능력

정보보호개발 분야와 연구 분야는 서로 협업이 되지 않으면 예상했던 제품이 개발되지 않는 경우가 있어, 두 개로 나뉘어 운영되던 조직이 현재에는 통합되어 운영되는 경우가 많다.

또한, 개발 과정에 표준을 적용하는데 익숙하지 않을 경우 담당자간 보안 표준 준수의 필요성에 대한 인식에 차이가 발생하여 의견충돌이 일어나는 경우가 많다. 따라서 표준과 인증에 대한 충분한 이해를 통해 개발 과정에서의 이해관계자들에게 설명하고 설득할 수 있는 이해 및 소통 능력이 중요하다.

5) 클라우드 기반 서비스로의 전환

국가 및 공공기관에서는 SaaS, IaaS 등 클라우드 기반의 제품을 우선 도입하는 추세로, 정부에서는 현재 클라우드 컨설팅 지원 사업을 수행하고 있으며 내년에는 더 확대되어 운영될 예정이다. 따라서 온프레미스 환경에 구축된 조직의 데이터 및 IT 인프라를 클라우드 서비스에 맞추어 전환하거나 설계하는 작업 능력이 요구된다.

6) AI 활용한 업무 수행

초기에는 사내에서 AI의 활용을 금지시켰지만, 이제는 금지시킬 수 없을 만큼 개발 과정에 AI를 활용하는 임직원이 늘어나고 AI의 영역이 확대되었다. AI를 통해 업무절차가 간소화, 빠른 시간 내에 많은 정보 수집, 담당자간 업무 및 지식 격차 완화 등의 장점이 존재하나 업무 기밀 유출, 잘못된 정보 활용 등 단점도 존재한다.

이에 따라, AI 활용 관련 사내 규정이 존재하며, 회사에서는 학습데이터를 제공하지 않는 AI 유료서비스를 제공하고 있다. 또한, 정보 검색 및 필터링 방법 등 AI 활용 방법을 교육하는 것이 중요해졌다. 특히 데이터 학습방법과 학습데이터에 맞는 파라미터 설정 방법 등을 알아야 한다.

7) 보안통합 및 오케스트레이션

국내에서는 기술유출을 고려하여 기업 간 제품 연동을 공유하지 않는 경향이 있었으나, 해외에서는 솔루션을 표준화하여 제품 연동 및 통합을 통해 범용적인 데이터를 활용하고 위협에 공통적으로 대응하고 있다.

최근에는 국내에서도 글로벌 시장의 진출을 위해 프로토콜과 표준을 준수하고 있다. 해외 업체의 제품에 맞춰 상호운영 하는 API를 만들어 연동시키는 작업을 수행하고 있는 추세이다.

② 직무 수준 및 변화

1) 채용수준

개발 분야는 대학 재학생, 특성화고 졸업생 등 대졸 이하의 학력에서도 뛰어난 인재가 많이 존재하므로 채용 시 학력에 제한을 두지는 않고 있다.

하지만 다양한 프로젝트 및 사회 경험을 기반으로 업무에 책임감을 가지고 임하는 태도를 중요시 여기며, 대학과정에서 전통적인 보안 지식, 운영체제, 관리 시스템, 네트워크 등 기초 지식에 대한 학습이 가능하므로 컴퓨터공학 및 유관 전공의 대학졸업자를 선호하는 경향은 있다.

이러한 정보보호개발 직무의 변화와 필요역량을 정리하면 다음과 같다.

정보보호개발 직무변화(정리)

구 분	과 거	현 재
주요 경력 분포 수준	· 3~4수준 · 5년차 이하의 초, 중급 수준 · 초급 보안인력의 양성 및 기존 재직자 직무 능력 개선으로 보안인력 시장수요에 대응 · 전산 전공 선호 · 매년 신입 채용 · 관련 전공을 졸업한 신입사원 또는 2~3년차 채용 후 인력 양성	· 4~6수준 · 5년차 이상의 전문 인력이 많아짐 · 보안인력의 꾸준한 유입 및 경력자 증가로 높은 수준의 과업 수행자 증가 · 대학 전공 뿐 아니라, 전문 교육 프로그램이 많아짐 · 주요 업무를 바로 수행할 수 있는, 높은 기술 수준 및 경험을 가진 시니어급 선호
직무변화 선행요인	· 주로 Windows 대상 · PC 등 단말 위주의 공격 · DevOps 문화 확산 · 블록체인 활용 · 보안위협 트랜드 변화 – 사이버 위협 인텔리전스의 확대 – 제로데이공격의 확대 – IoT 보안 공격 확대 – 가상화폐 거래소 해킹 공격 증가	· OS 등 환경의 변화(리눅스, iOS 등) · 단말기의 변화 (PC → 모바일, 태블릿) · 종이증명서에서 전자증명서로의 변화 · 공급망 보안 이슈 등장 · 클라우드 확산 · AI 활용 개발 · 제로트러스트

구 분	과 거	현 재
직무변화	· 클라우드 보안 서비스의 활성화 시동 · 네트워크 보안 취약점 점검 · 개별 IoT 기기 보안 대책 · 개인정보 유출방지를 위한 규정 강화 · 블록체인 보안 · 서버 기반의 서비스형 개발	· 클라우드 서비스로의 전환 (국내외 CSP 활용) · AI를 활용한 업무 수행 · 보안통합 및 오케스트레이션 · 제로트러스트 보안에 대한 요구 증대 · 자동차 등 산업, OT, CPS 보안 업무 수행 · 로봇, 드론 등 무인 이동체에 대한 보안 분야 신규 등장 · 전자증명서 보안 · IoT, Mobile 등 Attack Surface 확장으로 다양한 프로토콜과 플랫폼 고려
필요역량	· 기본 암호기술 · 시스템 및 네트워크 기본 지식 · 해킹 대응 및 분석 능력	· 기본적인 컴퓨터 공학 · 클라우드 네이티브 개발 능력 · 설계문서 작성 능력 · 표준 및 인증 해석 능력 · 문해력 및 커뮤니케이션 능력 · 신기술에 대한 이해
주요 사용 도구	· 형상관리: SVN, Git(Github, Gitlab 등) · 개발도구: Visual Studio. Eclipse · 협업도구: Jira, Slack · 개발언어: C/C++, Java · VM을 주로 활용 · 보안 취약점 점검 도구 · 역공학 도구 · PKI 기반의 암호/인증 모듈	· 형상관리: Git(Github, Gitlab 등) · 개발도구: VSCode · 협업도구: Teams, Jira, Slack, Confluence · 개발언어: Python. TypeScript · 개발, 테스트환경: Docker를 주로 활용 · 오픈소스 소프트웨어 · SBoM 기반 공급망 보안 점검 도구 · 도커, 쿠버네티스 등 클라우드 점검 도구 · 경량 타원곡선암호, 양자내성암호 모듈 · Visual Studio Code를 통한 개발 (golang, rust 등) · SaaS 기반 개발 도구의 활용

○ 신기술보안 (클라우드보안관리운영 직무)

① 필요 역량 및 변화

1) 자동화 및 코딩 능력

로그 관리는 시스템 사용 이력, 권한 신청, 구성 변경 등의 정보를 포함하는데, 보안 업무에서는 규제 감사나 보안사고 대응을 위해서 로그 관리 능력이 매우 중요하고 데이터 기록 및 분석 작업이 필수적이다.

클라우드는 처리해야 할 로그의 양이 온프레미스에 비해 훨씬 많으므로 방대한 양의 로그 관리를 수동으로 처리하는 것은 불가능하여, 자동화 환경을 구성하는 것이 중요하다. 이러한 자동화 과정에서 테라폼(Terraform)과 같은 도구를 사용하며, 기본적인 스크립팅 및 코딩 능력을 갖추어야 한다.

2) 클라우드 네이티브에 대한 이해

가상 머신(Virtual Machine) 환경에서 컨테이너 기반의 쿠버네티스[9] 환경으로 변화하면서, 과거의 보안 운영 및 장비 관리 중심에서 벗어나 클라우드 네이티브 환경에 맞춰 발전하고 있다. 클라우드 네이티브 환경에서는 보안이 더욱 복잡하고, 기존 온프레미스 환경에서의 보안 업무와는 다른 접근 방식이 필요하다.

이로 인해 보안 전문가에게 요구되는 기술적 역량이 확장되어, 기존 보안 업무 뿐 아니라, 클라우드 서비스 아키텍처 설계와 보안 요소를 결합하는 능력도 중요해졌다.

3) 문서화 및 문제해결능력

운영 절차와 중요 정보를 기록하는 것은 필수적이며, 오픈소스나 외부 솔루션 사용으로 인한 문제 추적을 위한 문서 작성이 매우 중요하다.

또한, 클라우드 서비스는 기술 담당자가 현장에서 직접 설치하거나 문제를 해결해주는 것이 아닌 CSP(Cloud Service Provider)가 매뉴얼화한 문서를 통해 서비스의 보안 기능을 이해하고 필요한 조치를 취할 수 있어야 한다. 특히, 이 과정에서 트러블 슈팅 경험 등 클라우드 서비스를 운영하면서 발생할 수 있는 문제를 해결해보는 경험이 요구된다.

9) 쿠버네티스(Kubernetes) : 오픈소스 기반의 운영을 자동화 하기 위해 컨테이너화된 관리시스템으로, 구글에 의해 설계되고 리눅스 재단에 의해 관리되고 있음

4) SLA 및 책임 공유 모델에 대한 이해

클라우드는 대부분 임대형 서비스를 사용하는 만큼 SLA[10]를 정확히 분석하고, 고객과 CSP의 책임 공유 모델에 대한 이해가 필요하다.

5) 다양한 클라우드 서비스 활용 능력

AWS(Amazon Web Service), MS(Microsoft) Azure, GCP(Google Cloud Platform) 등 각 CSP는 보안 도구와 기능을 다르게 제공하므로, 오픈소스나 다양한 실습 환경을 활용하는 방식이 필요하며 다양한 플랫폼에서의 경험이 매우 중요하다. 따라서 CSP의 서비스 운영 방식에 맞는 보안 도구나 정책을 이해하여 적용하고, 클라우드 네이티브 보안을 운영하는 능력이 필요하다.

AWS와 같은 클라우드 서비스 제공 업체들은 보안 관련 서비스에 AI를 내장하여 보안 코드의 취약점을 자동으로 탐지하고 수정 방법을 제시하는 등의 기능을 제공하고 있다. 이로 인해 보안 담당자들은 AI가 제시하는 가이드라인에 따라 더 효율적으로 업무를 수행할 수 있게 되었다.

또한, AI가 단순한 업무를 대체하면서 주니어 인력의 업무 범위가 줄어들었으며, 이로 인해 중급 및 고급 인력의 필요성이 더욱 높아지고 담당 인력들은 더 높은 수준의 기술을 요구받게 되었다.

10) SLA(Service Level Agreement) : 공급업체가 고객에게 제공하기로 약속한 서비스 수준을 명시하는 아웃소싱 및 기술 공급업체 계약으로, 가동·납품·응답·해결 시간 등의 지표가 포함되어 있음

② 직무 수준 및 변화

1) 세분화된 부서 운영

온프레미스와 클라우드 환경에 대한 보안 요구 사항이 다르기 때문에, 일부 기업에서는 클라우드 보안에 맞추어 세분화된 부서가 운영되고 있다.

구 분	특 징
설계 및 아키텍처	· 인프라(IaaS), 파스(PaaS), 사스(SaaS) 각 영역에 따라 설계 부서가 구분됨 · 인프라 서비스 : 서버 가상화, 네트워크 가상화, 스토리지 가상화 등을 다룸 · 네트워크 설계 : 클라우드 네트워크 아키텍처를 설계함 · 보안 설계 : 방화벽, IPS, 관제 시스템 등 보안 요소를 설계함
개발 및 서비스	· 파스(PaaS)와 사스(SaaS) 환경에서는 더 많은 개발 관련 팀이 필요함 · 컨테이너화된 환경에서는 쿠버네티스를 사용하는 팀이 별도로 존재함 · 이를 통해 클라우드 네이티브 애플리케이션을 개발함
운영	· 설계 부서에서 정의된 아키텍처에 따라, 실제 운영을 담당함 · 보안 모니터링 및 네트워크 보안 운영 등을 수행함

2) 수준 및 채용현황

클라우드보안관리운영 직무의 경우, 경력직을 선호하는 경우가 많아 2~5년의 경력의 인력이 많다. 특히, 기존 온프레미스 환경의 보안 담당자에서 클라우드보안관리운영 담당자로 이직하는 인력이 다수이다.

채용 시 학력보다는 경험이 중요하며, 요즘 신입 인력은 클라우드에 특화된 정규교육을 받거나 자격증을 많이 취득하는 등 수준이 상향평준화 되어 신입에 대한 기대치가 매우 높은 상황이다. 특히, 클라우드보안관리운영 직무에서는 아키텍처 설계와 같은 고급 기술에 대한 경험이 있으면 좋은 대우를 받고 있다.

클라우드보안관리운영 직무의 경우, 해당 기술이 최근 5년 사이 대두된 신기술 관련 보안 업무이므로 직무에 대한 과거와 현재의 확실한 변화를 파악하기에는 한계가 있었다.

전문가 인터뷰

추가적으로, 각 분야별 대표 직무에 대해 관련 전문가를 대상으로 심층 인터뷰를 실시하여 현장에서 체감하는 직무변화에 대해 확인하였다.

○ 연구·개발 (정보보호개발 직무)

① 필요 역량 및 변화

1) 표준 및 인증 준수

개발과정에서 표준을 해석하고 적용하는 능력이 필요하다. 국내에서는 민간에 제공될 제품에는 표준을 적용하지 않아도 출시가 가능한 경우가 있으므로, 우선 제품을 개발하고 난 후 인증을 받기 위해 표준을 적용하여 수정하는 경우가 많으며, 다수의 개발자가 이러한 표준 관련 업무를 경험해보지 않아 어려워하는 경향이 있다.

또한, 국제 표준을 기반으로 한 제품에는 모두 API가 존재하고 동일한 API를 기반으로 상호 운용을 하는 데에 문제가 없지만, 국내 제품들은 개발 과정에서 API 자체를 만들지 않는 경우가 많아 연계하여 사용하기 어려운 상황이다.

하지만, 궁극적인 목표는 해외시장에 국내 제품을 판매하는 것이므로, 초기부터 표준을 준수하여 개발하는 방향으로 진행되고 있는 추세이다.

2) 설계문서 작성 능력

전체 개발 과정에서 설계문서 작성 업무는 매우 중요하며, 설계문서를 잘 작성해놓으면 초보 개발자도 문서를 기반으로 쉽게 코딩하여 개발이 가능하다.

따라서 이러한 설계문서를 작성하는 것은 기존 일정 연차 이상의 개발자가 설계문서 작업을 하는 것이 아닌, 신입에서부터 설계문서 작성 업무를 담당하여 능력을 키우는 것이 중요하다고 생각된다.

하지만, 일부 기업에서는 소수의 인력이 개발의 모든 과정을 담당하여 설계문서의 필요성을 느끼지 못하여 작성하지 않거나, 담당자의 능력에 따라 구체적인 설계문서가 도출되지 않는 경우도 많다.

3) 프로그래밍 언어

윈도우 기반의 PC에서 핸드폰이나 태블릿, 리눅스 기반의 Mac을 많이 사용함에 따라 주로 사용되는 프로그래밍 언어가 계속해서 변화한다. C나 C++은 기본이며 웹 개발에서는 JavaScript를 많이 사용하고 있으며, Python은 요즘 사용도가 줄어드는 추세이다.

또한, 애플리케이션도 옛날처럼 패키지를 받아 소프트웨어를 설치하는 것이 아닌, 웹에서 서비스로 소프트웨어를 이용하는 추세로 관련 기술도 계속해서 변화하고 있다.

4) 신기술에 대한 이해

코드 제작 과정에서 오픈소스 모델을 활용하여 본인의 업무에 맞게 변형해서 사용하는 등 AI를 통해 업무를 수행하는 능력도 중요해졌다. 처음에는 정보 유출을 고려하여 사용하지 못하게 하였으나, 이제는 학습데이터를 저장하지 않는 유료버전을 사용하게 하며 관련해서 보안 유출에 대한 사내 규정 및 인식교육을 진행하고 있다.

또한, 현재 클라우드의 경우 여러 조건을 고려하여 국내 서비스보다는 AWS나 Azure와 같은 해외 클라우드 서비스를 많이 이용하고 있는데, 이러한 서비스에서는 부가적인 툴을 많이 제공하고 있다. 따라서 클라우드로 전환하거나 설계하는 능력이 요구되는 것은 기본이고, 클라우드 서비스를 이용하면서 제공되는 부가적인 소프트웨어 및 툴에 대한 이해가 필요하다.

이 외에도, 정부에서 SW공급망 보안 관련 가이드라인을 제공하고 법제도 개정을 진행하고 있으며, 민간에서는 이미 SW공급망 보안 관련 점검 결과를 요청하는 등 향후에는 더 많은 관련 요구가 있을 것으로 예상된다.

5) 윤리의식

보안은 동일한 기술을 가지고 방어에 활용하면 보안이지만, 공격에 활용하면 해킹이 될 수 있으므로 직업윤리가 굉장히 중요하다. 따라서 채용과정에서 이러한 경험 여부를 점검하여 고려하고 있다.

② 직무 수준 및 변화

1) 해당 직무에 대한 경험

정보보호개발 직무는 나이와 상관없이 전문 지식과 시장 분석 능력, 기술적인 문제를 해결하고 새로운 기술을 개발하는 능력이 중요하므로 경험과 창의성이 많은 영향을 미친다.

○ 운영·관리 (정보보호엔지니어링 직무)

① 필요 역량 및 변화

1) 기술 발전에 따른 요구 수준 증가

클라우드 서비스 도입 이후, 단순 장애 대응 및 솔루션 제공이 아닌 외부 해킹 위협에 대한 대응이 더욱 중요해졌다. 특히, 오픈소스 소프트웨어나 엔터프라이즈 시스템에서 발생하는 보안 취약성도 중요한 문제로 떠오르고 있으며, SSL 보안 취약점과 같은 새로운 보안 위협도 등장하였다.

이 과정에서 운영체제(OS), 데이터베이스(DB), Python이나 JavaScript 등의 언어, 인프라, API 연계에 대한 기본적인 이해와 보안 위협을 분석하고 해결할 수 있는 능력이 요구된다.

특히, 코로나 시기 대면이 불가능한 상황에서 원격 근무와 화상회의가 증가하여 클라우드와 같은 기술적 변화는 더욱 강조되었으며, 이에 따라 추가적인 보안 문제에 대한 기술적 요구가 고도화되고 있다.

AI의 경우, 업무 수행 방식에 많은 영향을 미치고 있지는 않으나, 문제 해결을 위한 정보 검색이 쉬워져 효율적인 업무 수행이 가능해졌다. 하지만, 고객은 여전히 조직과 보안 환경에 대한 충분한 이해를 바탕으로 실시간 문제 해결을 제공해주는 전문가의 조언을 원하므로 AI가 해당 업무를 대체할 수는 없다.

2) 보안 기술 통합에 따른 기업 간 협업 증가

다양한 보안 솔루션 및 시스템을 연동하여 사용하는 등 전체적인 보안 시스템 통합이 이루어짐에 따라, 각 분야에서 전문성을 가진 타 기업과의 협업을 통해 시너지를 창출하는 것이 중요해졌다.

예를 들어, 일반 통신 대기업에서 보유하고 있는 고객을 대상으로 이메일 보안이나 모바일 보안 분야에서 협업을 진행하는 등 각자의 기술적 한계를 보완해주고 있다.

② 직무 수준 및 변화

1) 담당 인력의 교육훈련 기간

보통 입직 후 1~3개월 정도의 직무 교육과 내부 트레이닝을 통해 실무를 배우고 경험을 쌓으며, 3~6개월에는 선임자와 함께 현장에 나가 업무에 대한 이해를 넓힌다. 이후 6개월~2년차에는 상대적으로 업무 범위가 작은 고객사를 담당하며, 그 이후 중견기업이나 엔터프라이즈 급 기업을 담당한다. 그러나 최근에는 인력 부족으로 인해 상대적으로 경험이 적은 인력들도 업무 범위가 큰 기업을 담당하는 상황이 발생하고 있다.

2) 담당 인력의 수준 및 채용현황

기술 발전 속도가 빨라지면서 추가적인 고객의 요구와 업무가 생겨나고, 예측 불가한 보안 사고에 대해 긴급하게 처리해야 하는 수시 업무가 발생함에 따라 업무의 강도가 지속적으로 증가하고 있다.

해외에서는 엔지니어가 시간당 적절한 보수를 제공받으며 정해진 업무 시간 내에서만 업무가 진행되지만, 국내에서는 엔지니어에 대한 고객들의 높은 의존도와 요구사항에 업무가 과중되는 경우가 많다. 이러한 부분에 많은 스트레스를 받는 인력들이 증가하여 이는 해당 직무의 인력 이탈로 이어지고, 기업에서는 경력직을 선호하게 된다.

채용 시 보통 2~5년차의 경력직 인력을 선호하며, 실제 산업현장에도 2~3년차의 인력들이 많이 분포되어 있다. 또한, 과거에 비해 업무 강도나 일과 삶의 균형을 고려하여 이직이 잦아지면서 장기 근속자가 점점 줄어드는 추세이다.

○ 조사·대응 (보안관제 및 디지털포렌식 직무)

① 필요 역량 및 변화

1) 자동화를 적용한 솔루션 도입

정보보호산업에는 위협 탐지 및 대응 솔루션 EDR이 출시되고 얼마 지나지 않아 XDR이 출시되었으며, 지금은 모두 SOAR라는 개념을 활용하고 있다. SOAR라는 모든 보안 운영을 통합하여 자동화하는 시스템을 도입함에 따라, 자동화 관련 기술적인 능력과 더불어 기업의 보안정책을 만들고 대응할 수 있는 능력도 요구된다.

자동화 솔루션을 도입함에 따라 보안 사고를 탐지하고 대응하는 보안관제 서비스의 업무 범위가 많이 축소되었다. 관제 인력에 대한 수요도 줄어들었으며, 교육훈련과정과 보수에 대한 기준이 모두 변화되었다. 실제로 일부 대기업에서는 파견관제 인력을 모두 중앙에서 제어하는 관제 인력으로 전환하는 등 구조적인 변화도 발생하였다.

이로 인해, 보안관제 인력이 더 이상 단순 관제만 수행하는 것이 아닌 보안 분석 및 대응 업무도 수행하는 역할로 업무의 범위가 확장되고 있다. 따라서 보안관제 인력들이 역량을 향상시키고 분석 및 대응 업무에도 집중할 수 있도록 지원하는 방향으로 기업 내 변화가 필요하다.

또한, 디지털포렌식에서도 기술적인 부분을 자동화를 하려는 추세이다. 수사라는 것은 적재적소에 빠르게 조사가 진행되어야 하는데, 일반 경찰서가 아닌 지방청에서만 포렌식 분석이 가능하여 관할 지역의 데이터를 모두 한 곳에서 처리하다 보니 시간이 너무 많이 소요되어 수사가 지연되는 경우가 많았다. 따라서 포렌식 전문가는 데이터 처리 과정을 자동화하고 분석된 결과를 판단하여 검증하는 등 업무방식이 변화되고 있다.

② 직무 수준 및 변화

1) 담당 인력의 수준 및 변화

기술에 대한 변화는 존재하지만, 업무 방식에 대해서는 정해져 있는 범위 내에서 유지되고 있으므로 조사·대응 분야의 직무는 변화가 빠르지 않다고 생각된다. 하지만 업무 자동화에 따라, 단순히 사고에 대한 기술적 대응을 넘어 조직의 관리 체계와도 연관이 있으며, 기술의 발전으로 분석적 사고와 위험 관리 역량이 더 중요해지고 있다.

보안관제 직무는 인력 파견을 위해 과학기술정보통신부공고 행정규칙인 「보안관제 전문기업 지정 등에 관한 공고」내 '기술인력의 자격기준'에 기반하여 주로 인력을 채용하고 있다. 따라서 보안관제 업무를 수행하기 위한 기본 역량으로 정보보호 유관 IT 전공이나 관련 자격증(정보처리기사 등)을 선호하는 기업이 많다.

디지털포렌식 직무는 기술적인 능력만으로 해결되지 않는 부분이 많아 다양한 경험과 책임감이 요구된다. 타 보안 직무보다 디지털 포렌식 업무의 결과는 구속, 법정 싸움, 인사 조치 등 직접적으로 영향을 줄 수 있는 물리적인 조치로 이어지므로 굉장히 신중하고 보수적인 판단이 요구된다. 그러다 보니 많은 경험과 넓은 시야를 통해 오류를 최소화하는 것이 필요하여, 고연차의 재직자가 많다.

○ 진단·평가 (정보보호컨설팅 직무)

① 필요 역량 및 변화

1) 법제도 관련 지식

개인정보보호법, 전자금융거래법 및 전자금융 감독 규정에 대한 지식이 많이 요구되며, 관련 판례와 함께 법률 해석과 기술적인 보안 적용 방법에 대한 판단 능력이 필요하다.

실제로, 다수의 정보보호컨설팅 인력이 법무법인에서 전문위원으로 활동하고 있는데, 이 인력들은 법과 보안 기술의 접목 방법에 대해 자문하는 역할을 수행하고 있다. 이 과정에서 기업의 사내 정보보호 정책·규정·지침·절차서 등에 대한 초안을 만들고, 변호사와 법적 논의를 하는 등 협업이 필요하다.

2) 사용 도구 및 방법론

기본적으로 Wire Shark, Burp Suite, Fiddler, IDA와 같이 모의해킹과 웹 취약점 분석을 위한 도구 사용능력이 필요하다. 또한, IT시스템(인프라)과 관련해서 서버, 네트워크, DBMS와 같이 하드웨어 장비의 진단 스크립트를 구성하고, 스크립트를 분석하여 취약점을 개선할 수 있는 능력이 요구된다.

관리적 측면에서는 PDCA, SWAT 분석 등의 방법론을 적용하여 장단점을 분석하고, 보안에 접목하기 위한 구조화 능력이 필요하다. 이 과정에서 AI를 활용하여 업무 시간이 상당히 단축되었지만, AI는 새로운 데이터에 대한 답변을 제공하지 못하기 때문에 컨설팅 인력을 완벽히 대체할 수는 없다.

② 직무 수준 및 변화

1) 담당 인력의 수준 변화

NCS 수준체계를 기준으로 대략 4수준 이상이 요구되며, 평균 7~8년의 업무 수행 경험을 통해 전반적인 지식 베이스를 습득하여 업무를 구조화시키는 등 컨설팅 업무에 적용이 가능하다.

하지만, 관련 인력들이 정보보호 전문업체에서 커리어를 쌓는 것이 아닌, 보다 많은 보상을 보장받을 수 있는 타 산업의 정보보호 담당자로 이직하는 경우가 많아졌으며 정보보호산업에 유입되는 인력이 상대적으로 많이 줄어들고 있다.

또한, 일반기업의 정보보호담당자 수준이 높아지면서, 정보보호 전문업체에 전반적인 보안 컨설팅을 의뢰하기 보다는 취약점 분석, 컴플라이언스 검토 등 내부 인력으로 물리적인 소화가 어려운 단순 업무를 아웃소싱하는 상황이 증가하여, 일부 정보보호컨설팅 인력들의 업무 방향성이 기존과는 바뀌어가고 있는 추세이다.

○ 신기술보안 (모빌리티보안 직무)

① 필요 역량 및 변화

1) 모빌리티 보안의 중요성 대두

자율주행 기술과 주행 보조 시스템(ADAS), 전자제어 시스템의 발전 등으로 모빌리티 분야는 점점 더 많은 데이터를 처리하고 네트워크와 연결되는 사이버 보안 위협을 초래하고 있다.

과거에는 주로 정보 탈취나 금융적인 피해가 주요 보안 위협이었다면, 현재에는 사람의 생명과 직결된 보안 사고가 우려된다. 예를 들어, 차량의 통신 시스템을 해킹해 차문을 열고 시동을 거는 등 차량을 도난 하는 방법에도 사이버 공격이 사용되고 있다.

유럽에서는 2024년부터 모든 신규 차종에 대해 보안 설계 및 증빙을 의무화하였으며, 한국에서도 대규모 제작사는 내년 8월부터, 소규모 제작사 및 자율주행차는 올해부터 적용하는 등 보안 강화 정책을 추진한다.

이에 따라, 자동차 제조업체들은 보안 라이프 사이클을 전면적으로 관리하고, 설계·생산·운영·테스트 등 모든 과정에서 보안을 고려해야 한다. 또한, 글로벌 OEM(자동차 제조사)에서는 보안 관련 산출물이 증빙되지 않으면 부품을 납품받을 수 없도록 규제를 강화하고 있어, 이를 위해 각 부품사들도 보안 관련 프로세스를 마련하고 있다.

모빌리티 보안은 이제 단순히 제품 개발에 국한되지 않고, 생산 라인과 운영 단계까지 보안 관리의 범위가 확장되고 있어 모빌리티 보안에 대한 수요는 꾸준히 증가하고 있다. 이러한 변화는 자동차뿐만 아니라 농기계, 건설기계, 이동형 장비 등 다양한 모빌리티 기계와 장비로 확장될 것으로 예상된다.

하지만 해당 산업에 대한 기업들의 진입 장벽이 높고, 어느 정도의 자본과 규모가 있어야만 보안을 위한 실질적인 테스트와 작업이 가능하다.

2) 임베디드 시스템 및 보안 지식

모빌리티 보안 분야는 임베디드 시스템 기반의 RTOS(실시간 운영체제)와 C언어로 개발된 커널 레벨의 소프트웨어 관련 지식이 필요하다. 특히, 암호화, 액세스 제어, 커널 드라이버 등과 같은 보안 기술이 핵심이며, 이는 IoT 보안 관련 경험과도 이어진다.

3) 소프트웨어 정의 차량(SDV)으로의 전환

SDV[11]로의 전환 과정에서 차량 내 SW가 탑재되면서 하드웨어 보안과 더불어, 소프트웨어 보안 및 커넥티드 시스템에 관한 지식이 요구된다. 예를 들어, 국내 현대자동차에 탑재되어 있는 블루링크와 같은 커넥티드 서비스 등이 있다.

특히, SDV 분야에서는 클라우드를 통해 개발, 테스트, 시뮬레이션을 시행할 수 있는 환경을 구축하려고 추진하고 있다. 또한, 소프트웨어 원산지 증명 및 클라우드 서비스와 관련된 보안 요구 사항이 증가하는 등 모빌리티 시스템 개발에서도 클라우드에 대한 보안 조치가 강화되고 있다.

4) 품질 관리 및 문서화

모빌리티 보안 분야는 품질 관리 라이프 사이클과 밀접하게 연관되어 있으며, ISO 21434 등에 기반하여 개발·설계·테스트·생산 등 모든 과정에서 보안 요구사항을 증빙하고 문서화하는 것이 중요하다.

5) 법률 모니터링 및 자문 능력

모빌리티 보안 분야는 현재 제도화가 진행 중인 법률이 많으므로, 관련해서 산업계의 요구사항을 정부 기관에 전달하여 협력하는 등 법제화를 준비하고 대응할 수 있는 능력이 필요하다. 이때 법률 전문가나 규제 전문가도 보안팀의 일원으로 활동하며, 새로운 법규가 제정될 때마다 이를 현장에 적용하는 과정이 필요하다.

특히, 자율주행 차량에서 수집되는 개인영상정보에 대한 규제가 강화되고 있으나, 현재에는 규제 샌드박스[12] 제도 등 규제가 일부 허용되고 있다. 이 과정에서 개인영상정보 원본 데이터 사용에 대한 엄격한 보안 조치가 필요하며, 차량이나 드론에 장착된 카메라는 필수적으로 익명화 또는 비식별화가 요구된다. 그러나 현재 기술로는 실시간 스트리밍 영상에 대한 마스킹 처리 과정에 어려움이 있어, 이를 해결하기 위한 연구와 개발이 진행 중이다.

11) SDV(Software Defined Vehicle) : 소프트웨어로 하드웨어를 제어하고 관리하는 자동차
12) 규제 샌드박스 : 특정 모빌리티 기업들은 2년 동안 원본 데이터를 활용할 수 있는 특례를 받아, 그 기간 동안 익명 처리 없이 데이터를 사용할 수 있음

6) AI의 활용의 확대

모빌리티 보안 분야에서 AI 기술은 자율주행, 첨단 운전자 보조 시스템(ADAS), 음성 인식 시스템 등에 널리 사용되고 있으며, 특히 생성형 AI는 개발 속도 및 업무 효율성을 증가시키고 있다.

② 직무 수준 및 변화

1) 높은 인력 수요

학계에는 아직 모빌리티 보안 관련 전공이 많이 개설되어 있지 않아, 전문적인 지식을 갖춘 인력이 많지는 않으므로 산업현장에서 업무를 숙지하는데 상당한 시간이 필요하다. 하지만, 모빌리티 보안에 대한 수요가 급격히 증가하고 있어 모빌리티 보안 전문 인력 양성의 필요성이 대두되고 있다.

2) 전문성 확장

모빌리티나 OT와 같은 특수 분야에서는 전통적인 IT 보안과 달리, 산업 시스템과 기계 제어 시스템에 대한 이해를 기반으로 산업 보안 지식이 매우 중요하다.

기존 IT 보안은 클라우드, 서버, 모바일 애플리케이션 등의 보안에 집중하지만, 모빌리티 보안은 임베디드 시스템과 자동차의 하드웨어, 소프트웨어 설계를 함께 고려해야 한다.

이에 따라, 기존 보안 전문가가 모빌리티에 대해 학습하거나, 모빌리티 제조 전문가가 보안에 대해 학습하는 등 모빌리티 보안 전문가들의 전문성이 확장되고 있다.

하지만 이러한 분야에서의 높은 인력 수요에 비해 전문 인력은 다소 부족한 상황이며, 경력이 매우 중요한 요소로 작용하여 주로 인력 추천을 통해 채용을 진행하는 경우가 많다.

○ 기타 (기술영업 직무)

① 필요 역량 및 변화

1) 트렌드 파악 능력

기술영업 직무는 보안기능을 고객에게 인정을 받아 기업에 제품구매를 유도하기까지의 전반적인 과정에 대한 고민이 필요한 업무이므로 빠르게 IT 트렌드를 파악하여 시장에서 요구하는 기술에 대한 정보를 습득해야 한다.

따라서 사내에서는 트렌드 파악을 위한 세미나 참석도 적극적으로 장려하고 있으며 파트너사를 대상으로 자체적인 교육도 많이 진행하는 경우가 많다.

2) 세일즈에 대한 마인드

제품이 우수해도 영업이 적절하지 않아 구매를 망설이는 경우가 있으므로, 고객의 성향에 맞추어 의견을 들어주고 솔루션을 제공해주는 등 기본적인 세일즈에 대한 마인드와 자세가 요구된다.

고객의 보안 문제점을 미리 파악하여 자사의 제품이 어떠한 혜택을 제공하고 해결책을 줄 수 있는지, 어떠한 업무 효율과 가치를 제공할 수 있는지를 명백하게 전달하는 능력이 필요하다. 지속적인 영업 기회를 확보하기 위해 고객과의 신뢰관계를 형성해나가는 것도 중요하다.

또한, 고객의 요구사항을 빠르게 파악하여 해결책을 제시하기 위해서는 지속적으로 소통하고 질문하는 자세를 지녀야 한다. 하지만 신입의 경우 불편한 소리를 듣고 말하는 경험이 적다보니 이러한 업무를 진행하는데 어려움을 겪는 경우가 있다.

3) 문서작성능력 및 업무 협업 능력

기술영업 담당자는 제품 소개하는 문서는 기본적으로 작성해야 하며, 최근에는 소프트웨어 품질성능 평가시험(BMT)나 PoC 등 제품 검증을 위한 자료를 작성하는 능력이 많이 요구되고 있다. 이 과정에서 제품 시연을 요구하여 엔지니어와 협업하는 경우도 많으며, 시연을 위한 시나리오 구성과 제품 안내서를 작성해야 한다.

또한, 고객인 기업의 보안 담당자의 입장에서 회사에 명백한 당위성을 제공하고 설득하는 것을 돕기 위해 시장 현황 및 제품 비교분석 등의 내용에 대한 문서작성 능력도 요구된다.

아울러, 현장의 의견을 반영한 제품을 개발하기 위해 기획 단계에 참여하기도 하며, 고객의 클레임을 엔지니어와 함께 해결하는 등 타 직무와 협업하는 능력도 많이 필요하다.

② 직무 수준 및 변화

1) 수준 및 교육훈련

현장에는 NCS 수준체계를 기준으로 3~4수준의 인력이 많으며, 4~5년 정도 근속하게 되면 시장에서 필요로 하는 인력으로 성장이 가능하다.

약 6개월의 교육을 통해 기술적인 설명이 가능하며, 1년 정도 업무를 수행하면 영업에 대한 부분까지 숙지가 가능하다고 생각된다. 회사마다 다를 수는 있으나 보통 전공과 학력은 크게 중요하지 않다.

2) 직무변화속도

전반적으로 영업 직무는 하나의 제품을 담당하면 그 담당이 계속 유지되는 경우가 많다. 특정 기술과 제품군에 대해 연구하다가 다른 영역의 제품으로 바꾸기는 어렵기 때문에 직무 변화도가 다소 낮다고 생각된다.

직무를 수행하는 방식에 대한 변화는 적을 수 있지만, 본인 담당하고 있는 제품이나 기술과 관련하여 주기적으로 트렌드를 파악하고 적용하는 등 관련 지식을 업데이트하는 것은 필요하다.

결론 및 제언

PART. 05

5 결론 및 제언

1. 시사점

정보보호 분야 직무의 빠른 변화 주기

다양한 기술혁신과 법·제도의 변화, 보안사고의 영향으로 정보보호의 필요성은 나날이 증가하고 있다. 이에 따라 정보보호 분야의 직무는 2~3년 주기로 빠르게 변화하기에 주기적인 모니터링이 필요하다. 직무별 전문가 인터뷰를 통해 파악한 정보보호산업 및 직무에 전반적인 영향을 미치는 주요 요인은 다음과 같다.

○ 신기술 등장으로 인한 시장환경변화

1) 생성형 AI의 영향

생성형 AI가 다양한 산업에 확산됨에 따라 보안산업에서도 AI를 접목시키려는 추세로, 보안 관련 AI 기술이 확장되고 있으며 AI 전문인력에 대한 수요가 증가하고 있다. 개발된 보안 제품에 AI 서비스를 접목 시키거나, 다수의 개발자가 코드를 제작하는 과정에서 오픈소스 코드가 학습된 AI를 활용하는 등 이미 보안산업에서도 AI가 많이 활용되고 있다.

특히, ChatGPT라는 제품이 나온 이후 우리나라 산업에 엄청난 영향을 미쳤다. 출시 이후, 정부에서도 연구 과제로 AI를 많이 도입하고 있으며, 기업에서도 챗봇을 이용하여 고객상담을 진행하는 등 이미 산업에 많이 적용된 상황이다.

또한, 이러한 AI 기술이 발전하고 범용화 되면서 해커 집단이 역추적을 통해 오픈소스 코드의 취약점을 알아내어 공격이 가능하고, AI 활용 과정에서 간접적으로 학습된 데이터를 통해 개인정보가 유출될 수 있으므로, 이에 대한 보안의 필요성은 더욱 대두되고 있다.

이에 AI 서비스 출시 초기에는 다수의 회사에서 AI를 사용하지 못하게 금지하였으나, 최근에는 업무 효율을 위해 사내 정책을 수립하여 AI 활용을 허용하고 있는 추세이다. AI 활용 관련 내부 규정을 통해 사용 내역을 모니터링 하거나, 데이터를 학습하지 않는 유료 버전을 구입하여 배포하는 등 정보유출을 막기 위한 다양한 사내 정책을 시행하고 있다.

향후 시장에서 전통적 보안 운영 솔루션, 데이터 분석 등의 자리는 AI로 대체될 가능성이 높다고 생각되며, 환경변화에도 의견을 조율하고 협업하는데 있어 사람의 역할이 필요한 부분은 유지될 것으로 예상되어 정보보호인력의 수요는 지속적으로 발생할 것으로 보인다.

2) 클라우드의 영향

정보보호산업의 인프라가 기존 온프레미스 환경에서 클라우드 기반의 시스템으로 전환되고 있으며, 이러한 과정에서 클라우드에 대한 보안지식이 많이 요구되고 있다. 특히, 금융권과 공공에서는 이러한 전환이 가속화되고 있으며, 이를 통해 데이터센터 화재와 같은 물리적인 장애 발생의 리스크를 줄이고 안정성을 높이려는 추세이다.

AWS, 오피스 365, 구글 워크스페이스 등 다양한 클라우드 플랫폼이 보편화되면서 클라우드 시스템에 대한 보안 기술의 중요성이 강조되고 있으며, AI와 클라우드 인프라의 결합으로 보안에 요구되는 수준이 고도화되고 있다.

이에 따라, 클라우드로 전환하거나 설계하는 능력이 요구되는 것은 기본이고, 클라우드 서비스를 이용하면서 제공되는 부가적인 소프트웨어 및 툴에 대한 이해가 필요하다.

○ 시장변화에 따른 법·제도 변화

현재 금융권에서는 클라우드 및 망분리 규제 완화를 위한 관련 법 개정을 추진 중에 있으며, 국정원에서도 MLS 체계 등을 통해 망분리 개념을 넘어선 기술 발전을 추진하고 있다.

이 외에도 소프트웨어 개발보안 의무제가 시행되면서 국내에서도 시큐어코딩 기술이 활발해지고, SW공급망 보안이 대두되면서 관련 가이드가 배포되는 등 전산업에서 요구하는 정보보호제품의 수요가 변화해가고 있다.

또한, 개인정보보호법·전자금융거래법 등 정보보호 관련 컴플라이언스가 강화됨에 따라 국가 및 기업의 조직이 변화되고 국내 보안 산업 뿐 아니라, 모든 산업의 일반기업에서도 보안인력의 수요가 증가하고 있다.

따라서 법·제도의 변동을 빠르게 파악하고 이를 반영한 기업의 보안 정책과 전략을 설정하는 것이 매우 중요하다.

기타

1) 글로벌 시장의 영향

글로벌 시장에서 특정 IT 기술이 유행하게 되면 해당 기술이 탑재된 제품이 범용화되며 이에 대한 보안상 취약점이 발견되고 해커의 공격대상이 된다. 이에 따라 국내에서도 피해 사례가 증가하게 되면서 국가 예산이 편성되고, 법제도가 강화되는 등 전반적인 정보보호 산업 환경이 변화된다.

특히, 미국, 유럽 등 사이버보안 선도국가에서 발표하는 보안 관련 정책, 조치, 보고서와 같은 글로벌 보안 트렌드에 많은 영향을 받는다.

2) 보안사고의 영향

정보보호산업은 보안사고가 크게 발생하고 나면 보안에 대한 투자 방향이 바뀌고 특정 보안 이슈를 해결하기 위한 솔루션이나 서비스에 개발이 집중되는 등 산업 전체가 변화되는 경향이 있다. 예를 들면, 예전 해외 SCADA[13] 보안사고 이후 기존 PC에만 집중되어 있던 국내 보안시장에서 산업보안의 필요성이 대두되었으며, 이후 연구회, 국가 연구과제가 생기는 등 학계와 정부기관에도 많은 영향을 주었던 사례가 있다.

3) 인력의 가치관 변화

직장 내 업무와 개인 생활의 균형을 중시하는 경향이 강해지면서 재택근무, 자율근무제 도입 등 근무환경도 많이 변화하고 있다. 정보보호산업에도 업무의 유연성과 개인의 가치관을 중시하는 문화가 확산되고, 이러한 인력이 유입되면서 산업에 많은 영향을 미치고 있다.

특히, 일부 직무는 24시간 업무가 필요한 직무로 3교대 근무와 야간 근무가 불가피한 상황에서 중급 이상의 인력 이탈이 많이 발생하고 있다. 따라서 정보보호산업의 지속적인 업무 환경 개선과 역량 향상 교육을 통해, 직무에 대한 부정적인 인식 전환과 해당 직무의 전문성을 강화시켜 고급 인력을 유지하는 것이 필요하다.

13) SCADA(Supervisory Control And Data Acquisition) : 산업 공정, 기반 시설, 설비를 바탕으로 한 작업공정을 감시하고 제어하는 산업 제어 컴퓨터 시스템

직무 세분화 및 추가를 통한 직무맵 보완 필요

○ 정보보호 분야 직무 세분화

현재 모의해킹이 '정보보호컨설팅' 직무의 세부 업무로 포함되어 있지만 실제 산업현장에서는 정보보호컨설팅과 모의해킹 직무를 별도의 업무로 구분하여 외주 계약을 진행하기도 하며, 실제 모의해킹만 단독으로 영위하는 업체가 꾸준히 증가하고 있다.

특히, 보안 솔루션 업체 중에서도 취약점 진단 툴이나 특정 인증 서비스를 제공하는 업체에서 모의해킹 서비스를 제공하고 있는데, 정보보호컨설팅 직무와는 적용하는 법제도와 기술적 요구사항, 기업 구분이 명확히 다르므로 **'모의해킹'**을 별도의 직무로 분리하는 것을 고려할 필요가 있다.

- 정보보호컨설팅 : 화이트박스 기반 관리적 업무 수행
- 모의해킹 : 블랙박스 기반 기술적 업무 수행

또한, 최근 모의해킹 직무가 취약점 관리와 대응 등으로 업무의 범위가 확장되고 있으므로, 모의해킹을 취약점 점검이나 취약점 관리 등 보안진단의 업무로 확대하여 직무를 정립하는 방향도 고려할 필요가 있다.

➲ **주요 키워드** : 기술적 취약점 진단, 취약점 탐지/분석, 기술적 대응 조치, 공격 시뮬레이션, 취약점 보고서 작성 등

○ 정보보호 분야 직무 추가

1) AI 보안

'AI for Security'와 'Security for AI'라는 두 가지 관점이 존재하나, 'Security for AI'를 의미하는 **'AI 보안'** 직무의 필요성이 높아지고 있다. 위협 동향 보고서나 컨퍼런스, 세미나 등을 통해 AI 보안에 대한 논의가 활발하게 진행되고 있으며, 산업계에서도 AI 보안 업무를 수행할 수 있는 인력에 대한 수요가 매우 높다.

실제 일부 정보보호 전문기업에서는 AI 학습데이터 모델 개발, AI 보안 탐지 및 위협 검증 등 AI 보안을 위한 AI 연구소를 운영하고 있으며, 내부인력의 역량 향상을 위한 자체 교육을 진행하거나 학계와의 연계를 통한 AI 보안 관련 교육훈련을 지원하고 있다.

이와 같이 AI 보안 시장이 매우 빠르게 성장하고 있는 추세이므로 해당 직무를 선제적으로 정립하는 것이 필요하다.

➲ **주요 키워드** : AI모델 보안, 데이터프라이버시, 모델공격/방어, 공정성/강건성/신뢰성, 적대적 공격, AI 취약점 및 위협 분석, AI 보안 정책/컴플라이언스 등

2) IoT 보안

스마트 헬스케어, 스마트 팩토리, 스마트 홈, 스마트 시티 등 각 분야에서 사용하는 프로토콜이 다르며, IoT 기반의 통신 프로토콜 보안에 대한 법 및 표준 등이 많이 생겨날 것으로 예상되므로 '**IoT 보안**' 관련 직무에 대한 정립 또한 고려해야 한다.

특히, IoT 분야의 경우 개인정보보호나 영상보안 등과 연결되어 각 산업에서 해당 분야의 보안에 대한 수요가 매우 높은 상황이다.

➲ **주요 키워드** : 디바이스 인증, 네트워크보안(게이트웨이), 보안 업데이트 및 패치, 엣지 컴퓨팅 보안, 펌웨어보안, 보안 프로토콜, 디바이스 생애주기 관리 등

3) 보안 아키텍처링

보안 아키텍처는 IT와 보안을 연결하는 중요한 도구이며, 최근 많은 업체에서 클라우드 환경으로 시스템을 전환하고 있는 시점에서 이해관계자들과의 중요한 의사소통 도구로 사용되고 있다.

실제 일부 기업에서는 제품 개발 과정에 참여해서 보안 요구 사항을 정의하고 보안 관점에서 아키텍처를 설계·검증하여 보안성 심의를 담당하는 시큐리티 아키텍처(SA) 전담 인력이 존재한다. 또한, 정보보호 전문기업에서는 해당 업무를 기술지원 또는 개발 관련 업무 종사자가 겸업하여 수행하는 경우가 있다.

이에 따라, 시스템 아키텍처 중 보안 관련 아키텍처를 구조화하고 분석하는 업무를 수행하는 '**보안 아키텍처링**' 직무를 정립하는 것이 필요하다.

➲ **주요 키워드** : 암호화, 위험관리, 접근제어, 모니터링 및 감사, 보안정책 및 표준, 고가용성 및 복구, 보안 아키텍처 설계/검증 등

이를 통해 도출된 정보보호 분야의 직무맵(안)은 다음과 같이 예상된다.

그림 V-1 | 정보보호 분야 예상 직무맵(안)

수준 \ 직무	정보보호 운영/관리	(가칭) 보안진단	정보보호 컨설팅	보안사고 대응	정보보호 개발	영상정보 보안	디지털 포렌식	(가칭) AI보안	클라우드 보안관리 운영	모빌리티 보안	OT보안	(가칭) IoT보안
8												
7		예상										
6								예상				예상
5												
4												
3												
2												
1												
산업분야	정보보호											
소관분야	정보보호ISC 소관분야											

수준 \ 직무	정보보호 기획	(가칭) 보안 아키텍처링	정보보호 엔지니어링	보안 품질관리	기술영업	마케팅/ 홍보	정보보호 교육	보안감사	보안감리	보안 인증평가
8										
7										
6		예상								
5										
4										
3										
2										
1										
산업분야	정보보호									
소관분야	정보보호ISC 소관분야									

신규 교육 훈련 분야에 대한 수요

○ 융합 보안 기술에 대한 교육

현재 정보보호산업에서 보안 관련 단일기술은 이미 많이 개발된 상태이므로 그 기술들을 융합하여 활용하는 것이 중요해졌다. AI와 클라우드, 모빌리티 등 신기술이 등장하거나 새로운 산업군에서 보안에 대한 수요가 급증하고 있다.

또한, 정보보호산업은 IT 트렌드에 따라 보안 기술에 대한 수요가 빠르게 변화하므로, 기존 전통적인 보안 기술과 새로운 보안 기술이 더해져 활용되는 융합 보안 기술에 대한 교육의 수요가 더욱 늘어날 것으로 예상된다.

예를 들어, OT보안의 경우 산업 시스템과 기계 제어 시스템에 대한 이해를 기반으로 한 산업 보안 지식이 매우 중요하다. 하지만, 이러한 제조 공정의 프로토콜을 이해하고 있는 인력이 부족하여 일부 기업은 외부 컨설팅을 통해 이러한 문제를 해결하고 있다.

이에 따라, 보안 인력에 대한 높은 수요가 있는 산업으로의 직무전환 교육이나, 사내에서 관련 보안 사업을 영위할 수 있도록 특정 산업과 융합되는 보안 기술에 대한 교육이 필요하다.

신기술보안 분야는 인력에 대한 수요가 매우 높은 분야이지만 관련 지식을 보유하고 있는 인력이 적어 높은 수요에 비해 공급이 저조한 상황이다. 따라서 신기술보안 관련 트렌드를 공유하고 정보를 학습할 수 있는 지속적인 세미나와 교육이 필요할 것으로 생각한다.

○ 보안 개발자를 위한 교육

보안 개발 업무에서는 '보안 오케스트레이션'의 필요성이 증가하고 있다. 이러한 과정에서 보안제품 개발 관련 표준 및 인증 문서, API 규격 등을 이해하여 적용하고, 이러한 전반적인 보안 개발에 대한 설계문서를 작성할 수 있어야 한다.

현재 정규 교육과정에서는 코드 제작과 같은 전반적인 제품 개발 관련 기술 위주의 교육이 진행되고 있으나, 정보보호개발 직무 수행을 위해서는 보안 개발 관련 표준 및 인증을 선택하고 적용하는 방법과 설계문서를 작성하는 방법 등에 대한 교육도 강화될 필요가 있다.

따라서 보안 개발자를 위한 해당 내용 관련 교육을 진행하여 실제 산업현장의 수요에 맞는 인력양성이 필요하다.

2. 향후 계획

직무변화 모니터링 사업 수행 방향

2024년도 직무변화 모니터링은 심층인터뷰 전 산업 및 직무 변화 파악을 위해 총 30개의 국내 정보보호 기업을 대상으로 사전 설문조사를 진행하였으나, 산업 규모 대비 다소 적은 표본으로 전반적인 변화를 파악하기에는 한계가 있었다.

더불어, 금번 직무변화 모니터링 설문 및 인터뷰 과정에서는 기업 담당자의 직무변화 모니터링 사업과 직무맵에 대한 이해도 부족으로 인하여 설문조사에 어려움이 있었다.

따라서 차년도에는 대면 설명회를 통해 모니터링 사업에 대한 이해도를 제고시키고 설문조사의 효과성을 향상시키고자 한다. 또한, 설문조사 및 인터뷰 대상자의 소속 기업 규모, 영위 사업 등에 의한 업무 환경 차이도 함께 분석할 예정이다.

차년도 직무변화 모니터링 사업 수행 방향

2020년 8월에 개인정보보호를 전담하는 중앙행정기관으로 '개인정보보호위원회'가 출범되면서, 데이터 3법·개인정보보호책임자(CPO) 지정 요건·영상정보처리기기 운영 규정 및 안전조치 기준 등 개인정보보호 관련 법령 및 제재 규정이 개정됨에 따라 개인정보보호산업에 많은 직무변화가 있을 것으로 예상된다.

또한, 금번 '정보보호산업 직무변화 모니터링' 설문조사에서도 개인정보보호산업의 직무 관련 의견이 다수 제출되었다. 가명·익명처리, AI 활용에 따른 개인정보보호, 각종 개인정보 유출 사고 등에 따라 개인정보보호의 중요성이 증가함에 따라 개인정보보호 직무의 세분화 및 추가 정립의 필요성이 제시되었다.

따라서 차년도에는 정보보호ISC의 소관 산업 중 하나인 '개인정보보호산업'의 직무변화 모니터링을 수행하여 개인정보보호 분야의 직무의 필요 역량 및 변화를 파악하고, 이를 기반으로 개인정보보호 분야의 직무맵을 보완할 예정이다.

2024 정보보호산업 직무변화 모니터링 보고서

부 록

PART. 06

6 부 록

1. 직무변화 모니터링 설문지

직무변화 모니터링

(인사 및 현업부서 대상 CATI 조사)

안녕하십니까?
정보보호 인적자원개발위원회는 고용노동부에서 지원하는 산업 거버넌스로서 직업능력개발의 기초정보를 제공하기 위한 다양한 사업을 수행하고 있습니다.

본 위원회에서는 금년도 사업 가운데 하나로「직무변화 모니터링」사업을 수행하고 있으며, 이를 위해 정보보호산업의 기업 관계자를 대상으로 '직무변화 모니터링'을 실시하고 있습니다.

이번 모니터링을 통해 정보보호산업의 직무변화 양상을 파악하고 그에 따른 역량 변화에 대응하기 위한 시사점을 도출하고자 합니다.

귀하의 소중한 의견은 직업능력개발의 발전을 위한 자료로 활용될 예정이니 잠시 시간을 내어 끝까지 설문에 응답해 주시기를 당부드립니다.

응답을 완료한 경우 모니터링 완료 이후에 소정의 답례품을 지급해 드릴 예정입니다.

귀하께서 응답하신 내용은 통계 목적으로만 사용되며,「통계법」제33조와 34조에 의해 비밀이 보장되고 타 목적으로는 사용되지 않을 것임을 약속드립니다. 감사합니다.

2024년 7월

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

- 주관기관 : 정보보호 인적자원개발위원회(대표기관 : 한국정보보호산업협회(KISIA))
  이보연 팀장 Tel(02)6748-2011 / 이은수 주임 Tel(02)6418-5651

개인정보 수집 · 이용 동의 안내

개인정보보호법 등 관련 법규에 의거하여 정보보호 인적자원개발위원회(한국정보보호산업협회)는 응답자의 개인정보 수집 및 활용에 대해 개인정보 수집·이용 동의를 받고 있습니다.

해당 정보는 명시된 제공목적 이외에는 활용되지 않으며, 제공한 개인정보의 이용을 거부하고자 할 경우에는 열람·정정·삭제를 요청할 수 있습니다.

아래와 같이 민감정보를 처리합니다.

제공 항목	제공목적	보유기간
성명, 전화번호, E-mail	데이터 검증 및 오류 수정을 위한 추가 연락	'24.12.31(화)까지

본인은 위 사항에 따라 조사 사실을 충분히 설명 받고 숙지하였으며, 조사 참여를 거부할 권리가 있다는 사실을 인지하고 있으며, 개인정보 제공에 동의합니다.

동 의		비동의	

2024년 월 일

성명 (서명 또는 인)

대표 응답자 정보			
성명		전화번호	
부서/직위		e-mail	
직무경력		휴대폰 번호 (답례품 수령)	
비고	* 조사 관련 요구 사항 있으면 기입		

A. 귀사의 일반현황 정보를 기재해 주십시오.

기업명		설립년도	년
대표자 성명			
소재지	① 서울 ② 부산 ③ 대구 ④ 인천 ⑤ 광주 ⑥ 대전 ⑦ 울산 ⑧ 경기 ⑨ 강원 ⑩ 충북 ⑪ 충남(세종) ⑫ 전북 ⑬ 전남 ⑭ 경북 ⑮ 경남 ⑯ 제주		
기업형태	① 대기업 ② 중견기업 ③ 중소기업 ④ 공공기관 ⑤ 협회 또는 단체 ⑥ 기타( )		
주사업 구분	① 정보보호(정보보안, 물리보안)가 주사업 ② 타사업이 주사업		
주력제품/서비스			
전체 종사자 수 (2024년 응답일 기준)	명 * 상시근로자, 일용근로자, 파견 종사자 모두 포함		

<주력제품 / 서비스>

구분	주력제품 / 서비스	예시
정보보안	네트워크보안 솔루션	방화벽, IPS, DDoS, NAC, 네트워크 위협 탐지 및 대응, 망분리 등
	엔드포인트보안 솔루션	엔드포인트 위협 탐지 및 대응, 악성코드/랜섬웨어 대응, APT 대응 등
	플랫폼보안/보안관리 솔루션	서버 접근 통제, 패치관리시스템, 디지털 포렌식 시스템, SOAR, XDR, TI 등
	클라우드보안 솔루션	워크로드 보안, 보안 형상관리, CASB, SASE, 가상화 관리 등
	컨텐츠/데이터 보안 솔루션	DLP, DRM, DB보안, 인쇄물 보안, 메일 보안, 개인정보 비식별화 솔루션 등
	공통인프라보안 솔루션	통합계정관리, 공개키기반구조, 차세대 인증, SIEM, 로그관리/분석 시스템 등
	보안 컨설팅	정보보호 평가/인증, 정보감사, 개인정보보호컨설팅, 진단 및 모의해킹 등
	보안시스템 유지관리/보안성 지속 서비스	보안시스템 유지관리, 보안성 지속 서비스 등
	보안관제 서비스	원격관제 서비스, 파견관제 서비스 등
	보안교육 및 훈련 서비스	보안교육 및 훈련 서비스
	보인인증 서비스	공동인증/간편인증/신기술인증, 본인확인서비스/본인인증서비스 등
	기타	기타
물리보안	보안용 카메라	아날로그 카메라, 열화상카메라, 방폭카메라, IP카메라, 멀티센서카메라 등
	보안용 저장장치	DVR, NVR, 서버스토리지, 예비저장장치 등
	보안장비 부품	렌즈, 이미지센서, 칩셋, 모듈/보드 등
	물리보안 솔루션	영상감시관제 솔루션, 지능형 영상감지 솔루션 등
	물리보안 주변장비	영상전송장비, 전용용품, 암호화 장비 및 솔루션, 보안용 모니터 등
	출입통제 장비	스마트카드/카드리더/컨트롤러, 보안용 게이트 등
	생체인식 보안시스템	얼굴인식 시스템, 지문인식 시스템, 홍채인식 시스템 등
	경보/감시 장비	적외선/레이저/진동/장력센서/모션디텍터/침입탐지장비 등
	기타제품	이동식 제품, 물리적 방호 장비 등
	출동보안 서비스	보안출동 제공 서비스
	영상보안 서비스	보안영상 제공 서비스(출동서비스 제외)
	클라우드 서비스	클라우드 기반 물리보안 서비스
	기타 보안 서비스	기타 보안 서비스(설치 및 유지관리 포함)

B. 다음은 정보보호산업의 직무변화 선행요인과 관련된 질문입니다.

B-1. 최근 정보보호산업의 직무나 일하는 과정의 변화를 초래하는 요인이 무엇이라고 생각하십니까? (복수선택 가능)

① 기술혁신(인공지능, 자동화 등)
② 법·제도변화
③ 인력변화(인구감소, 처우·급여 등 개인욕구변화 등)
④ 시장환경변화(시장수요, 경쟁 등)
⑤ 업무환경변화(재택근무, 스마트오피스 등)
⑥ 기타(　　)

B-2. (B-1 요인 이외에) 정보보호산업의 직무나 일하는 과정의 변화를 초래하는 요인은 구체적으로 무엇입니까?

구분	의견
요인	

C. 다음은 직무변화의 직무별 세부내용 관련 질문입니다.

<정보보호 분야 직무 구분>

구분	직 무	정 의
연구·개발	정보보호기획	조직의 목표 달성과 정보자산의 보호를 위해 정보보호 전략, 거버넌스, 운영정책, 정보보호 제품 및 솔루션을 기획하는 일이다.
	정보보호개발	정보보호제품에서 요구되는 요구사항을 분석하여 정보보호제품을 설계하고, 보안 요구사항에 대한 테스트 및 검증하는 일이다.
운영·관리	정보보호운영/관리	정보 자산을 안전하게 운영하기 위하여 정보보호 제품 및 솔루션을 운영하고, 법제도를 준수하여 보호관리 활동을 수행하며, 도출된 정보보호 대책을 기반으로 관리하는 일이다.
	정보보호엔지니어링	정보서비스의 보안 요구사항에 따라 정보보안 시스템 설치를 위한 설계, 구축, 유지보수를 수행하는 일이다.
	보안품질관리	정보보호 품질관리를 위하여 전사적인 보안대책을 수립하고 제품 등의 품질보증을 위한 시험 분석, 테스트케이스 작성, 시험 수행 및 보고서를 작성하는 일이다.
	영상정보보안	영상정보의 수집, 저장, 반출, 파기 등 처리 과정에서 기밀성, 무결성, 가용성을 확보하고 접근통제와 오남용 방지, 영상정보관제, 보안사고 대응 등을 수행하는 일이다.
조사·대응	보안사고대응	보안사고의 피해확산 방지를 위해 위협정보를 수집, 탐지 및 분석하여 침해사고에 대응하며 정보시스템을 복구하는 일이다.
	보안관제	원격이나 파견 통합 보안관제센터의 시스템, 조직, 역할을 설계하고, 사업목적에 따라 침해사고를 예방하고 대응하는 보안관제센터(SOC)를 구축, 운영, 관리하는 일이다.
	디지털포렌식	디지털기기에서 발생된 특정 행위의 사실 관계를 규명하고, 추후 법정에서 증거 자료로 인정될 수 있도록 요건을 갖추어 과학적 방법으로 증거물을 수집, 이동, 보존, 분석, 제출, 검증하는 일이다.
진단·평가	정보보호컨설팅	정보자산을 보호하기 위한 관리적, 물리적, 기술적 영역의 보안 요구사항 및 프로세스를 객관적으로 분석하여 모의해킹, 취약점 점검 등을 통해 개선 방안을 제안하는 일이다.
	보안감사	정보보호를 위한 관련 법, 제도, 정책, 역할, 가이드라인, 규범, 기술표준 등을 준수하도록 지속적으로 통제하고 관리하는 일이다.
	보안감리	정보보호의 효율성과 효과성을 향상시키고 안전성을 확보하기 위하여 제3자의 관점에서 정보보호의 정책 및 기획, 정보시스템 구축 및 운영 등에 관한 사항을 종합적으로 점검하고 문제점이 개선 되도록 시정조치사항을 도출하고 확인하는 일이다.
	보안인증평가	정보보호 제품에 대한 신뢰성 확보와 제품경쟁력 강화를 위하여 정보보호 제품에 대한 보안 요구사항과 보증 요구사항의 적합성 여부를 인증하거나 인증취득을 준비하는 일이다.
신기술보안	클라우드보안관리운영	조직이 클라우드 인프라를 안전하게 활용하기 위하여 정보보호 정책을 기획하며, 이에 따른 보안 운영 업무를 수행하고, 감사를 통해 조직의 클라우드 정보보호 거버넌스를 구현하는 일이다.
	모빌리티보안	모빌리티의 안전한 활용을 위하여 모빌리티 생명주기 전 단계에 걸쳐 보안위협과 위험을 식별하고, 정보보호 조직 구성, 전략과 정책 수립, 법령 준수, 보안성 검증 활동과 대응방안의 수립, 적용, 평가, 인증을 통하여, 모빌리티의 안정성을 확보하는 일이다.
	OT보안	OT환경의 시스템 및 네트워크에 대한 사이버 안전성을 확보하기 위하여 OT보안 체계를 구축하기 위한 개발, 운영, 평가와 위협 및 사고대응 업무를 수행하는 일이다.
기타	기술영업	정보보호 지식을 바탕으로 고객 관리 및 영업 전략 수립과 사업기회를 창출하고 요구사항에 적합한 솔루션제안으로 협약, 계약, 판매, 사후관리를 수행하는 일이다.
	마케팅/홍보	브랜드 인지도와 시장 경쟁력 강화에 기여하기 위한 정보보호 솔루션 마케팅전략을 설계하고 대내외 소통을 통한고객 유지관리와 신규시장을 개척하는 일이다.
	정보보호교육	정보보호 분야의 기술교육을 수행하기 위하여 교육 환경을 조성하며, 교육과정 개발 및 성과 평가를 수행하는 일이다.

C-1. 위와 같은 정보보호산업 직무 구분이 얼마나 적절하다고 생각하십니까?

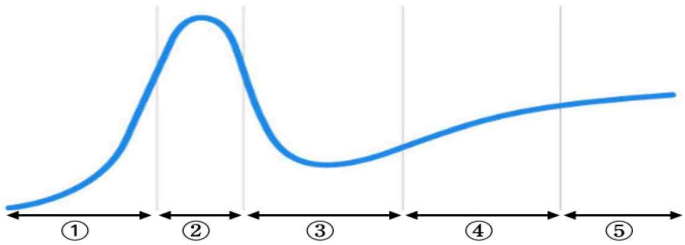
구 분	적절함	· · ·			적절하지 않음
적절성	①	②	③	④	⑤

C-2. (C-1 ③~⑤ 응답자만) 직무가 적절하지 않다고 생각하는 이유는 무엇입니까?

① 직무내용이 현실을 잘 반영하지 못해서
② 직무 단위가 대기업 중심으로 되어 있어서
③ 과거의 직무로 현재와 달라서
④ 직무내용이 지나치게 분절되어 있어서
⑤ 직무내용이 지나치게 통합되어 있어서
⑥ 기타( )

C-3. 다음 직무에 대해 현재 산업 내 성숙도를 선택하여 주십시오.

[참고] 가트너의 하이프 사이클



단계		특징
1	촉발	· 잠재적 기술이 관심을 받기 시작하는 시기이며, 초기 단계의 개념적 모델과 미디어의 관심이 대중의 관심을 불러일으킨다. · 상용화된 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다. → 해당 업무에 대한 관심이 높아지기 시작하여, 직무의 수요가 예상되는 단계
2	기대	· 초기의 대중성이 일부의 성공적 사례와 다수의 실패 사례를 양산해 낸다. · 일부 기업이 실제 사업에 착수하지만, 대부분의 기업들은 관망한다. → 해당 업무에 대한 관심이 매우 높아져, 직무 종사자가 나타나기 시작하는 단계
3	환멸	· 실험 및 구현이 결과물을 내놓지만 실패함에 따라 관심이 시들해진다. · 제품화를 시도한 주체들은 포기하거나 실패한다. · 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속된다. → 해당 업무에 대한 관심이 시들해짐에 따라, 일부 회사에서만 직무 담당자를 지정하는 단계
4	계몽	· 기술의 수익 모델을 보여 주는 좋은 사례들이 늘어나고 더 잘 이해되기 시작한다. · 2-3세대 제품들이 출시된다. · 더 많은 기업들이 사업에 투자하기 시작한다. · 보수적인 기업들은 여전히 유보적인 입장을 취한다. → 해당 업무가 인정받기 시작하여, 다수의 회사에서 직무 담당자를 보유하기 시작하는 단계
5	안정	· 기술이 시장의 주류로 자리 잡기 시작한다. · 사업자의 생존 가능성을 평가하기 위한 기준이 명확해진다. · 시장에서 성과를 거두기 시작한다. → 해당 업무가 자리 잡기 시작함에 따라, 다수의 회사에서 직무 담당자를 안정적으로 보유하는 단계

구분	직 무	촉발	기대	환멸	계몽	안정
연구·개발	정보보호기획	①	②	③	④	⑤
	정보보호개발	①	②	③	④	⑤
운영·관리	정보보호운영/관리	①	②	③	④	⑤
	정보보호엔지니어링	①	②	③	④	⑤
	보안품질관리	①	②	③	④	⑤
	영상정보보안	①	②	③	④	⑤
조사·대응	보안사고대응	①	②	③	④	⑤
	보안관제	①	②	③	④	⑤
	디지털포렌식	①	②	③	④	⑤
진단·평가	정보보호컨설팅	①	②	③	④	⑤
	보안감사	①	②	③	④	⑤
	보안감리	①	②	③	④	⑤
	보안인증평가	①	②	③	④	⑤
신기술보안	클라우드보안관리운영	①	②	③	④	⑤
	모빌리티보안	①	②	③	④	⑤
	OT보안	①	②	③	④	⑤
기타	기술영업	①	②	③	④	⑤
	마케팅/홍보	①	②	③	④	⑤
	정보보호교육	①	②	③	④	⑤

C-4. 정보보호산업 성장에 가장 큰 영향력을 미치는 직무는 무엇이라고 생각하십니까?

1순위 : _____ 2순위 : _____ 3순위 : _____

① 연구·개발(정보보호기획, 정보보호개발 등)
② 운영·관리(정보보호운영/관리, 정보보호엔지니어링, 보안품질관리, 영상정보보안 등)
③ 조사·대응(보안사고대응, 보안관제, 디지털포렌식 등)
④ 진단·평가(정보보호컨설팅, 보안감사, 보안감리, 보안인증평가 등)
⑤ 신기술보안(클라우드보안관리운영, 모빌리티보안, OT보안 등)
⑥ 기타(기술영업, 마케팅/홍보, 정보보호교육 등)

C-5. 다음 문항에 대해 지난 3년간의 전체적인 직무 변화도를 선택하여 주십시오.

구분	직 무	전혀 달라지지 않음	···			완전히 달라짐
연구·개발	정보보호기획	①	②	③	④	⑤
	정보보호개발	①	②	③	④	⑤
운영·관리	정보보호운영/관리	①	②	③	④	⑤
	정보보호엔지니어링	①	②	③	④	⑤
	보안품질관리	①	②	③	④	⑤
	영상정보보안	①	②	③	④	⑤
조사·대응	보안사고대응	①	②	③	④	⑤
	보안관제	①	②	③	④	⑤
	디지털포렌식	①	②	③	④	⑤
진단·평가	정보보호컨설팅	①	②	③	④	⑤
	보안감사	①	②	③	④	⑤
	보안감리	①	②	③	④	⑤
	보안인증평가	①	②	③	④	⑤
신기술보안	클라우드보안관리운영	①	②	③	④	⑤
	모빌리티보안	①	②	③	④	⑤
	OT보안	①	②	③	④	⑤
기타	기술영업	①	②	③	④	⑤
	마케팅/홍보	①	②	③	④	⑤
	정보보호교육	①	②	③	④	⑤

C-6. (C-5 ②~⑤ 응답자 중, 해당 직무에만 응답) 각 직무별 변화 요인은 무엇이라고 생각하십니까? (복수선택 가능)

구분	직 무	기술혁신	법·제도 변화	인력변화	시장환경 변화	업무환경 변화
연구·개발	정보보호기획	①	②	③	④	⑤
	정보보호개발	①	②	③	④	⑤
운영·관리	정보보호운영/관리	①	②	③	④	⑤
	정보보호엔지니어링	①	②	③	④	⑤
	보안품질관리	①	②	③	④	⑤
	영상정보보안	①	②	③	④	⑤
조사·대응	보안사고대응	①	②	③	④	⑤
	보안관제	①	②	③	④	⑤
	디지털포렌식	①	②	③	④	⑤
진단·평가	정보보호컨설팅	①	②	③	④	⑤
	보안감사	①	②	③	④	⑤
	보안감리	①	②	③	④	⑤
	보안인증평가	①	②	③	④	⑤
신기술 보안	클라우드보안관리운영	①	②	③	④	⑤
	모빌리티보안	①	②	③	④	⑤
	OT보안	①	②	③	④	⑤
기타	기술영업	①	②	③	④	⑤
	마케팅/홍보	①	②	③	④	⑤
	정보보호교육	①	②	③	④	⑤

C-7. C-6 응답 이외의 각 직무별 기타 변화 요인이 있다면 무엇입니까? (해당 직무에만 응답)

직 무	기타 요인

C-8. 다음 직무에 대해 전체 인력의 수준을 범위로 선택하여 주십시오.
(귀사에서 수행하는 직무만 선택하여 응답 / 예시 : 정보보호 기획 ④~⑧)

구분	직 무	1	2	3	4	5	6	7	8
연구·개발	정보보호기획	①	②	③	④	⑤	⑥	⑦	⑧
	정보보호개발	①	②	③	④	⑤	⑥	⑦	⑧
운영·관리	정보보호운영/관리	①	②	③	④	⑤	⑥	⑦	⑧
	정보보호엔지니어링	①	②	③	④	⑤	⑥	⑦	⑧
	보안품질관리	①	②	③	④	⑤	⑥	⑦	⑧
	영상정보보안	①	②	③	④	⑤	⑥	⑦	⑧
조사·대응	보안사고대응	①	②	③	④	⑤	⑥	⑦	⑧
	보안관제	①	②	③	④	⑤	⑥	⑦	⑧
	디지털포렌식	①	②	③	④	⑤	⑥	⑦	⑧
진단·평가	정보보호컨설팅	①	②	③	④	⑤	⑥	⑦	⑧
	보안감사	①	②	③	④	⑤	⑥	⑦	⑧
	보안감리	①	②	③	④	⑤	⑥	⑦	⑧
	보안인증평가	①	②	③	④	⑤	⑥	⑦	⑧
신기술보안	클라우드보안관리운영	①	②	③	④	⑤	⑥	⑦	⑧
	모빌리티보안	①	②	③	④	⑤	⑥	⑦	⑧
	OT보안	①	②	③	④	⑤	⑥	⑦	⑧
기타	기술영업	①	②	③	④	⑤	⑥	⑦	⑧
	마케팅/홍보	①	②	③	④	⑤	⑥	⑦	⑧
	정보보호교육	①	②	③	④	⑤	⑥	⑦	⑧

[참고] 수준별 특징

수준	특징	수준	특징
1	· 단순하고 반복적인 과업 수행	5	· 경력 : 약 11년~14년 (4수준 + 1~3년) · 매우 복잡하고 비일상적인 과업 수행 · 타인에게 지식 전달 가능
2	· 경력 : 약 1년 (1수준 + 6개월~12개월) · 절차화되고 일상적인 과업 수행	6	· 경력 : 약 15년~17년 (5수준 + 1~3년) · 다양한 과업 수행 · 타인에게 지식 및 노하우 전달 가능
3	· 경력 : 약 2~5년 (2수준 + 1~3년) · 다소 복잡한 과업 수행	7	· 경력 : 약 19년~21년 (6수준 + 2~4년) · 광범위한 작업 수행 · 타인의 결과에 대한 의무 및 책임
4	· 경력 : 약 6~10년 (3수준 + 1~4년) · 복잡하고 다양한 과업 수행	8	· 경력 : 약 23년~25년 (7수준 + 2~4년) · 광범위한 기술적 작업 수행 · 조직 및 업무 전반에 대한 권한 및 책임

C-9. 다음 문항에 대해 향후 3년 이내 직무 전망을 선택하여 주십시오.

구분	직 무	매우 비유망	비유망	보통	유망	매우 유망
연구·개발	정보보호기획	①	②	③	④	⑤
	정보보호개발	①	②	③	④	⑤
운영·관리	정보보호운영/관리	①	②	③	④	⑤
	정보보호엔지니어링	①	②	③	④	⑤
	보안품질관리	①	②	③	④	⑤
	영상정보보안	①	②	③	④	⑤
조사·대응	보안사고대응	①	②	③	④	⑤
	보안관제	①	②	③	④	⑤
	디지털포렌식	①	②	③	④	⑤
진단·평가	정보보호컨설팅	①	②	③	④	⑤
	보안감사	①	②	③	④	⑤
	보안감리	①	②	③	④	⑤
	보안인증평가	①	②	③	④	⑤
신기술 보안	클라우드보안관리운영	①	②	③	④	⑤
	모빌리티보안	①	②	③	④	⑤
	OT보안	①	②	③	④	⑤
기타	기술영업	①	②	③	④	⑤
	마케팅/홍보	①	②	③	④	⑤
	정보보호교육	①	②	③	④	⑤

C-10. 현재 구분된 직무 외에 새롭게 생겨난 직무(신생직무)나 사라진 직무(소멸직무), 통합·분할 등 대체되고 있는 직무(대체직무)가 있다면 관련하여 자유롭게 작성하여 주시기 바랍니다.

구분	직 무
신생직무	
소멸직무	
대체직무	

D. 정보보호 분야의 직무구분 및 정의, 직무변화 요인, 직무변화 양상 등 직무 및 직무변화와 관련하여 기타의견이 있으면 자유롭게 작성하여 주시기 바랍니다.

구분	의 견
기타의견	

2024 정보보호산업 직무변화 모니터링 보고서

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〉

2024

정보보호산업 직무변화 모니터링 보고서