

## 사이버보안학과

위치 및 연락처 : 산학협력원 210호 (☎ 219-3678)

### 학과소개

인터넷과 모바일 서비스에 기반한 소셜 네트워크 등의 발전으로 IT산업은 하드웨어 중심에서 소프트웨어 중심으로 급격하게 변화하고 있으며 이러한 산업에서의 우수한 소프트웨어 개발 인력 수요는 가히 폭발적이라고 말할 수 있다. 특히 SW개발이나 SW가 적용되는 산업 전반의 모든 시스템에서는 이제 보안성을 고려하지 않고는 그 존재 가치를 의미를 가질 수 없는 상황이다. 따라서 사이버보안 전공은 정보보안의 근원이 되는 플랫폼, 네트워크 및 서비스라는 정보통신의 종적구조를 망라하여, 보안 위협의 목표이며 대상이 되는 소프트웨어의 개발과 운영 과정을 밀도 있게 습득하고 분석함으로써 소프트웨어 생명주기에서의 보안요소들을 학습할 수 있는 교육과정을 제공하며, 현대사회에서 보안이 요구되는 어느 곳에서도 적용력을 가진 보안 기술 인력의 양성을 목표로 한다.

전공 교육은 세 단계로 구분하여 기반단계인 저학년 과정에서 정보통신의 기초적인 과목을 이론과 실습을 병행하며 철저하게 학습하여서 정보보안의 토대를 마련하고, 심층단계인 고학년 과정에 정보통신의 종적 구조상에 나타나는 소프트웨어 보안 요소들을 심도 있게 학습하고, 마지막으로 종합단계에서 기술적인 우위를 가진 전문가로서의 능력을 배양하기 위하여 전 교육과정을 통하여 습득된 지식을 종합적으로 융합하는 과목들을 이수하여 사회 각 분야에서 요구되는 능력을 골고루 배양시킨다.

이러한 체계적인 전공교육을 이수한 학생은 국내 IT관련 기업체는 물론 해외 기업체로 진출 할 수 있는 능력을 갖추 수 있으며 빠르게 변화하는 IT산업 기술에 능동적으로 대처할 수 있는 역량을 가질 수 있을 것이다.

### 교육목표

1. 사이버보안 전공 지식기반의 정보보안 응용 능력을 갖춘 전문인
2. 창의적인 사고를 바탕으로 정보보안 시스템 설계 능력을 갖춘 전문인
3. 공학도로서 기술진화를 선도하고 평생학습 능력을 갖춘 전문인
4. 미래 정보화 사회에 동참할 수 있는 인문소양을 겸비한 전문인
5. 올바른 윤리의식과 의사소통 능력을 가진 글로벌 전문인

### 졸업 후 진로

정보통신, S/W, 전자 등 IT전반에 관련된 기업에 정보보안 전문가로서 활동하거나 또는 금융, 자동차, 공공기관 등 IT가 접목된 거의 모든 기관에 보안 담당자로서 진로를 설정할 수 있다. 또한 이외에도 보안 기반지식을 바탕으로 보안 관련 기술이나 서비스를 필요로 하는 다양한 산업체에 소프트웨어 설계 및 개발자, 시스템 엔지니어, 통신 전문가 등 다양한 직종으로 진출할 수 있으며 또한 본교를 비롯한 국내외 우수한 대학원에 진학이 가능하다.

### 실험실

분산이동컴퓨팅 연구실, 인터넷 연구실, 인터넷보안 연구실, 정보보호응용 및 보증 연구실, ICS 연구실

직책	성명	전공분야	연구실	전화	보직
대우교수	홍만표	정보보호(Information Security),			
명예교수	김동규	통신보안(Computer Security)			
명예교수	유승화	컴퓨터네트워크(Computer Networks)			
교수	김기형	네트워크 보안 (Network Security) 및 블록체인 (Blockchain), IoT와 임베디드 소프트웨어(Embedded Software)	산학원 516호	2433	
교수	김재훈	분산시스템(Distributed Systems) IoT 플랫폼(IoT Platform) 사이버물리시스템(Cyber-Physical Systems)	산학원 512호	2546	
교수	예홍진	계산이론(Theory of Computation), 정보보호(Information Security)	산학원 513호	2642	학과장

직책	성명	전공분야	연구실	전화	보직
교수	곽진	정보보안(Information Security)	산학원 511호	3812	혁신융합원장, 데이터보안 활용융합 혁신융합대학 사업단장
교수	손태식	정보보호(Information security)	산학원 515호	3321	
부교수	김강석	딥러닝 응용 보안(Applied Deep Learning for Security)	산학원 514호	2496	

## 사이버보안전공

### 교육과정표

#### 1. 졸업 이수학점 및 구성 현황

가. 총 졸업 이수학점 : 128학점

나. 교육과정별 필수 이수학점 구성 현황

(※ 필수 이외의 학점은 교양선택 등으로 이수하여 총 졸업 이수학점을 충족하여야 함.)

구분	대학필수 (소계:26)							BSM (소계:10)		전공기초 (소계: 6)	전공	
	아주희망 전공진로탐색	아주인을 위한 마중물	아주상상 프로젝트	영어	대학 글쓰기	영역별 교양	AI 리터러시	수학	기초과학		전공필수	전공선택
사이버보안전공심화	1	1	3	3	3	12	3	6	4	6	29	24
사이버보안전공	1	1	3	3	3	12	3	6	4	6	29	12
Cloud/Bigdata 보안 트랙	1	1	3	3	3	12	3	6	4	6	트랙필수9	트랙선택6
IoT/Mobile 보안 트랙	1	1	3	3	3	12	3	6	4	6	트랙필수9	트랙선택6
복수전공	학생 소속 제1전공을 기준으로 이수							6	4	6	29	6
부전공	학생 소속 제1전공을 기준으로 이수							6	4	6	29	-

- 제1전공 전필과목 : 사이버보안입문(3), 이산수학(3), 컴퓨터프로그래밍및실습(4), 자료구조(3), 컴퓨터구조(3), 객체지향프로그래밍및실습(4), 현대암호이론및응용(3), 운영체제(3), 컴퓨터네트워크(3)
- Cloud/Bigdata 보안 트랙 필수과목 : 정보보호법과정(3), 데이터베이스(3), 사이버보안관계(3), 클라우드보안(3), 빅데이터응용및보안(3), 사이버보안사례특강(3)
- IoT/Mobile 보안 트랙 필수과목 : 정보보호법과정(3), IoT보안(3), 사이버보안관계(3), 사이버보안사례특강(3), 기계학습(3)
- 복수전공 전필과목 : (제1전공 전필과목과 상동)
- 부전공 전필과목 : (제1전공 전필과목과 상동)

#### 2. 졸업요건

- 총 졸업 이수학점 : 128 학점
- 평점 : 2.0 이상
- 외국어(영어) 공인 성적

TOEIC	TEPS	TOEFL			G-TELP		TOEIC Speaking	OPlc
		PBT	CBT	IBT	level 2	level 3		
730	329	534	200	72	67	89	Lv.5 (IM1)	IL

#### ■ 전공 이수원칙

- 전공심화 과정 이수 및 트랙(Cloud/Bigdata 보안, IoT/Mobile 보안) 선택 이수

- 전공심화 과정 미이수 시, 복수전공 또는 부전공 이수

※ 예외 : 복수학위생, 학·석사연계과정으로 본교 대학원 진학이 확정된 자

■ 기타 졸업요건 (본 전공을 제1전공 또는 복수전공으로 이수 시 필수)

- 산학프로젝트 인증 기준 : 자기주도연구 및 프로젝트 과목군 또는 캡스톤디자인과목군 중 1개 이상 선택 이수 의무 (평가는 ABCF제)
- 자기주도연구 및 프로젝트 과목군 : 자기주도연구1,2 / 자기주도프로젝트
- 캡스톤디자인과목군 : 사이버보안캡스톤디자인
- 전공 역량 인증 : 컴퓨터프로그래밍및실습 ABF

3. 교육과정

■ 일반 및 심화과정

이수구분	학수 구분	과목명		개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점수)			학점 수 합계		
				1학년		2학년		3학년		4학년		이론	설계	실험 실습			
				1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기						
대학필수	교필	아주희망전공진로탐색		●								1			1		
	교필	아주인을 위한 마중물		●								1			1		
	교필	아주상상프로젝트		●								3			3		
	교필	영어			●							3			3		
	교필	시리터러시-인공지능이해와응용			●							3			3		
	교필	대학글쓰기		●								3			3		
	교필	'역사와 철학'영역(택1)			●							3			3		
	교필	'문학과 예술'영역(택1)				●						3			3		
	교필	'인간과 사회'영역(택1)					●					3			3		
	교필	'연결과 통합'영역(택1)				●						3			3		
소계														26			26
BSM	수학	교필	수학1			●						3			3		
		교필	수학2				●					3			3		
	기초 과학	교필	물리학	Set	Set 중 택1			●					3	1	4		
		교필	물리학실험														
		교필	화학	Set				●									
		교필	화학실험														
		교필	생명과학	Set				●									
교필	생명과학실험																
소계														9	1	10	
전공기초	전기	확률및통계1					●					3			3		
	전기	선형대수1				●						3			3		
소계														6		6	
전공필수	전필	사이버보안입문			●							3			3		
	전필	이산수학			●							3			3		
	전필	컴퓨터프로그래밍및실습(소프트웨어)			●	◐						3	1		4		
	전필	자료구조(소프트웨어)				●	◐					3			3		
	전필	컴퓨터구조				●						3			3		
	전필	객체지향프로그래밍및실습(소프트웨어)				●						3	1		4		
	전필	현대암호이론및응용					●					3			3		
	전필	운영체제					●	◐				3			3		
	전필	컴퓨터네트워크(소프트웨어)					●	◐				3			3		
	소계														27	2	29
전공선택	전선	데이터사이언스입문(인공지능융합학과)				●						3			3		
	전선	정보보호법과정책					●					3			3		
	전선	시와윤리(인공지능융합학과)					●					3			3		
	전선	알고리즘(소프트웨어)					●	◐				3			3		
	전선	취약점분석					●					3			3		
	전선	정보보호(소프트웨어)						●				3			3		
	전선	시스템소프트웨어보안						●				3			3		

이수구분	학수구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
전공선택	전선	데이터베이스(소프트웨어)					●				2	1		3
	전선	오픈소스SW입문(소프트웨어)					●	◐			1	2		3
	전선	IoT보안					●				3			3
	전선	기계학습(소프트웨어)					●	◐			2	1		3
	전선	사이버보안관제					●				3			3
	전선	네트워크보안및응용					●				3			3
	전선	분산클라우드컴퓨팅					●				2		1	3
	전선	보안아키텍처						●			3			3
	전선	침해사고분석						●			3			3
	전선	데이터마이닝(소프트웨어)						●			2	1		3
	전선	디지털자산과블록체인						●			1.5	1.5		3
	전선	임베디드소프트웨어(소프트웨어)						●			1.5		1.5	3
	전선	소프트웨어공학(소프트웨어)						●			2	1		3
	전선	지능형사물인터넷(소프트웨어)						●			2	1		3
	전선	클라우드보안						●			3			3
	전선	실전코딩1(소프트웨어)						●			1		2	3
	전선	실전코딩2(소프트웨어)						●			1		2	3
	전선	자기주도프로젝트(소프트웨어)						●				3		3
	전선	인공지능보안						●			3			3
	전선	해킹과침해대응							●		3			3
	전선	시큐어코딩							●		3			3
	전선	사이버보안캡스톤디자인							●			6		6
	전선	분산시스템							●		3			3
	전선	SW창업론(소프트웨어)							●		3			3
	전선	빅데이터응용및보안							●		3			3
	전선	모바일네트워크(소프트웨어)							●		3			3
	전선	자기주도연구1(소프트웨어)							●			3		3
	전선	앱과웹보안								●	3			3
	전선	사이버보안사례특강								●	3			3
	전선	인공지능(소프트웨어)								●	3			3
	전선	자기주도연구2(소프트웨어)								●	2	1		3
	전선	인간과컴퓨터상호작용(소프트웨어)								●	3			3
	전선	시기반사이버보안:이론과응용								●	3			3
	전선	디지털포렌식								●	3			3
	전선	보안현장실습1					●						3	3
	전선	보안현장실습2						●					3	3
전선	보안현장실습3							●	◐			3	3	
전선	보안현장실습4							◐	●			3	3	
전선	창업실습1							●	◐			3	3	
전선	창업실습2							◐	●			3	3	
전선	창업현장실습1							●	◐			3	3	
전선	창업현장실습2							◐	●			3	3	
소계											98	21.5	30.5	150
총계											166	21.5	33.5	221

■ Cloud/BigData 보안 트랙

이수구분	학수구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
트랙필수	전선	정보보호법과정책				●					3			3
	전선	데이터베이스(소프트웨어)					●			2	1		3	
	전선	사이버보안관제					●			3			3	
	전선	클라우드보안						●		3			3	

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
트랙필수	전선	빅데이터응용및보안							●		3			3
	전선	사이버보안사례특강								●	3			3
소계											17	1		18
트랙선택	전선	알고리즘(소프트웨어)			●						3			3
	전선	분산시스템							●		3			3
	전선	기계학습(소프트웨어)					●				2	1		3
	전선	데이터마이닝(소프트웨어)						●			2	1		3
	전선	시스템소프트웨어보안					●				3			3
소계											13	2		15
총계											30	2		33

■ IoT/Mobile 보안 트랙

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
트랙필수	전선	정보보호법과정책			●						3			3
	전선	IoT보안					●				3			3
	전선	사이버보안관제					●				3			3
	전선	사이버보안사례특강								●	3			3
	전선	기계학습(소프트웨어)					●				2	1		3
소계											14	1		15
트랙선택	전선	정보보호(소프트웨어)					●				3			3
	전선	임베디드소프트웨어(소프트웨어)						●			3			3
	전선	모바일네트워크(소프트웨어)							●		3			3
	전선	지능형사물인터넷(소프트웨어)						●			2	1		3
	전선	데이터마이닝(소프트웨어)						●			2	1		3
소계											13	2		15
총계											27	3		30

4. 권장이수 순서표

■ 심화 및 일반과정

학 년	1학기					이수구분	2학기				
	과목명	학점	시간	선수과목	외국어 강의여부		과목명	학점	시간	선수과목	외국어 강의여부
1 학 년	아주희망전공진로탐색	1	1			대학필수	영어	3	3		
	아주인을 위한 마중물	1	1				영역별교양 (역사와 철학)	3	3		
	아주상상프로젝트	3	3				영역별교양 (연결과 통합)	3	3		
	대학글쓰기	3	3				시리터러시-인공지능이해와응용	3	3		
						BSM	수학1	3	3		
	사이버보안입문	3	3			전공필수	자료구조	3	3	컴퓨터프로그래밍및실습	
	이산수학	3	3								
	컴퓨터프로그래밍및실습	4	5								
	-	18	19			계		18	18	-	
2 학 년	영역별교양 (문학과 예술)	3	3			대학필수	영역별교양 (인간과 사회)	3	3		
	선형대수1	3	3			전공기초	확률및통계1	3	3		
	수학2	3	3			BSM					
	물리학										
	화학	3	3								
	생명과학	실험포함 Set 택1									
	물리학실험										
	화학실험		1	2							
	생명과학실험										
컴퓨터구조	3	3			전공필수	현대암호이론및응용	3	3			

학 년	1학기					이수구분	2학기				
	과목명	학점	시간	선수과목	외국어 강의여부		과목명	학점	시간	선수과목	외국어 강의여부
2 학 년	객체지향프로그래밍및실습	4	5	컴퓨터프로그래밍및실습		전공필수	운영체제	3	3	컴퓨터프로그래밍및실습	
	데이터사이언스입문	3	3				컴퓨터네트워크	3	3		
						전공선택	정보보호법과정책	3	3		
							알고리즘	3	3	자료구조	
						취약점분석	3	3			
						시와윤리	3	3			
	-	23	25			계		27	27		-
3 학 년	정보보호	3	3	자료구조		전공선택	데이터마이닝	3	3	자료구조	
	시스템소프트웨어보안	3	3	컴퓨터프로그래밍및실습			디지털자산과블록체인	3	3		
	데이터베이스	3	3	자료구조			임베디드소프트웨어	3	3	컴퓨터프로그래밍및실습	
	오픈소스SW입문	3	3	컴퓨터프로그래밍및실습			소프트웨어공학	3	3	객체지향프로그래밍및실습	
	IoT보안	3	3				지능형사물인터넷	3	3	운영체제	
	기계학습	3	3	자료구조			클라우드보안	3	3		
	사이버보안관제	3	3	현대암호이론및응용			침해사고분석	3	3		
	네트워크보안및응용	3	3	컴퓨터프로그래밍및실습			실전코딩1	3	3		
	분산클라우드컴퓨팅	3	3				실전코딩2	3	3		
	보안현장실습1	3	3				자기주도프로젝트	3	3	객체지향프로그래밍및실습	
							보안아키텍처	3	3	사이버보안입문	
					인공지능보안	3	3				
					보안현장실습2	3	3				
	-	30	30			계		39	39		-
4 학 년	사이버보안캡스톤디자인	6	9			전공선택	사이버보안사례특강	3	3		
	분산시스템	3	3	컴퓨터프로그래밍및실습			앱과웹보안	3	3		
	SW창업론	3	3				인공지능	3	3	자료구조	
	빅데이터응용및보안	3	3				인간과컴퓨터상호작용	3	3	알고리즘	
	모바일네트워크	3	3	컴퓨터네트워크			시기관사이버보안:이론과응용	3	3		
	자기주도연구1	3	3				디지털포렌식	3	3		
	해킹과침해대응	3	3				자기주도연구2	3	3		
	시큐어코딩	3	3				보안현장실습4	3	3		
	보안현장실습3	3	3				창업실습2	3	3		
	창업실습1	3	3				창업현장실습2	3	3		
	창업현장실습1	3	3								
	-	36	39			계		30	30		-

5. 유의사항

■ 선수과목표

학수구분	과목명	선수과목명
전필	객체지향프로그래밍및실습(소프트웨어)	컴퓨터프로그래밍및실습
전필	운영체제	컴퓨터프로그래밍및실습
전필	자료구조(소프트웨어)	컴퓨터프로그래밍및실습
전선	네트워크보안및응용	컴퓨터프로그래밍및실습
전선	분산시스템	컴퓨터프로그래밍및실습
전선	시스템소프트웨어보안	컴퓨터프로그래밍및실습
전선	오픈소스SW입문(소프트웨어)	컴퓨터프로그래밍및실습
전선	임베디드소프트웨어(소프트웨어)	컴퓨터프로그래밍및실습
전선	정보보호(소프트웨어)	자료구조
전선	기계학습(소프트웨어)	자료구조
전선	데이터마이닝(소프트웨어)	자료구조
전선	데이터베이스(소프트웨어)	자료구조
전선	알고리즘(소프트웨어)	자료구조
전선	인공지능(소프트웨어)	자료구조
전선	소프트웨어공학(소프트웨어)	객체지향프로그래밍및실습
전선	자기주도프로젝트(소프트웨어)	객체지향프로그래밍및실습

학수구분	과목명	선수과목명
전선	사이버보안관제	현대암호이론및응용
전선	모바일네트워크	컴퓨터네트워크
전선	안전과컴퓨터상호작용(소프트웨어)	알고리즘
전선	지능형시물인터넷(소프트웨어)	운영체제
전선	보안아키텍처	사이버보안입문

6. 과목개요

SOS111 사이버보안입문

———— Introduction to Cyber Security

본 과목에서는 인터넷윤리, 관리자윤리, 개발자 윤리 등 사이버보안의 일반적인 윤리를 익힌다.

SOS102 이산수학

———— Discrete Mathematics

수학이 무한하고(infinite) 조밀한(dense) 집합을 대상으로 추상적인 수학적 구조를 연구하는 학문인 데 비하여 이산수학은 유한하고(finite) 셀 수 있는(countable or numerable) 집합으로 대상을 국한하여 실제 생활에서 접하는 문제들을 주로 다룬다. 컴퓨터를 이용하여 문제를 해결함에 있어서 행렬이나 그래프 등과 같은 다양한 수학적 모델을 이용하여 문제를 정의하고, 그에 따른 해결 방법을 수학적 이론이나 방법을 활용하여 검증하기 위한 기초 지식을 학습한다. 본 교과목은 컴퓨터구조와 자료구조의 선수과목으로 지정되어 있으며, 본격적으로 전공 관련 교과목을 수강하기 위해 반드시 이수해야 할 과목 중의 하나이다.

SCE103 컴퓨터프로그래밍및실습

———— Computer Programming and Practice

소프트웨어및컴퓨터공학 전공 ‘컴퓨터프로그래밍및실습’ 과목 개요 참조

SCE205 자료구조

———— Data Structures

소프트웨어및컴퓨터공학 전공 ‘자료구조’ 과목 개요 참조

SCE212 컴퓨터구조

———— Computer Organization and Architecture

소프트웨어및컴퓨터공학 전공 ‘컴퓨터구조’ 과목 개요 참조

SCE204 객체지향프로그래밍및실습

———— Object-oriented Programming and Practice

소프트웨어및컴퓨터공학 전공 ‘객체지향프로그래밍및실습’ 과목 개요 참조

SOS252 현대암호이론및응용

———— Modern Cryptography and Applications

컴퓨터 공학 전공자에게 필요한 암호의 기초부터 암호의 적용까지를 포함하는 강의로서 암호의 기반이 되는 수학적 배경지식 강의, 암호 이론 기초 강의, 암호 프로토콜 및 어플리케이션 강의를 진행하며 세부 수업내용으로는 정수론, 암호 기술 및 암호화 개요, 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 암호 프로토콜(키분배 및 인증), 해쉬, MAC, PKI, 전자서명, 타원곡선 암호, 암호기술의 적용 : SSL, TLS, S/MIME, PGP등을 진행한다.

SCE213 운영체제

———— Operating Systems

소프트웨어및컴퓨터공학 전공 ‘운영체제’ 과목 개요 참조

SCT221 컴퓨터네트워크

———— Computer Networks

소프트웨어및컴퓨터공학 전공 ‘컴퓨터네트워크’ 과목 개요 참조

AAI336 데이터사이언스입문

———— Introduction of data science

인공지능융합전공 ‘데이터사이언스입문’ 과목 개요 참조

SOS222 정보보호법과정책

———— Security Law and Policy

정보보호는 빠르게 진화하고 변화해 나가고 있으며 해킹이나 불법적인 접근, 바이러스 DoS등 다양한 형태의 네트워크 및 시스템에 대한 공격과 위협행위에 대한 법적인 접근과 정책 수립이 필요하다. 또한 이러한 네트워크와 시스템에 대한 불법적인 접근과 위협행위는 실제의 범죄와도 연관될 수 있기 때문에 정보보호 기술의 학습에 앞서 관련된 법제도와 정책은 필수적으로 고려되어야 한다.

AAI334 AI와윤리

———— Artificial Intelligence and Ethics

인공지능융합전공 ‘AI와윤리’ 과목 개요 참조

SCE332 알고리즘

———— Algorithms

소프트웨어및컴퓨터공학 전공 '알고리즘' 과목 개요 참조

SOS211 취약점분석

———— Threat Analysis

사이버보안전문가가 되기 위해서 모의해킹과 취약점 분석 능력은 필수적이다. 국내 정보보안 산업 현장에서 필요로 하는 모의해킹 및 취약점 분석 지식들을 익히기 위하여, 먼저 국내의 기술적 취약점 진단 가이드를 바탕으로 취약점 분석 방법을 학습한다. 이러한 학습을 통해 웹 서비스, 윈도우 및 리눅스 운영체제와 DBMS의 취약점을 기본 진단할 수 있는 지식을 학습한다.

SCE3314 정보보호

———— Introduction to Information Security

소프트웨어및컴퓨터공학전공 '정보보호' 과목 개요 참조

SOS337 시스템소프트웨어보안

———— System Software Security

본 교과목은 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 기술 보안, 응용서비스 및 콘텐츠 보안에 관한 다양한 주제를 다룬다. 즉, 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 학습함으로써 소프트웨어 기반 보안에 대한 전반적인 기초 및 응용 능력을 키우고, 소프트웨어 기반 보안에 관한 실습을 진행한다.

실습에서는 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 보안, 응용서비스 및 콘텐츠 보안에 관한 실습을 다룬다. 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안 실습, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안 실습, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 실습함으로써 소프트웨어 기반 보안에 대한 전반적인 설계와 응용 능력을 키운다.

SCE333 데이터베이스

———— Database

소프트웨어및컴퓨터공학 전공 '데이터베이스' 과목 개요 참조

SCE331 오픈소스SW입문

———— Introduction to Open Source Software

소프트웨어및컴퓨터공학 전공 '오픈소스SW입문' 과목 개요 참조

SOS3312 IoT보안

———— IoT Security

IoT(사물인터넷) 환경은 기존의 중앙집중화된 네트워크 구조(centralized network structure)와는 달리 다양한 스마트 디바이스로 구성되는 복잡한 네트워크 구조를 가지고 있다. 이는 기존의 네트워크 환경에서 제공할 수 있는 서비스 보다 더욱더 다양한 서비스를 제공할 수 있으며, 이로 인해 기존의 네트워크 환경에서 발생할 수 있는 보안 취약점보다 더욱 다양하고 복잡한 형태의 보안 취약점이 발생할 수 있음을 의미한다. 그러므로 본 과목에서는, 다음과 같은 IoT 플랫폼보안(IoT Platform Security)와 관련된 내용에 대하여 학습한다.

- 비연결 디바이스를 위한 End-to-end 플랫폼 보안
- 호환성 및 상호연결성을 고려한 디바이스, 센서, 데이터베이스 등의 안전한 연결 기술
- 각 기기들로부터 수집되는 정보들의 안전한 전송 기술
- 플랫폼 융합 및 검증 기술

SCE3315 기계학습

———— Machine Learning

소프트웨어및컴퓨터공학 전공 '기계학습' 과목 개요 참조

SOS346 사이버보안관제

———— Cyber Security Operation Control

사이버보안관제는 다양한 정보보호 솔루션들을 사용하여 모니터링하고 관리하는 다양한 형태의 정보보호 기술들을 실제로 다루어본다. 특히 점점 더 복잡해지고 융합 기술이 적용되어가는 정보보호 분야에 있어 실제 기술의 적용과 상황 대응은 사이버보안에 있어 가장 필요한 요구 기능이다.

SOS3310 네트워크보안및응용

———— Network Security and Applications

본 교과목에서는 인터넷 보안의 목표와 그 목표를 달성하기 위한 각 계층별 보안 프로토콜을 이론적으로 배우고 또한 실습한다. 주요 교육내용은 TLS와 IPsec의 기본이 되는 PKI에 대해 배우고, TLS와 IPsec의 주요 원리 및 프로토콜을 학습한다.

SOS321 분산클라우드컴퓨팅

———— Distributed Cloud Computing

분산클라우드 컴퓨팅은 일반적으로 센서네트워크에서 사물인터넷, 가상현실(VR,AR, MR,XR), 인공지능 등 방대한 데이터를 실시간으로 처리해야 하는 각종 애플리케이션에서 주로 사용되고 있다. 특히 요즘은 블록체인기술을 활용하여 기업이나 연구소 등에서 국가별 또는 산업별 정보보호와 관련된 문제를 해결하는 데에도 기여하고 있다. 또한 최근

COVID-19 팬데믹으로 인해 다양한 지역에 분산 배치된 직원 및 최종 사용자에게 IT 서비스를 제공하는 데에도 큰 역할을 하고 있다. 따라서 애플리케이션 컴포넌트가 네트워크로 연결된 여러 컴퓨터(클라우드 컴퓨팅)에 흩어져 있는 상태에서 메시징 또는 API를 통해 통신하는 방식이 활용되고 있다. 따라서 소프트웨어와 정보통신 및 정보보안 관련 전공 학생들에게 컴퓨팅 활용 측면에서 필수적인 응용지식을 제공하고자 한다.

### SOS312 보안아키텍처

#### Security Architecture

본 교과목은 클라우드 및 하이브리드 환경에서 보안 아키텍처 설계 원칙과 모범 사례를 기반으로 시스템 보안 구조를 설계하고 운영하는 과목으로, 이론과 실무 중심 내용을 다룬다. 보안아키텍처 모델과 Zero Trust 기반 보안 정책 및 책임 모델, 사용자 인증 구조, 컨테이너 및 서버리스 보안, 다계층 보안 설계 등의 내용 위주로 이론 학습과 테스트베드를 통한 실습을 추가로 포함한다.

### SOS322 침해사고분석

#### Incident Analysis and Digital Forensics

실제 침해사고 사례를 분석하고 로그·네트워크·디지털 포렌식 기법을 활용하여 사고 원인을 규명하고 대응 능력을 기른다.

### SCE3313 데이터마이닝

#### Data Mining

소프트웨어및컴퓨터공학 전공 '데이터마이닝' 과목 개요 참조

### SOS3313 디지털자산과블록체인

#### Digital Assets and Blockchain

본 과목은 블록체인과 분산원장, 그리고 블록체인 응용 기반 기술로써 IoT 보안의 기본지식을 배운다. 주요 강의 내용은 블록체인 및 분산원장의 기본원리, 블록체인 보안, 비트코인, 이더리움 등의 주요 블록체인에 대한 이해, 스마트 계약, NFT, DAO, IoT 보안 등이다.

### SCE312 임베디드소프트웨어

#### Embedded Software

소프트웨어및컴퓨터공학 전공 '임베디드소프트웨어' 과목 개요 참조

### SCE337 소프트웨어공학

#### Software Engineering

소프트웨어및컴퓨터공학 전공 '소프트웨어공학' 과목 개요 참조

### SCE3317 지능형사물인터넷

#### Artificial Intelligence of Things

소프트웨어및컴퓨터공학 전공 '지능형사물인터넷' 과목 개요 참조

### SOS3311 클라우드보안

#### Cloud Security

클라우드 컴퓨팅 기술 및 데이터의 저장기술은 사용자와 기업에게 다양한 서비스를 제공할 수 있다. 그러나 클라우드 서비스 환경에서는 클라우드 환경에 저장되는 다양한 데이터와 응용기술 등을 제어하기 위한 여러 가지 정책과 보안기술 등에 대한 고려가 필요하다. 그러므로 본 과목에서는 다음과 같은 클라우드서비스 보안기술들에 대하여 학습한다.

- 조직의 정보보안 정책 적용 방안
- 안전한 데이터 전송 및 저장 기술
- 조직의 자산 보호 및 복구 기술
- 안전한 클라우드 서비스 구축 기술

### SCE3310 실전코딩 1

#### Practical Coding1

본 과목에서는 산업체의 현업 소프트웨어 개발자가 현장 실무환경에서 라이브코딩 형태로 강의를 진행한다. 특히 대학 정규 과정에서 다루지 않지만 현업 개발 현장에서 활용되는 Agile 협업 프로세스, 협업 도구, Jenkins, SonarQube, Maven, TDD, 리팩토링 등을 교육하고 인턴십 수행 또는 취업 시 도움이 될 수 있도록 학생들이 직접 실습을 수행하게 된다.

### SCE3311 실전코딩 2

#### Practical Coding2

실전코딩1과 동일하다.

### SCE395 자기주도프로젝트

#### Undergraduate Project

전공심화로 진입하기 위한 역량을 배양하고 진단하는 교과목이다. 팀을 구성하여 산업체에서 제시하는 혹은 산업체에 프로젝트 주제를 제시하여 한 학기 동안 프로젝트를 진행한다.

### SOS361 인공지능보안

#### AI Security

AI는 수많은 분야에 높은 성능을 보여 주며 각광받고 있으나, 기존과는 다른 새로운 보안 이슈가 발생한다. AI 기술이 내재하는 보안 이슈 및 이들을 완화하는 기법에 대해 학습하며, Adversarial attack, Membership inference attack 등에 사용되는 이론 및 이들을 방어하기 위한 최신 기법을 학습한다.

SOS422 해킹과침해대응

———— Hacking and Incident Response

다양한 해킹 기법과 이에 대응하는 보안 기술을 학습하며, 모의해킹 및 침투테스트 실습을 통해 침해사고 대응 역량을 기른다.

SOS438 시큐어코딩

———— Secure Coding

소프트웨어 개발 과정에서 발생할 수 있는 보안 취약점을 예방하고, 안전한 코드를 작성하는 방법을 학습한다. 보안 취약점 유형과 이에 대응하는 안전한 코딩 기법을 익히며, 실제 사례를 통해 보안 위협을 이해하고 이를 차단할 수 있는 코드를 작성하는 실무 역량을 높일 수 있다.

SOS402 사이버보안캡스톤디자인

———— Cyber Security Capstone Design

학과 과정에서 학습한 소프트웨어보안 도메인의 전공 지식과 설계의 요소 기술들을 종합하는 과목으로서 학습성과를 성취하는 것과 더불어 학습 성과의 성취 여부를 종합적으로 평가받는 기회를 제공한다. 문제 정의, 구성 요소 설계, 구현, 평가 등 개발 절차의 전 과정을 이 과목에서 거치게 된다. 실제 산업체에서 요구하는 기술들을 중심으로 개발 과정을 거침으로써 학생들이 졸업 후에 소프트웨어보안 도메인 산업체에서 핵심적인 개발 인력으로서 참여할 수 있도록 하는 준비 기회를 제공한다.

SOS434 분산시스템

———— Distributed Systems

소프트웨어및컴퓨터공학 전공 '분산시스템' 과목 개요 참조

SCE492 SW창업론

———— SW Business Start-up

창업이란 개인 혹은 법인이 이윤추구를 혹은 자기만족을 추구하기 위한 목적으로 사업아이템을 가지고 적성, 특성, 기술, 자금, 영업 및 경영능력 등을 동원하여 수익을 창출하는 기업을 새로이 설립하는 것이다. 특히 이 과목에서는 SW 창업의 의의와 중요성을 이해하고 다양한 사례를 검토하고 성공요건을 논의한다.

첫째로, 요즘은 창조경제가 바라보는 창업트렌드를 환경 및 시대적 시각에서 검토한다. 이스라엘을 포함한 다양한 국내외 사례들을 검토하고 그에 대한 시사점을 찾는다.

둘째로, 기업이 정신을 이해하고 창업 과정, 창업 아이템, 자금조달과 운영 및 창업 법률과 세무에 대해서 실무적으로 자세히 알아본다.

셋째로, 모바일 소호 쇼핑물, 온라인 쇼핑물, 인터넷 경제, 공동 구매 등 다양한 창업 사례를 검토한다. 이러한 사례들

중 실패요인과 성공요인을 분석 검토한다.

넷째로, 이 과목에서 배운 이론을 기반으로 창업을 위한 사업계획서(Business Plan) 작성을 실습한다. 사업 타당성 분석 및 자금 조달 계획이 포함되고 투자유치 전략이 수립되어야한다.

마지막으로 각자 창업자 사업역량 자기 진단을 실시하여 자기 역량을 분석한다.

SOS444 빅데이터응용및보안

———— Big Data Application and Security

본 과목은 빅데이터와 AI-LLM 기반 서비스에서 발생하는 보안 및 개인정보 문제를 데이터 프라이프라인 전 주기 관점에서 이해하는 것을 목표로 한다. 머신러닝·딥러닝과 LLM의 기본 원리와 구조를 바탕으로, 입력·표현·출력 단계에서 형성되는 공격 표면과 취약성을 분석하고, 데이터 공격·프라이버시 침해·추론 공격 등 핵심 이슈를 다룬다. 또한 위협 모델링과 실습을 통해 LLM 기반 서비스의 공격·방어 특성을 이해하고, 보안 설계와 그 한계를 판단하는 능력을 기른다.

SCE421 모바일네트워크

———— Mobile Communication Networks

소프트웨어및컴퓨터공학전공 '모바일네트워크'과목 개요 참조

SCE493 자기주도연구1

———— Undergraduate Research I

대학원 진학을 희망하는 학생들이 대학원 진학 전 가능한 연구 분야를 탐색하고 본격적인 대학원 과정에서의 연구를 준비하는 단계에서의 자기주도적인 연구를 해볼 수 있는 기회를 제공한다. 4학년 2학기 자기주도연구2와 연계하여 1년 동안 지도교수, 대학원생, 산업체 멘토와 연계하여 체계적이고 실용적인 연구를 진행한다

SOS463 앱과웹보안

———— Application and Web Security

웹 및 모바일 앱 환경의 주요 보안 위협과 취약점을 이해하고, OWASP 기반 실습을 통해 대응 기술을 습득한다.

SOS492 사이버보안사례특강

———— Special Topic in Cyber Security

매학기 정보보호의 공격과 기술동향에 관한 주제를 선정하고, 이를 다루는 매거진과 기술문서, 논문들을 학생들이 읽고, 정리하여 발표하며, 주제에 관련한 전문가를 초청하여 특강을 진행하는 형태의 수업이다. 강의를 마치는 학생들은 진행하였던 주제를 토대로 분석 결과를 보고서로 제출하거나 학술지 등에 투고하게 된다.

## SCE432 인공지능

———— Artificial Intelligence

소프트웨어및컴퓨터공학전공 '인공지능' 과목 개요 참고

## SCE494 자기주도연구2

———— Undergraduate Research II

자기주도연구1과 동일하다.

## SCE436 인간과컴퓨터상호작용

———— Human Computer Interaction

소프트웨어및컴퓨터공학전공 '인간과컴퓨터상호작용' 과목 개요 참고

## SOS443 시기반사이버보안:이론과응용

———— AI for Cybersecurity:Theory and Applications)

〈빅데이터 응용 및 보안〉과목이 데이터·LLM 중심 보안이었다면, 〈AI 기반 사이버보안: 이론과 응용〉은 AI를 '보안 도구'로 사용하는 과목으로, 인공지능과 딥러닝을 활용하여 침입탐지, 이상행위 탐지, 악성코드 분석 등 주요 사이버보안 문제를 해결하는 방법을 학습한다. 머신러닝과 딥러닝의 기본 원리를 바탕으로 로그·트래픽·시스템 이벤트 등 대규모 보안 데이터를 분석하고, 지능형 탐지 모델을 설계·구현한다. 또한 적대적 공격, 데이터 오염, 모델 우회 등 AI 기반 보안 시스템의 한계를 이해하고, 실습과 프로젝트를 통해 강력한 보안 모델을 설계·평가하는 능력을 기른다.

## SOS338 디지털포렌식

———— Digital Forensics

본 교과목은 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 기술 보안, 응용서비스 및 콘텐츠 보안에 관한 다양한 주제를 다룬다. 즉, 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 학습함으로써 소프트웨어 기반 보안에 대한 전반적인 기초 및 응용 능력을 키우고, 소프트웨어 기반 보안에 관한 실습을 진행한다.

실습에서는 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 보안, 응용서비스 및 콘텐츠 보안에 관한 실험을 다룬다. 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안 실습, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안 실습, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 실습함으로써 소프트웨어 기반 보안에 대한 전반적인 설계와 응용 능력을 키운다.

## SOS192 보안현장실습 1

———— Information Security Field Practice 1

회사를 정하여 회사의 프로젝트에 참여하여 현장체험을 통하여 정보보호 지식의 활용 및 학습의 동기부여를 이루는 것을 목표로 한다. 현장의 실무에 참여하여 학교에서 배운 기초 지식을 응용하는 기회를 가진다. 회사에 근무하면서 회사의 실무자와 같이 현장의 문제와 해결방법을 체득한다

## SOS191 보안현장실습 2

———— Information Security Field Practice 2

보안현장실습1과 동일하다

## SOS493 보안현장실습3

———— Information Security Field Practice 3

보안현장실습1과 동일하다

## SOS494 보안현장실습4

———— Information Security Field Practice 4

보안현장실습1과 동일하다

## SCE499 창업실습 1

———— Startup Practice 1

학생들에게 창업현장의 개발자로서 업무수행에 필요한 여러 가지를 미리 준비하면서 공식적인 사회진출 이전에 창업자로서 준비를 마칠 수 있도록 한다. 주요 활동은 창업 아이디어에 대한 사업계획서 작성, 시제품 제작, 수익모델 검토, 창업자금 확보 방안 등이다.

## SCE4910 창업실습 2

———— Startup Practice 2

창업실습1과 동일하다.

## SCE4911 창업현장실습 1

———— Startup Field Practice 1

일정수준을 충족하는 창업활동을 학점으로 인정함으로써 학생의 부담을 경감하고 학생이 창업과 학업을 병행할 수 있는 프로그램이다. 구체적으로 사업전략 수립, 수익모델 확보, 인력확보, 창업자금 준비, 콘텐츠 개발, 마케팅, 매출 등을 통하여 지속가능한 기업활동을 준비한다

## SCE4912 창업현장실습 2

———— Startup Field Practice 2

창업현장실습1과 동일하다.

## 블록체인마이크로전공

### 교육과정표

**1. 졸업 이수학점 및 구성 현황**

가. 총 졸업 이수학점 : 9학점

나. 교육과정별 필수 이수학점 구성 현황

구분	대학필수							BSM		전공		
	아주희망 전공진로탐색	아주인을 위한 마음물	아주상상 프로젝트	영어	대학 글쓰기	영역별 교양	AI 리터러시	수학	기초 과학	전공기초	전공필수	전공선택
블록체인마이크로전공	학생 소속 제1전공 기준으로 이수									-	9	

- 블록체인(Blockchain Security) 마이크로전공 편성 교과목 : 데이터마이닝(3), 현대암호이론및응용(3), 시스템소프트웨어보안(3), 네트워크보안및응용(3), 디지털자산과블록체인(3), 분산시스템(3), 블록체인과산업보안(3)

**2. 졸업요건**

■ 총 졸업 이수학점 : 9 학점

**3. 교육과정**

■ 일반 및 심화과정

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
전공선택	전선	데이터마이닝(소프트웨어)									2	1		3
	전선	현대암호이론및응용				●					3			3
	전선	시스템소프트웨어보안					●				3			3
	전선	네트워크보안및응용					●				3			3
	전선	디지털자산과블록체인						●			1.5	1.5		3
	전선	분산시스템								●	3			3
	전선	블록체인과산업보안(대학원)									●	3		3
		소계									18.5	2.5		21
		총계									18.5	2.5		21

**4. 권장이수 순서표**

■ 심화 및 일반과정

학 년	1학기					이수구분	2학기				
	과목명	학점	시간	선수과목	외국어 강의여부		과목명	학점	시간	선수과목	외국어 강의여부
2학년						전공선택	현대암호이론및응용	3	3		
	-					계		3	3	-	
3학년	네트워크보안및응용	3	3	컴퓨터프로그래밍및실습		전공선택	데이터마이닝	3	3	자료구조	
	시스템소프트웨어보안	3	3	컴퓨터프로그래밍및실습		계	디지털자산과블록체인	3	3		
	-		6	6		계		6	6	-	
4학년	분산시스템	3	3	컴퓨터프로그래밍및실습		전공선택	블록체인과산업보안(대학원)	3	3		
	-		3	3		계		3	3	-	

5. 유의사항

■ 선수과목표

학수구분	과목명	선수과목명
전선	데이터마이닝	자료구조
전선	네트워크보안및응용	컴퓨터프로그래밍및실습
전선	시스템소프트웨어보안	컴퓨터프로그래밍및실습
전선	분산시스템	컴퓨터프로그래밍및실습

6. 과목개요

SOS252 현대 암호이론 및 응용

———— Modern Cryptography and Applications

컴퓨터 공학 전공자에게 필요한 암호의 기초부터 암호의 적용까지를 포함하는 강의로서 암호의 기반이 되는 수학적 배경지식 강의, 암호 이론 기초 강의, 암호 프로토콜 및 어플리케이션 강의를 진행하며 세부 수업내용으로는 정수론, 암호기술 및 암호화 개요, 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 암호 프로토콜(키분배 및 인증), 해쉬, MAC, PKI, 전자서명, 타원곡선 암호, 암호기술의 적용 : SSL, TLS, S/MIME, PGP등을 진행한다.

SOS3310 네트워크보안및응용

———— Network Security and Applications

본 교과목에서는 인터넷 보안의 목표와 그 목표를 달성하기 위한 각 계층별 보안 프로토콜을 이론적으로 배우고 또한 실습한다. 주요 교육내용은 TLS와 IPsec의 기본이 되는 PKI에 대해 배우고, TLS와 IPsec의 주요 원리 및 프로토콜을 학습한다.

SOS337 시스템소프트웨어보안

———— System Software Security

본 교과목은 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 기술 보안, 응용서비스 및 콘텐츠 보안에 관한 다양한 주제를 다룬다. 즉, 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 학습함으로써 소프트웨어 기반 보안에 대한 전반적인 기초 및 응용 능력을 키우고, 소프트웨어 기반 보안에 관한 실습을 진행한다.

실습에서는 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 보안, 응용서비스 및 콘텐츠 보안에 관한 실습을 다룬다. 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안 실습, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안 실습, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 실습함으로써 소프트웨어 기반

보안에 대한 전반적인 설계와 응용 능력을 키운다.

SOS3313 디지털자산과블록체인

———— Digital Assets and Blockchain

본 과목은 블록체인과 분산원장, 그리고 블록체인 응용 기반 기술로써 IoT 보안의 기본지식을 배운다. 주요 강의 내용은 블록체인 및 분산원장의 기본원리, 블록체인 보안, 비트코인, 이더리움 등의 주요 블록체인에 대한 이해, 스마트 계약, NFT, DAO, IoT 보안 등이다.

SCE3313 데이터마이닝

———— Data Mining

소프트웨어및컴퓨터공학 전공 '데이터마이닝' 과목 개요 참조

SOS434 분산시스템

———— Distributed Systems

소프트웨어및컴퓨터공학 전공 '분산시스템' 과목 개요 참조

KIS6714 블록체인과산업보안

———— Blockchain and Industrial Security

대학원 산업보안전공 '블록체인과산업보안' 과목 개요 참고

## 빅데이터지식재산마이크로전공

### 교육과정표

#### 1. 졸업 이수학점 및 구성 현황

가. 총 졸업 이수학점 : 9학점

나. 교육과정별 필수 이수학점 구성 현황

구분	대학필수							BSM		전공		
	아주희망 전공전로탐색	아주인을 위한 마중물	아주상상 프로젝트	영어	대학 글쓰기	영역별 교양	시 리터러시	수학	기초 과학	전공기초	전공필수	전공선택
빅데이터지식재산마이크로전공	학생 소속 제1전공 기준으로 이수									6	3	

- 빅데이터 지식재산(Big Data Intellectual Property) 마이크로 전공 편성 교과목 : 지식재산과학기술사업화(3), 정보보호 법과정책(3), 디지털포렌식(3), 빅데이터응용및보안(3), 사이버보안사례특강(3)
- 빅데이터 지식재산(Big Data Intellectual Property) 마이크로 전공 필수 교과목 : 지식재산과학기술사업화(3), 정보보호 법과정책(3)

#### 2. 졸업요건

■ 총 졸업 이수학점 : 9 학점

#### 3. 교육과정

■ 심화 및 일반과정

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계	
			1학년		2학년		3학년		4학년		이론	설계	실험 실습		
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기					
전공필수	일선	지식재산과학기술사업화						●				3			3
	전선	정보보호법과정책				●						3			3
	소계											6			6
전공선택	전선	빅데이터응용및보안								●		3			3
	전선	디지털포렌식									●	3			3
	전선	사이버보안사례특강									●	3			3
	소계											9			9
총계												15			15

#### 4. 권장이수 순서표

■ 심화 및 일반과정

학 년	1학기					이수구분	2학기				
	과목명	학점	시간	선수과목	외국어 강의여부		과목명	학점	시간	선수과목	외국어 강의여부
2학년						전공필수	정보보호법과정책	3	3		
	-					계		3	3		-
3학년	지식재산과학기술사업화	3	3			전공필수					
	-	3	3			계		0	0	-	
4학년	빅데이터응용및보안	3	3			전공선택	사이버보안사례특강	3	3		
							디지털포렌식	3	3		
	-	3	3			계		6	6	-	

## 5. 과목개요

## DGMD103 지식재산과기술사업화

———— Intellectual Property and Technology commercialization

본 과목에서는 지식재산을 기반으로 하는 기술창업 및 기술사업화를 체계적으로 수행할 수 있도록, 지식재산의 기초 개념에서부터 기업가 정신, 비즈니스 아이디어에 대한 지식재산화와 가치평가 및 전략적 활용에 필요한 방법들을 살펴보고, 최종 사업계획의 수립의 단계까지 순차적으로 학습함으로써 지식재산 기반 기술창업의 이론과 실제의 역량을 강화하고자 한다. 특히, 기술창업의 지속가능성을 확보하기 위한 창업 아이템의 지식재산 권리화를 수행하도록 한다. 마지막으로 지식재산능력에 따른 국가공인자격 취득을 지원하여 학생들의 전공기반 지식재산 진로 및 취업의 선택의 폭을 넓혀주고자 한다. 이를 통해, 지식기반 기술창업을 중심으로 사업화 전략을 종합적으로 수립하여 본 학기의 학습 내재화를 진행하고자 한다.

## SOS222 정보보호법과정책

———— Security Law and Policy

정보보호는 빠르게 진화하고 변화해 나가고 있으며 해킹이나 불법적인 접근, 바이러스 DoS등 다양한 형태의 네트워크 및 시스템에 대한 공격과 위협행위에 대한 법적인 접근과 정책 수립이 필요하다. 또한 이러한 네트워크와 시스템에 대한 불법적인 접근과 위협행위는 실제의 범죄와도 연관될 수 있기 때문에 정보보호 기술의 학습에 앞서 관련된 법제도와 정책은 필수적으로 고려되어야 한다.

## SOS338 디지털포렌식

———— Digital Forensics

OS , NFC,

OS , NFC,

## SOS444 빅데이터응용및보안

———— Big Data Application and Security

본 과목은 빅데이터와 AI·LLM 기반 서비스에서 발생하는 보안 및 개인정보 문제를 데이터 파이프라인 전 주기 관점에서 이해하는 것을 목표로 한다. 머신러닝·딥러닝과 LLM의 기본

원리와 구조를 바탕으로, 입력·표현·출력 단계에서 형성되는 공격 표면과 취약성을 분석하고, 데이터 공격·프라이버시 침해·추론 공격 등 핵심 이슈를 다룬다. 또한 위협 모델링과 실습을 통해 LLM 기반 서비스의 공격·방어 특성을 이해하고, 보안 설계와 그 한계를 판단하는 능력을 기른다.

## SOS492 사이버보안사례특강

———— Special Topic in Cyber Security

매학기 정보보호의 공격과 기술동향에 관한 주제를 선정하고, 이를 다루는 매거진과 기술문서, 논문들을 학생들이 읽고, 정리하여 발표하며, 주제에 관련한 전문가를 초청하여 특강을 진행하는 형태의 수업이다. 강의를 마치는 학생들은 진행하였던 주제를 토대로 분석 결과를 보고서로 제출하거나 학술지 등에 투고하게 된다.

## 지능정보안마이크로전공

### 교육과정표

**1. 졸업 이수학점 및 구성 현황**

가. 총 졸업 이수학점 : 9학점

나. 교육과정별 필수 이수학점 구성 현황

구분	대학필수							BSM		전공		
	아주희망 전공진로탐색	아주인을 위한 마음물	아주상상 프로젝트	영어	대학 글쓰기	영역별 교양	AI 리더러시	수학	기초 과학	전공기초	전공필수	전공선택
지능정보안마이크로전공	학생 소속 제1전공 기준으로 이수										-	9

- 지능정보안(AI Security) 마이크로 전공 편성 교과목 : 인공지능보안(3), 기계학습(3), 정보보호(3), 네트워크보안및응용(3), 디지털포렌식(3), 빅데이터응용및보안(3), AI기반사이버보안:이론과응용(3), 딥러닝이론및실습(3), 지능형사이버보안(3)

**2. 졸업요건**

■ 총 졸업 이수학점 : 9 학점

**3. 교육과정**

■ 일반 및 심화과정

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
전공선택	전선	기계학습(소프트웨어)					●	(●)			2	1		3
	전선	정보보호(소프트웨어)					●				3			3
	전선	네트워크보안및응용					●				3			3
	전선	인공지능보안							●		3			3
	전선	빅데이터응용및보안								●	3			3
	전선	디지털포렌식									●	3		3
	전선	SI기반사이버보안:이론과응용									●	3		3
	전선	딥러닝이론및실습(대학원)									●	3		3
	전선	지능형사이버보안(대학원)									●	3		3
		소계									26	1		27
		총계									26	1		27

**4. 권장이수 순서표**

■ 심화 및 일반과정

학 년	1학기				이수구분	2학기				
	과목명	학점	시간	선수과목		외국어 강의여부	과목명	학점	시간	선수과목
3 학 년	기계학습	3	3	자료구조	전공선택	인공지능보안	3	3		
	정보보호	3	3	자료구조						
	네트워크보안및응용	3	3	컴퓨터프로그래밍및실습						
	-	9	9		계		3	3		-
4 학 년	빅데이터응용및보안	3	3		전공선택	딥러닝이론및실습	3	3		
						지능형사이버보안	3	3		
						SI기반사이버보안:이론과응용	3	3		
						디지털포렌식	3	3		
	-	3	3		계		12	12		-

## 5. 유의사항

## ■ 선수과목표

학수구분	과목명	선수과목명
전선	정보보호	자료구조
전선	기계학습	자료구조
전선	네트워크보안및응용	컴퓨터프로그래밍및실습

## 6. 과목개요

## SCE3315 기계학습

———— Machine Learning

소프트웨어및컴퓨터공학전공 '기계학습' 과목 개요 참고

## SCE3314 정보보호

———— Introduction to Information Security

소프트웨어및컴퓨터공학전공 '정보보호' 과목 개요 참고

## SOS3310 네트워크보안및응용

———— Network Security and Applications

본 교과목에서는 인터넷 보안의 목표와 그 목표를 달성하기 위한 각 계층별 보안 프로토콜을 이론적으로 배우고 또한 실습한다. 주요 교육내용은 TLS와 IPsec의 기본이 되는 PKI에 대해 배우고, TLS와 IPsec의 주요 원리 및 프로토콜을 학습한다.

## SOS361 인공지능보안

———— AI Security

AI는 수많은 분야에 높은 성능을 보여 주며 각광받고 있으나, 기존과는 다른 새로운 보안 이슈가 발생한다. AI 기술이 내재하는 보안 이슈 및 이들을 완화하는 기법에 대해 학습하며, Adversarial attack, Membership inference attack 등에 사용되는 이론 및 이들을 방어하기 위한 최신 기법을 학습한다.

## SOS444 빅데이터응용및보안

———— Big Data Application And Security

본 과목은 빅데이터와 AI-LLM 기반 서비스에서 발생하는 보안 및 개인정보 문제를 데이터 프라이버시 전 주기 관점에서 이해하는 것을 목표로 한다. 머신러닝·딥러닝과 LLM의 기본 원리와 구조를 바탕으로, 입력·표현·출력 단계에서 형성되는 공격 표면과 취약성을 분석하고, 데이터 공격·프라이버시 침해·추론 공격 등 핵심 이슈를 다룬다. 또한 위협 모델링과 실습을 통해 LLM 기반 서비스의 공격·방어 특성을 이해하고, 보안 설계와 그 한계를 판단하는 능력을 기른다.

## SOS338 디지털포렌식

———— Digital Forensics

본 교과목은 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 기술 보안, 응용서비스 및 콘텐츠 보안에 관한 다양한 주제를 다룬다. 즉, 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 학습함으로써 소프트웨어 기반 보안에 대한 전반적인 기초 및 응용 능력을 키우고, 소프트웨어 기반 보안에 관한 실습을 진행한다.

실습에서는 소프트웨어 기반 보안 시스템, 웹기반 운영체제 플랫폼 및 무선 통신 소프트웨어 보안, 응용서비스 및 콘텐츠 보안에 관한 실습을 다룬다. 임베디드 리눅스 혹은 안드로이드와 같은 모바일 OS에서의 소프트웨어 관련 보안 실습, NFC, 무선랜 와이파이 등에서의 응용 소프트웨어 보안 실습, 클라이언트와 모바일 웹, 모바일 기기 소프트웨어 보안에 대한 최근 이슈 등을 실습함으로써 소프트웨어 기반 보안에 대한 전반적인 설계와 응용 능력을 키운다.

## SOS443 AI기반사이버보안:이론과응용

———— AI for Cybersecurity:Theory and Applications

<빅데이터 응용 및 보안>과목이 데이터·LLM 중심 보안이었다면, <AI 기반 사이버보안: 이론과 응용>은 AI를 '보안 도구'로 사용하는 과목으로, 인공지능과 딥러닝을 활용하여 침입탐지, 이상행위 탐지, 악성코드 분석 등 주요 사이버보안 문제를 해결하는 방법을 학습한다. 머신러닝과 딥러닝의 기본 원리를 바탕으로 로그·트래픽·시스템 이벤트 등 대규모 보안 데이터를 분석하고, 지능형 탐지 모델을 설계·구현한다. 또한 적대적 공격, 데이터 오염, 모델 후회 등 AI 기반 보안 시스템의 한계를 이해하고, 실습과 프로젝트를 통해 강건한 보안 모델을 설계·평가하는 능력을 기른다.

## AI502 딥러닝이론및실습

———— Deep Learning Theory and Practice

대학원 AI융합네트워크전공 '딥러닝이론및실습' 과목 개요 참고

## CSEC713 지능형사이버보안

———— Intelligent Cyber Security

대학원 사이버보안전공 '지능형사이버보안' 과목 개요 참고

## AI와 사이버보안 나노전공

### 교육과정표

#### 1. 졸업 이수학점 및 구성 현황

가. 교육과정별 졸업 이수학점 구성 현황: 6학점 이상 이수

나. 교육과정별 필수 이수학점 구성 현황

구분	대학필수							BSM		전공		
	아주희망 전공진로탐색	아주인물 위한 마음물	아주상상 프로젝트	영어	대학 글쓰기	영역별 교양	시리터러시- 인공지능 이해와응용	수학	기초 과학	전공기초	전공 필수	전공 선택
AI와 사이버보안 나노전공	학생 소속 제1전공 기준으로 이수							3	학생 소속 제1전공 기준으로 이수		-	3

• AI와사이버보안(AI and Cybersecurity) 나노전공 이수 교과목 : AI리터러시-인공지능이해와응용(3), AI와윤리(3)

\* 나노전공: 전공이해를 위한 소단위 과정으로,

#### 2. 졸업요건

■ 총 졸업 이수학점 : 6 학점

#### 3. 교육과정

■ 일반 및 심화과정

이수구분	학수 구분	과목명	개설 학년 및 학기(해당란에 '●'표시)								학점구성(구성 요소 별 학점 수)			학점 수 합계
			1학년		2학년		3학년		4학년		이론	설계	실험 실습	
			1학기	2학기	1학기	2학기	1학기	2학기	1학기	2학기				
대학필수	교필	시리터러시-인공지능이해와응용		●							3			3
전공선택	전선	AI와윤리(인공지능융합학과)			●						3			3
총계			0	1	0	1	0	1	0	0	6	0	0	6

#### 4. 권장이수 순서표

■ 심화 및 일반과정

학 년	1학기					이수구분	2학기				
	과목명	학점	시간	선수과목	외국어 강의여부		과목명	학점	시간	선수과목	외국어 강의여부
1학년	-					대학필수	시리터러시-인공지능이해와응용	3	3		
						계		3	3	-	
2학년	-					전공선택	AI와윤리(인공지능융합학과)	3	3		
						계		3	3	-	

#### 5. 과목개요

학습한다.

##### SOS462 시기반사이버보안:이론과응용

———— AI for Cybersecurity:Theory and Applications)  
빅데이터 및 인공지능 기술을 접목한 지능화된 보안 패러다임의 변화가 일어나고 있다. 그러나 빅데이터의 사용은 개인정보 보호와 보안 문제를 야기할 수 있으며, 이를 해결하는 것이 필수적이다. 이 과목에서는 대규모 언어 모델(LLM), 연합학습(Federated Learning), 그리고 개인정보 보호 기술을 중심으로 인공지능 기반의 데이터 보호 기술을

##### AAI334 AI와윤리

———— Artificial Intelligence and Ethics  
인공지능융합전공 'AI와윤리' 과목 개요 참조