정보보호론
오리엔테이션

박종혁 교수

(서울과학기술대학교, 컴퓨터공학과)
Email: jhpark1@seoultech.ac.kr

1. 교과목 소개

2. 평가 방법

3. 강의 계획

4. 정보보호 산업, 기관 및 자격증

5. 정보보안 전문가 직군

1. 교과목 소개

1.1 담당교수

1.2 교과목

1.3 교과목 개요

1.4 학습 목표

1.5 수업 교재

1.1 담당교수 소개

박종혁 교수 (Jong Hyuk Park)

- 최종학위: 공학박사 (정보보안)
- 주 연구분야: 컴퓨터보안, IoT 및 클라우드 보안, 양자정보 보안, 인공지능 보안, 블록체인
- 교수연구실: 미래관 325호
- 홈페이지: http://www.parkjonghyuk.net
- 담당 대학원연구실: UCS Lab (컴퓨터보안)
  https://ucs.seoultech.ac.kr

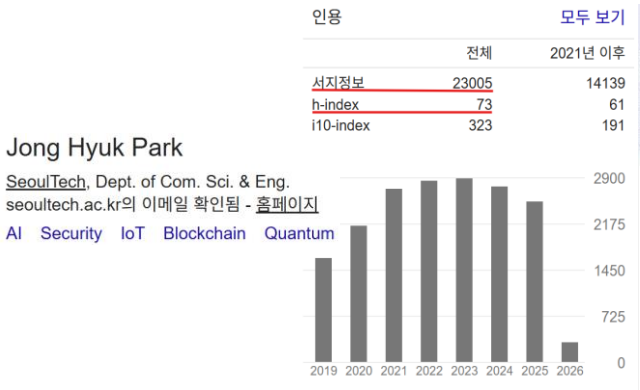
- 대표 약력

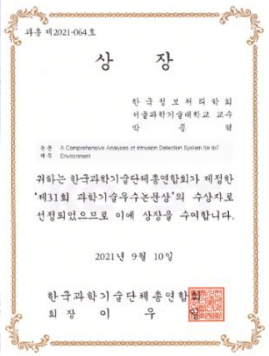
연도	기관명	업무	직위
2009.9 ~ 현재	서울과학기술대학교 컴퓨터공학과	교육 및 연구	교수
2002.12 ~ 2007.7	한화에스앤씨㈜ 기술연구소	선임연구원	연구
2011.1 ~ 현재	국제 HCIS 논문지 (세계 저명저널)	총괄편집위원장	편집위원장

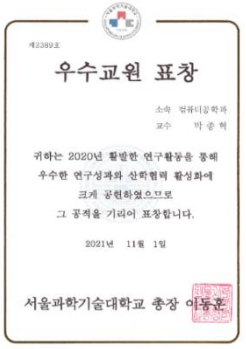
- 서울과기대 최우수 연구교수 선정 (5년 연속)
- 세계 상위 2% 과학자 선정 – 스탠포드 대학 (5년 연속)

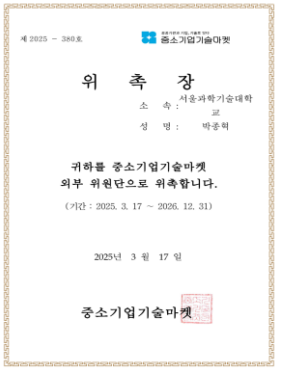
❖ 박종혁교수 세부 이력 (요약)

- 서울과학기술대학교 글로벌양자AI보안연구소(GQAS) 연구소장
- 한국연구재단, 한국전자통신연구원, 미래창조과학부, 국가보안연구소 등 국가 R&D기관의 ICT 보안 및 응용 연구 과제 다수 수행
- IEEE AINA, CUTE, 한국정보처리학회 학술대회 등 국내외 학술대회우수 논문상 다수 수상
- Information Fusion, IEEE TII, JNCA 등 세계 최상위 5% 저널 논문 포함 최신 ICT 융합보안 관련 약 500편의 SCI 논문 연구성과 보유 (JCR 상위 25% 저널 약 50편 이상)
- 구글 스칼라 기준 인용횟수 23,005회 (h-index 73회, i10-index 323회)로 정보보호 및 ICT 분야의 세계적인 파급효과
- 다수의 국제 컨퍼런스 운영위원장, SCI 및 SCOPUS급 저널 EiC 등 국제 학술회의 활동을 통한 국제 교류 및 협업 능력 입증
- 최근 3년간 국제 특허 포함 퀀텀, AI, 보안 등 사이버 보안 관련 10여건 특허 출원 및 등록









1.2 교과목 소개

교과목 명	정보보호론 (Information Protection Theory)
교과 구분	전공 선택 (3학점)
강의 시간	월 2,3,4 교시 (미래관 107호)
강의 구성	이론 (3)
강의 방법	대면 (보강: 온라인 강의영상)

- 1~14주차
- 8 주차: 중간고사
- 15 주차: 기말고사
- 14 주차: 과제 2 발표 수업 (희망자 최대 10명)

1.3 교과목 개요

- 정보 (Information)에 대한 훼손, 변조, 유출 등 공격 위협이 점차적으로 증가하고 있으며, 이를 방지하기 위한 대책이 필요함
- 최근 바이러스 및 악성코드 침투, 해킹 등 여러 가지 보안 이슈들이 사회적으로 자주 발생하고 있으며 이러한 보안 이슈들을 예방하기 위한 정보보호 기술이 필수적임
- 본 교과목에서는 정보보호의 개념과 기술 등 기본적인 이론부터 실생활에 필요한 응용기술까지 현대 암호와 함께 정보보호의 전반적인 이론 및 기초 지식에 대해 학습함

정보보호 필요성

[시청]

- 해킹과 보안기술의 발전, 우리의 정보는 과연 안전한가**?** - 애쓰디애쓴 지식영상
- 사이버 보안이 중요한 5가지 이유!– 위드네트웍스
- '보안 참사' 얼룩진 2025년…SKT부터 쿠팡까지 **- KBS**
- 털릴 수밖에 없었던 KT 보안, "문자·통화 빼낼 만큼 허술" - JTBC 뉴스룸
- "무료 충전·와이파이 썼다가 털려"…스마트폰 해킹 주의보 [지금이뉴스] - YTN

[기타 참고영상]

- 스마트 시대의 사이버 보안 : 인공지능과 보안이 만나면 **? – KIRD**
- 정보보안전문가는 해킹도 잘할까**?** 정보보안전문가 **Q&A (w.**스틸리언 **CTO)**
- 편하다고 '자동 로그인'**?…**'비밀번호' **8**백만 개 유출 **- KBS**
- **'챗GPT'**로 **IP** 카메라 해킹**?** 실제로 해 봤더니 결과 **'**충격**' - KBS**
- 나를 유혹하는 디지털 악마들 [개인정보] – 금융감독원
- 나라를 뒤흔들었던 해킹 사건들 **- YTN** 사이언스
- [비대면 사회의 정보보호] 주소지 오류**?** 본인인증 재요청 한다면**! –** 과기정통부

1.4 학습 교재

- 주 교재

  알기 쉬운 정보보호 개론, 히로시 유키 지음 (이재광 외 2 공역), 인피니티북스, 2017

- 보조 교재
  - 정보보안 이론과 실제 (마크 스탬프 저/김경곤역, 한빛아카데미, 2023년 08월) 등 정보보호 도서
  - 최근 정보보호 이슈 사항, 컨퍼런스/워크숍 등 저명 학자/연구자 발표자료
  - 저명 저널 및 매거진 출판 논문
  - 인터넷 미디어 등

2. 평가 방법 및 과제물

2.1 학습평가 방법

2.2 과제물 설명

2.1 학습평가 방법

- 출석 (10%), 과제물 (20%), 중간고사 (30%), 기말고사 (30%), 기타 (10%)*
- 기타: 수강생의 수업태도 (발표, 과제 등)에 대한 가산점 부여
- 정기 과제물 양식 철저히 지킬 것
  - 홈페이지 공고된 양식만 사용 (Pls. do not use non-official format !!)
- 과제물 작성시 Chat GPT 등 AI 툴 사용 금지
  - 사용 확인시 0점 처리!!

2.2 과제물 설명

과제 #1

- 최신 암호응용 / 정보보호 관련 인터넷 및 자료조사 등을 통해 기술 동향 보고서 작성하여 기한 내 E-class에 업로드한다.
  (8주차 중간고사 전일 23시 까지)

과제 #2 :

- 개인과제 #1을 기반으로 정보보호 아이디어 제안 보고서 및 발표 자료를 제작하여 기한 내 E-Class에 업로드 한다.
  (14주차 수업 전일 23시 까지)

** 과제 양식을 꼭 사용하여 작성할 것 (다른 양식 사용시 감점)

** Copy Killer 검사 결과 꼭 제출할 것

기타 발표 : (14주차 수업 시)

* 희망자 선착순 최대 10명
  - 개인과제 #2 관련 내용 발표 (10분) ← 기타 점수 추가점 부여!!
  - 희망자는 조교선생님한테 3/20일까지 메일을 보내세요
    (정보보호론 조교, fgds8@seoultech.ac.kr)

과제 제출 관련 중요사항!!

도서관 표절 검사기 (Copykiller) 활용

– 각 과제 보고서를 도서관의 표절검사기로 유사율을 검사하여 함께 제출 해야 함 (유사율이 높을 경우, 표절로 판정함)

Copy Killer CAMPUS 서울과학기술대학교 https://seoultech.copykiller.com

- 최근 전세계적으로 문서(레포트, 논문 등)에 관한 유사도를 확인하고 있으며, 연구 윤리 측면에서 심각한 문제로 대두됨
- 우리 수업에서도 **표절률** 이용 감산제를 적용함

- 유사도 검사 결과 표절율이 30% 이상인 학생에게 패널티를 부여함
  – 과제점수 * 표절율 감점 적용

- 예) 과제점수 7점, 표절율 40%
  – 패널티 점수 =3점
  – 과제점수 (7) * 표절율 (40%) = 2.8 (3점 적용)
  – 최종 과제 점수 = 기본점수 (7) – 패널티 점수 (3점) = 4점

- 표절률이 60% 이상인 보고서는 완전 표절로 판단 "0점"을 부여함

3.강의 계획

3.1 주차별 강의 운용 계획

3.2 강의 내용 간단 소개

3.1 주차별 강의 운용 계획

주별	날짜	강의내용	강의방법, 과제, 평가내용	비고	보강일
1	3/9	오리엔테이션 및 교과목 개요 1장 정보보호	강의 개요 소개 및 이론강의		
2	3/16	2장 암호의 세계	이론강의		
3	3/23	3장 암호의 역사	이론강의		
4	3/30	4장 대칭 암호	이론강의		
5	4/6	5장 블록 암호 모드	이론강의		
6	4/13	6장 공개 키 암호	이론강의		
7	4/20	7장 하이브리드 암호 시스템	이론강의		
8	4/27	중간고사	필기시험	* 과제 1 제출기한: 4/26 23시	

주별	날짜	강의내용	강의방법, 과제, 평가내용	비고	보강일
9	5/4	8장 일방향 해시 함수	이론강의		
10	5/11	9장 메시지 인증 코드	이론강의		
11	5/18	10장 디지털 서명	이론강의		
12	5/25	11장 인증서	공식 휴강 (공휴일)	부처님 오신 날 대체 휴일	온라인 강의
13	6/1	12장 키 13장 난수	이론강의		
14	6/8	1. 최신 정보보호 동향 2. 수강생 희망자 발표	이론강의	* 과제 2 제출기한: 6/7, 23시	
15	6/15	기말고사	필기시험		

3학년 정보보안 관련 과목

학기	과목명	주요 내용
1	정보보호론	• 암호학 / 정보보호 기초 이론 ✓ 암호시스템 DES, AES, RSA ✓ 해쉬함수, 메시지인증코드 ✓ 디지털서명, 인증서 ✓ 키, 난수 ✓ 개인정보보호, IoT보안 등
2	컴퓨터보안	• 정보보호 응용 및 네트워크/ 시스템 보안 ✓ 사용자 인증, 접근제어 ✓ 데이터베이스와 클라우드 보안 ✓ 악성코드 ✓ 네트워크 보안, 시스템 보안 ✓ 디지털 포렌식, 보안관리

3.2 강의 내용 간단 소개

1장. 정보보호

1절 네트워크 사회와 정보보호

2절 정보보호란?

3절 정보의 특성

4절 정보보호의 인적 요소

2장 암호의 세계

3장 암호의 역사

1절 시저 암호

2절 단일 치환 암호

3절 다중 치환 암호

4절 에니그마

5절 전치 암호와 치환 암호

6절 암호 알고리즘과 키

4장 대칭 암호

1절 문자 암호에서 비트열 암호로

2절 일회용 패드-절대 해독 불가능한 암호

3절 DES란?

4절 트리플 DES

5절 AES 선정 과정

6절 Rijndael

5장 대칭 암호(공통 키 암호)

1절 블록 암호 모드

2절 ECB 모드

3절 CBC 모드

4절 CFB 모드

5절 OFB 모드

6절 CTR 모드

7절 모드 선택

6장 공개 키 암호

1절 키 배송 문제

2절 공개 키 암호

3절 정수론

4절 RSA

5절 RSA에 대한 공격

6절 다른 공개키 암호

7절 공개 키 암호에 관한 Q&A

7장 하이브리드 암호 시스템

1절 하이브리드 암호 시스템

2절 강한 하이브리드 암호 시스템이란

3절 암호 기술의 조합

8장 일방향 해시 함수

1절 일방향 해시 함수

2절 일방향 해시 함수의 응용 예

3절 일방향 해시 함수의 예

4절 일방향 해시 함수 SHA-1

5절 일방향 해시 함수 SHA-512

6절 일방향 해시 함수에 대한 공격

7절 어떤 일방향 해시 함수를 사용하면 좋은가?

8절 일방향 해시 함수로 해결할 수 없는 문제

9장 메시지 인증 코드

1절 메시지 인증 코드

2절 메시지 인증 코드 이용 예

3절 메시지 인증 코드의 실현 방법

4절 인증암호

5절 HMAC

6절 메시지 인증 코드에 대한 공격

7절 메시지 인증 코드로 해결할 수 없는 문제

10장 디지털 서명

1절 디지털 서명

2절 디지털 서명 방법

3절 디지털 서명에 대한 의문

4절 디지털 서명 활용 예

5절 RSA에 의한 디지털 서명

6절 다른 디지털 서명

7절 디지털 서명에 대한 공격

8절 기타 기술과의 비교

9절 디지털 서명으로 해결할 수 없는 문제

11장 인증서

1절 인증서

2절 인증서 만들기

3절 공개 키 기반 구조 (PKI)

4절 인증서에 대한 공격

5절 인증서에 대한 Q&A

12장 키

1절 키란 무엇인가?

2절 다양한 키

3절 컨텐츠를 암호화하는 키와 키를 암호화 하는 키

4절 키 관리

5절 Diffie-Hellman 키 교환

6절 패스워드를 기초로 한 암호(PBE)

7절 안전한 패스워드를 만들려면

13장 난수

1절 난수가 사용되는 암호 기술

2절 난수의 성질

3절 의사난수 생성기

4절 구체적 의사난수 생성기

5절 의사난수 생성기에 대한 공격

14장-1 개인정보보호

1절 개인정보 보호 이해

2절 개인정보 보호 원칙

3절 정보보호 법규 및 제도

4절 개인정보 보호법 개정안

14장-2 IoT 보안

1절 사물인터넷 개요

2절 사물인터넷 보안위협과 고려사항

3절 사물인터넷 보안

16장 암호기술과 현실 세계

1절 암호 기술의 정리

2절 완전한 암호 기술을 꿈꾸며

3절 완전한 암호 기술과 불완전한 인간

4. 정보보호 산업, 기관 및 자격증

- 정보보호 산업 : 범위

정보보안	물리보안	융합보안
		
해킹/침입탐지, 개인정보유출방지 컴퓨터포렌식 등	영상감시, 바이오인식, 무인전자경비 등	운송보안(자동차/항공 등) /의료/건설/국방 보안 방법보안로봇 등
정보보안(클린인터넷경제)	물리보안(안전안심생활)	융합보안(안전성강화)

- 정보보호산업 – 정보보안 / 물리보안 제품 및 서비스 분류

대분류	중분류
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

대분류	중분류
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

- 정부 및 공공기관

기관 이름	관련 업무
국가정보원 (NIS)	국가 차원의 사이버 안보, 정보 보호
과학기술정보통신부	사이버 보안 정책 수립 및 사이버 방어 대응
국방부 사이버사령부	군사적 사이버 공격 대응 및 방어
행정안전부	국가 사이버 보안 정책 및 공공부문 보안 지원
방송통신위원회	통신 및 방송 관련 법률, 규제 관리
한국전자통신연구소(ETRI)	정보통신 및 보안 기술 연구 개발
한국인터넷진흥원 (KISA)	사이버 보안 관리, 취약점 점검 및 보안 교육
국가보안연구소(NSR)	국가 차원의 정보 보호 및 보안 기술 연구
경찰청 포렌식센터	디지털 증거 수집 및 분석, 사건 수사 지원
검찰청 포렌식센터	디지털 증거 분석, 법적 증거 제공
금융보안원	금융 시스템의 보안 강화 및 데이터 보호
사이버범죄수사대	사이버 범죄 수사 및 범죄 대응
금융결재원	금융 거래 보안, 전자 결제 시스템 보안 관리

- 자격증

자격증명	시험 주관 기관	개요	가점 부여 기관
CISSP (Certified Information Systems Security	(ISC)²	정보보호 및 보안 전문가로서의 권위 있는 국제 인증.보안 전반에 걸친 전문 지식 평가	정부:국가정보원, KISA 등 공공기관:공공기관의 IT보안 부서 대기업 및 IT기업(삼성, LG, SK등)
CISA (Certified Information Systems Auditor)	ISACA	정보시스템 감사와 관련된 지식을 평가하며,시스템의 안전성과 감사 능력을 인증	정부:KISA,금융위원회 등 공공기관:공공기관의 감사부서,국가기관의IT 감사 부서 사설 기업:금융기관,감사 관련 기업 등
정보보호기사	한국인터넷진흥원 (KISA)	정보보호 분야에서의 전문성을 평가하는 국가자격증.보안 정책,기술,관리 등 다양한 분야 포함.	정부:KISA,,경찰청,국방부 등 공공기관:모든 정부 및 지방자치단체 IT부서 사설 기업:대기업, IT기업 등
디지털 포렌식 기사	(사)한국포렌식학회, KISA	디지털 포렌식 및 사이버 범죄 수사 관련 전문 지식과 기술을 평가하는 국가자격증인증.	정부:경찰청, KISA, 공수처 등 공공기관:경찰청 사이버 범죄 수사 부서 사설 기업:보사이버 보안, 디지털 포렌식 전문 기업 및 로펌
CISM (Certified Information Security Manager)	ISACA	정보보안 관리 전문가로서의 인증.보안 프로그램 관리 및 리스크 관리를 위한 지식 평가.	정부:국방부,국가정보원, KISA 등 공공기관:공공기관의 보안 및 IT관리 부서 사설 기업:대기업, IT기업,금융기관,보안 관련 기업
CEH (Certified Ethical Hacker)	EC-Council	윤리적 해킹 및 사이버 공격 대응 능력 평가.취약점 분석과 보안 테스트 수행 능력 인증.	정부:경찰청,국방부,KISA 등 공공기관:공공기관의 보안 부서 사설 기업:보안 전문 기업,대기업IT부서,금융기관,사이버 보안 업체

5.정보보안 전문가 직군

5.1 정보보안의 중요성

5.2 정보보안 전문가 직군

5.3 직군별 핵심 업무 및 산출물

5.4 현업 조직에서의 배치 예시

5.5 최근 3년 보안 직무 변화

5.1 정보보안의 중요성

최근 3년 보안 트렌드 = 서비스 연속성 + 개인정보 + 신뢰

- **사례 1) 통신 인프라 보안 이슈 — SK Telecom 이상 트래픽 사건(2025)**
  - 대규모 이상 트래픽 탐지 후 KISA에 신고, 정부가 최종 조사 결과를 공개하며 **통신 인프라 보안의 중요성**을 강조

- **사례 2) 개인정보 유출 — LG U+ 고객정보 유출 제재(2023)**
  - 개인정보보호위원회(PIPC)가 보안 미흡에 따른 제재(과징금 등)를 발표
    → "개인정보 보호 실패 = 법·규제 리스크 + 신뢰 하락"

- **사례 3) '보안 업데이트'가 대규모 장애로 — CrowdStrike IT 대란(2024)**
  - 보안 제품 업데이트 오류로 Windows 대규모 장애 → 항공/병원 등 **핵심 서비스 중단**까지 확산
  - "해킹이 아니어도" 사이버 복원력(Resilience)이 중요하다는 걸 보여줌

- **사례 4) 랜섬웨어 — Change Healthcare 공격(2024)**
  - 의료 결제·처방 등 의료 서비스에 영향을 준 대형 사고로, 미 보건당국(HHS)이 **조사/가이드**를 공개

이 사례들의 공통점(핵심 메시지)

✓ 보안 사고는 **돈(금전피해)**만이 아니라 **서비스 마비(가용성)**와 **개인정보(규제), 사회 인프라 신뢰**까지 흔든다.
✓ 그래서 보안은 "**개발/운영/정책/대응**"을 함께 보는 조직 역량이다.

5.2 정보보안 전문가 직군

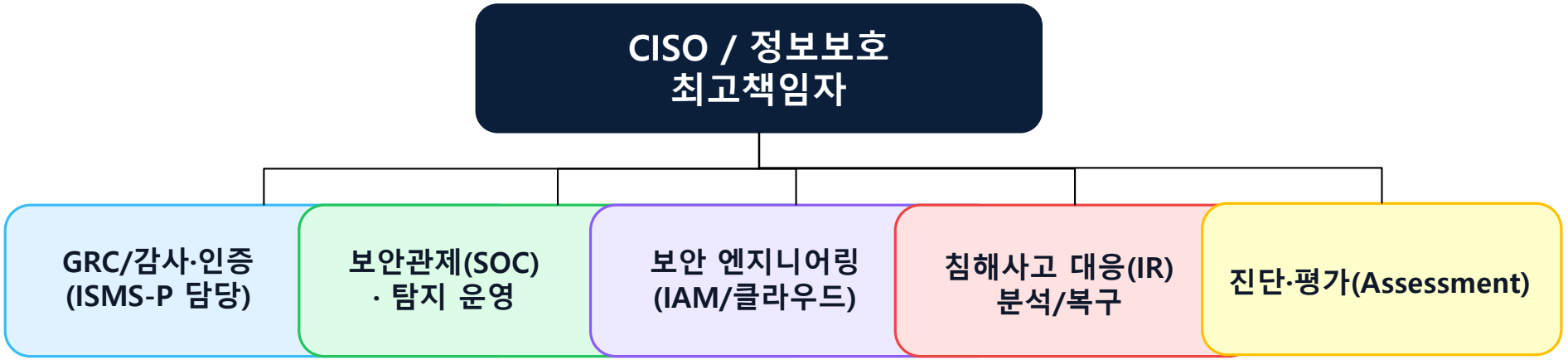
- ✓ 정보보안 직군은 **예방(Prevent)–탐지(Detect)–대응(Respond)–복구(Recover)** 전 주기를 담당
- ✓ 업무는 크게 **거버넌스/관리**, **보안 운영**, **진단/평가**, **대응/조사**, **보안 엔지니어링/개발**로 나뉨
- ✓ 조직 규모가 커질수록 **전문화**, 작을수록 **겸임**이 많음

➢ 정보보안 전문가 직군 맵

5.3 직군별 핵심 업무 및 산출물

직군	주요 업무	대표 산출물 (Deliverables)	주로 쓰는 도구 및 기술	신입이 먼저 하는 일
GRC / 보안관리	정책/규정 수립 및 운영, 위험평가, ISMS-P 대응	보안정책 관련 지침, 위험평가서, 점검 결과보고서, 개선 계획서	ISMS-P/ISO 체계, 문서·프로세스 관리, 자산/위험관리 툴	자산목록 정리, 점검 체크리스트 운영, 증적 수집/정리
SOC / 관제(분석)	보안 이벤트 모니터링, 탐지룰 운영, 경보 분석 및 분류	경보 분석 리포트, 탐지룰, 시그니처, 티켓 처리 이력	SIEM, EDR, SOAR, 로그 분석	경보 분류(Triage), 오탐/정탐 분류, 티켓 처리/에스컬레이션
취약점 / 모의해킹	취약점 진단, 침투 테스트, 재현(PoC) 및 개선 권고	진단보고서, PoC(재현 자료), 재현 절차, 재점검 결과	Burp Suite, Nmap, Metasploit, 웹 보안 지식	스캐너 결과 정리, 취약점 재현 테스트, 보고서 초안 작성
침해사고 대응(IR)	사고 분석, 격리 및 차단, 복구 지원, 원인 분석	타임라인, RCA(원인분석), 재발방지 대책, 대응 플레이북 기록	로그/포렌식 도구, 대응 플레이북, 협업 티켓	초기 대응 절차 수행, 증거 보존, 상황보고 작성
디지털 포렌식(DF)	디지털 증거 수집·분석, 법적 절차 지원	증거목록(Chain of Custody), 분석보고서, 해시 검증 기록	디스크/메모리 분석 도구, 파일시스템/아티팩트 분석	이미지 획득, 해시 검증, 기본 아티팩트 (로그/브라우저 등) 수집
보안 엔지니어 / 개발	보안 설계, 보안 기능 개발, 보안 자동화 및 정책 적용	보안 아키텍처, 보안 설정/정책(IaC), 코드리뷰 결과, 자동화 스크립트	Cloud, DevSecOps, SAST/DAST, IaC(Terraform 등)	설정 점검, 정책 코드 수정 PR, CI 파이프라인 보안 점검

5.4 현업 조직에서의 배치 예시



직무	진출 분야 예시(기업/기관)
GRC(정책·감사/인증)	SK쉴더스, LG CNS 보안, 삼성 SDS 보안
SOC(관제·탐지)	SK쉴더스, 안랩, 이글루코퍼레이션
보안 엔지니어링(클라우드/IAM)	안랩, 시큐아이, 파수
IR/DF(침해사고·포렌식)	경찰청 사이버수사대, 국과수, KISA 침해사고대응센터
Assessment(진단·모의해킹)	라온시큐어, 펜타시큐리티, NSHC

5.5 최근 3년 보안 직무 변화

✓ 최근 3년간 **제로트러스트, 공급망 보안, 클라우드 / SaaS, AI** 확산으로 보안 직무가 **IAM, SBOM, 클라우드 설정 점검 및 데이터 모델 리스크 대응** 중심으로 빠르게 재편되는 중임

기술 트렌드	핵심 포인트	영향 직무	현업에서 늘어난 업무
제로트러스트	"신뢰하지 말고, 매번 검증"	GRC, 엔지니어링, SOC	접근제어(IAM), 세션/정책 기반 통제, 로그 연계
SW 공급망 보안	"코드/빌드/배포까지 보안"	AppSec, 엔지니어링, GRC	SBOM, 취약 라이브러리 관리, CI/CD 보안
클라우드·SaaS 확산	"경계가 사라짐"	엔지니어링, SOC	클라우드 설정 점검, 권한관리, CSPM
AI 활용 확산	"데이터·모델·프롬프트 리스크"	GRC, AppSec, SOC	개인정보/데이터 처리 기준, 유출 탐지, 보안 점검 강화

참고문헌

- 본 교재
- 2024 국내정보보호산업 실태조사, 한국정보보호산업협회 / 과학기술정통부
- 2025 SK텔레콤 침해사고 최종 조사결과 발표, 과학기술정보통신부
- 2023 개인정보위, ㈜엘지유플러스 개인정보 유출사고에 대해 과징금 68억 원, 과태료 2,700만 원 및 시정명령(보도자료), 개인정보보호위원회(PIPC)
- 2024 Widespread IT Outage Due to CrowdStrike Update (Alert), 미국 사이버보안 및 인프라 보안국(CISA)
- 2024 Cyberattack on Change Healthcare (Office for Civil Rights Letter), 미국 보건복지부(HHS)
- 2024 제로트러스트 가이드라인 2.0, 한국인터넷진흥원(KISA)
- 2024 SW 공급망 보안 가이드라인 1.0, 과학기술정보통신부 / 국가정보원 / 한국인터넷진흥원(KISA)
- 2025 OT 환경 제로트러스트 적용 안내서, 한국인터넷진흥원(KISA)
- 2024 개인정보보호책임자(CPO) 핸드북, 개인정보보호위원회(PIPC)
- 2024 AI 개발·서비스를 위한 공개된 개인정보 처리 안내서, 개인정보보호위원회(PIPC)
- 2024 CSK(국가 사이버안보) 정책방향(보도자료), 국가정보원(NIS)
- 2024~2025 ISMS-P 안내서/심사기준 자료, 한국인터넷진흥원(KISA) / 과학기술정보통신부

Q & A

Thank You!