금융정보보안학과
(Dept. of Financial Information Security)

설치 과정 : 석사과정, 박사과정, 석·박사통합과정

학과 소개

금융정보보안학과는 2014년에 정보보안 전공, 금융공학 및 창업 전공, 금융정보시스템 전공 교수진이 참여하여 일반대학원의 협동과정으로 설립되었다. 본 협동과정에서는 신뢰 기반 사회 및 경제 정보 생태계 구현을 위한 금융정보보안 관련 제반 문제를 학문적으로 심도 있게 연구하고 이를 실무적으로 응용할 수 있는 전문성과 국제 경쟁력을 겸비한 창의적 정보보안 전문인력 양성을 목적으로 융합형 교육과정을 운영하고 있다. 금융정보보안학과의 전체 교수진은 2013년 하반기부터 정부의 핵심 교육사업 중의 하나인 BK21플러스 특화전문인재양성 사업에 선정되어 '미래 금융정보보안 전문인력 양성 사업단' 운영을 통하여 연구 개발 및 관련 산업 분야에서 활발히 활동하고 있다. 본 학과에서는 학생들이 프라이버시 보호 및 인증 기술, 암호 알고리즘과 프로토콜 설계 및 안전성 분석 기술, 스마트 디바이스 보안기술, 정보보안시스템 구현 및 평가 기술 등으로 구성된 정보보안 분야, 정보시스템 및 인프라플랫폼, 네트워크 및 통신 프로토콜, 빅데이터 인프라 등으로 구성된 정보시스템 분야, 그리고 금융리스크 측정 및 관리, 주식 및 채권 투자, 금융 및 보험 상품, 창업 및 사업화 등으로 구성된 금융 및 경영 분야의 유용한 지식을 상호 융합적으로 습득함으로써 미래의 진정한 금융정보보안 전문가로 자리매김 할 수 있도록 지원 및 육성하고자 한다.

교육 목표

본 학과의 가장 중요한 목표는 신뢰 기반 사회・경제 정보생태계 구현을 위한 금융정보보안 관련 문제를 연구하고 이를 학문적・실무적으로 응용 및 확장할 수 있는 전문성과 국제 경쟁력을 겸비한 창의적 금융정보보안 전문인력을 양성하는 것이며, 변화하는 미래 금융 서비스의 발생가능한 정보보안의 취약점을 극복하고, 창의 금융 서비스를 선도하는 핵심 인력 양성을 목표로 한다. 또한 금융과 지식정보보안 관련 지식을 결합하여 금융기업에서의 미래 정보기술 환경에 능동적으로 대처할 수 있는 금융정보보안 전문가 및 금융정보보안솔루션 고급 개발자 양성을 목표로 한다. 금융관련 정보보안전문인력(CISO, Chief Information Security Officer), CIO(Chief Information Officer), CTO(Chief Technology Officer), CRO(Chief Risk Officer)가 갖추어야 할 이론적 기반과 실무 능력을 겸비한 금융정보보안 특화 전문 인력 양성을 목표로 한다.

본 학과는 이를 구체적으로 실천하기 위하여 다음과 같이 세 가지 세부목표를 설정한다.

첫째, 본 학과는 금융정보보안 전문가 양성을 위해 사회・경제적 신뢰 저해 징후를 감지하고, 이에 대해 선제적으로 대응하기 위한 프라이버시 보호 기술, 인증 기술, 해킹 대응기술, 정보보안 제품 평가 기술 등의 전문인력을 양성하고자 하며, 구체적으로 금융정보보안 관련 핵심 원천기술인 공개키, 대칭키 암호 및 PKI 등의 금융 인프라 보호 기술을 교육하고, 이러한 요소기술의 새로운 조합을 통해 금융정보보안의 신뢰 프로세스 점검 및 개선을 위한 금융정보보안 분석 모델을 수립한다.

둘째, 본 학과는 첫 번째 세부목표를 통해 도출된 사회・경제적 신뢰 향상을 위한 암호기술의 문제해결

모델을 금융 빅데이터 보호, 금융관련 법규 및 제도, 미래의 창조금융 서비스 및 e-Discovery 등의 미래 금융경영 환경에 적용할 수 있도록 교육한다. 이를 위해 우리 사회에서 필요로 하는 다양한 유형의 금융 관련 사회・경제적 신뢰 프로세스 구축을 위한 연구주제들을 발굴 및 선정하여 심도 있게 연구하고 그 해결능력을 갖춘 정보보안 전문인력을 양성한다.

셋째, 본 학과는 금융정보보안 시스템 설계 및 구현기술, 금융정보보안 기반의 서비스 개발기술, 금융정보보안 컨설팅 기술 등 금융정보보안 전문역량을 갖춘 미래의 금융정보보안 전문인력 양성을 목표로 한다. 금융정보보안과 연관되어 구체적으로 제안된 문제해결 모델 및 시스템의 활용을 통해 사회적 자본을 얼마나 증진시킬 수 있는가를 측정 및 평가하며, 지속가능한 신뢰기반 사회・경제 금융 생태계를 위한 일자리 창출 방안 및 정책 대안을 제시한다.

전공 분야

분 야	개 요
정보융합보안 전공 (Information Security Major)	정보보안 관련 전문 기술을 바탕으로 금융 및 경영 지식을 겸비하여 미래 금융정보보안 환경 발전에 기여할 수 있는 연구 및 기술 인력을 양성한다.
금융보안 전공 (Financial Security Major)	금융 및 경영 관련 지식을 기반으로 정보시스템 및 정보보안 기술을 겸비하여 미래 금융정보보안 환경 발전에 기여할 수 있는 전문 인력을 양성한다.

학과 운영내규

1. 선수과목

1) 타계열 출신 석사과정과 박사과정 학생에게는 필요에 따라 주임교수와의 협의를 통해서 하위 과정의 교과목(석사과정 12학점, 박사과정 24학점)을 이수하게 할 수 있다.
2) 출신 대학에서 이미 이수한 과목이 있는 경우, 학과 주임교수의 승인을 받아 이를 면제 받을 수 있다. 출신대학에 따라 과목명이 상이하므로, 동일한 교과내용으로서 과목명이 다른 경우에는 학과 주임교수의 승인을 받아 이를 이미 이수한 것으로 인정받을 수 있다.

2. 외국어 시험

1) 외국어시험의 응시자격 및 응시절차는 대학원 학칙 및 대학원 학사운영규정에 준한다.
2) 박사과정에 대하여 제2외국어 시험을 실시하지 않는다.
3) 대학원 학사운영규정 제 47조(외국어시험의 면제) 제7항에 의거 다음 각호의 경우 본 내규에 의해 외국어시험을 면제한다.

가. 석사과정: 내국인 중 영문 학위논문 작성자
나. 박사과정: 내국인 중 SCI급 국제학술지에 제 1저자로 최소 1편의 논문 투고 및 영문 학위논문 작성자. 한국어 응시대상 외국인의 경우는 제외

4) 외국어시험 대체 온라인수업(모의TOEIC) 기준 점수는 750점으로 한다.

3. 종합시험

1) 종합시험의 응시자격 및 응시절차는 대학원 학칙 및 대학원 학사운영규정에 준한다.
2) 종합시험은 석사과정 2과목, 박사과정 3과목으로 한다.

3) 대학원 학사운영규정 제 52조2(종합시험의 면제)에 의거 다음 각호의 경우 본 내규에 의해 종합시험을 면제한다.
가. 석사과정: KCI 학술지에 주저자로 1편이상의 논문 게재(예정)자
나. 박사과정: SCIE 학술지에 주저자로 1편 이상의 논문 게재(예정)자
다. 공동저자는 공동주저자 수만큼 나눠서 계산되며, 논문 편수의 합이 1편 이상 되어야 함.
라. 면제 신청 시 게재 확정 확인(게재예정증명서 제출, 온라인 출간 등)이 가능해야 함.

4. 학위청구논문

1) 논문계획서는 지도교수의 확인을 받아 석사과정은 3차 학기 개강 1주내, 박사과정은 4차 학기 개강 1주내에 주임교수에게 제출하여야 한다.
2) 본심사 직전 학기말까지 논문지도평가를 통과(pass)하여야 한다.
3) 석사과정은 논문예비심사를 실시하지 않는다.
4) 박사과정 논문예비심사는 본심사 학기 초까지 실시하며, 예비심사용 논문원고를 심사일 2주 전에 주임교수에게 제출하여 예비심사위원에게 전달되도록 해야 한다.
5) 본심사용 학위청구논문은 전기에 졸업하고자 하는 대학원생은 10월 초까지, 후기에 졸업하고자 하는 대학원생은 4월 초까지 제출하여야 한다. 기간 내 제출하지 않은 논문은 심사에서 제외한다.
6) 논문심사는 석사과정은 2회, 박사과정은 3회를 실시하며, 논문심사 날짜는 지도교수가 심사위원과 협의하여 정한다. 논문은 각 심사일 2주 전에 심사위원에게 제출하여야 한다.

부 칙

이 내규는 2014년 3월 1일부터 시행한다.
이 변경내규는 2024년 3월 1일부터 시행한다.

교과과정표

○ 전공 공통(Core Courses)

교 과 목		학점	강의	실습	수강대상
금융정보보안론	(Financial Information Security)	3	3	0	석·박사 공통
연구윤리와논문연구	(Research Ethics & Thesis Study)	3	3	0	
암호알고리즘	(Cryptographic Algorithm)	3	3	3	
PKI개론	(Introduction to PKI)	3	3	3	

○ 정보융합보안 전공(Information Security Major Courses)

교 과 목		학점	강의	실습	수강대상
정보보호프로토콜	(Information Security Protocols)	3	3	0	
해쉬함수와데이터인증	(Hash Function and Message Authentication)	3	3	0	
공개키암호분석이론	(Cryptanalysis of Public-key Cryptosystem)	3	3	0	

교 과 목		학점	강의	실습	수강대상
대칭키암호분석	(Topics in Symmetric Key Cryptanalysis)	3	3	0	
병렬암호구현	(Parallel Implementation of Cryptographic Algorithms)	3	3	0	
암호모듈평가및검증	(Evaluation and Validation Techniques for Cryptographic Modules)	3	3	0	
부채널공격론	(Side Channel Attacks)	3	3	0	
부채널공격대응론	(Countermeasures of Side Channel Attacks)	3	3	0	
보안구현개발방법론	(Security Implementation Methodology)	3	3	0	
이동통신보안	(Mobile Security)	3	3	0	
무선보안특강	(Wireless Security)	3	3	0	
융합보안특강	(IT Convergence and Security)	3	3	0	
금융정보보호정책	(Financial Security Policy)	3	3	0	
정보보호컨설팅	(Information Security Consulting)	3	3	0	
정보보호시스템평가방법론	(Information Security System Evaluation Methodology)	3	3	0	
보안기술표준분석및구현	(Analysis and Implementation of Security Technical Standards)	3	3	0	
디지털포렌식개론	(Introduction to Digital Forensic)	3	3	0	석·박사 공통
디지털포렌식특수연구	(Special Research of Digital Forensic)	3	3	0	
금융디바이스공격론	(Financial Device Attacks)	3	3	0	
금융디바이스공격대응론	(Countermeasures against Financial Device Attacks)	3	3	0	
금융키관리시스템	(Financial Key Management System)	3	3	0	
금융네트워크보안	(Financial Networks Security)	3	3	0	
전자상거래	(Electronic Commerce Security)	3	3	0	
증명가능안전성론	(Provable Security)	3	3	0	
암호소프트웨어구현	(Implementation of Cryptographic S/W)	3	3	0	
난수성분석론	(Analysis of Randomness)	3	3	0	
인공지능과보안이론	(AI and Security)	3	3	0	
자율성장인공지능특론	(Advanced Self-supervised AI)	3	3	0	
인공지능융합기술특강	(AI Convergence)	3	3	0	
사물지능망특론	(Advanced Internet of Things)	3	3	0	
무선이동통신네트워크	(Wireless Cellular Network)	3	3	0	

○ 금융보안 전공(Financial Security Major Courses)

교 과 목		학점	강의	실습	수강대상
고급정보통신론	(Advanced Information Communication Theory)	3	3	0	
모델기반시스템설계	(Model-based System Design)	3	3	0	
데이터마이닝	(Data Mining)	3	3	0	
IoT네트워크	(IoT Network)	3	3	0	석·박사 공통
임베디드시스템	(Embedded System)	3	3	0	
실시간시스템	(Real-time System)	3	3	0	
정보시스템개발방법론	(Information System Development Methodology)	3	3	0	
비즈니스정보통신	(Business Data Communication)	3	3	0	
클라우드컴퓨팅	(Cloud Computing)	3	3	0	

교과목 개요

○ 전공 공통(Core Courses)

- 금융정보보안론(Financial Information Security)
  전자화폐 및 전자지불시스템, 인터넷 뱅킹 시스템 등의 금융 관련 정보보안 기술에 대하여 학습한다.

- 연구윤리와논문연구(Research Ethics & Thesis Study)
  연구윤리 강화와 논문표절 근절을 위해 올바른 태도와 가치관을 갖도록 기본 인성을 함양시킨다.
- 암호알고리즘(Cryptographic Algorithm)
  고전 암호, Shannon의 이론에 기초한 스트림 암호와 블록 암호의 안전성 이론, 사용방법에 따른 문제점, 설계방법 등을 학습한다.
- PKI개론(Introduction to PKI)
  공개키 기반구조(PKI)의 필요성을 인식하고, 인프라 구축에 필요한 기술에 대한 이해를 목표로 한다. 공인인증서 체계를 비롯한 PKI의 사례를 중심으로 활용 현황과 보안 이슈를 점검하고 금융보안과 PKI의 관계를 조망해본다.

○ 정보융합보안 전공(Information Security Major Courses)

- 해쉬함수와데이터인증(Hash Function and Message Authentication)
  전자서명에 활용되는 충돌 회피 해쉬 함수 및 이를 이용하여 데이터 위변조를 검출할 수 있는 MAC 생성 방법의 설계원리를 학습한다.
- 공개키암호분석이론(Cryptanalysis of Public-key Cryptosystem)
  인수분해, 이산로그, 등의 수학적 문제에 기반한 공개키 암호에 대한 기본적인 공격법 및 프로토콜의 적용에 따라 발생하는 제반 문제점을 소개한다. 아울러 각종 공개키 암호에 대한 안전성을 학습한다.
- 대칭키암호분석(Topics in Symmetric Key Cryptanalysis)
  블록암호 및 스트림암호 해시함수 등에 대한 안전성 분석을 위한 기본기술을 습득하고, 사용환경에 따라 안전한 알고리즘의 선택과 활용능력을 기른다.
- 병렬암호구현(Parallel Implementation of Cryptographic Algorithms)
  병렬처리를 위한 하드웨어와 운영체제에 대한 체계적인 이해를 바탕으로 암호알고리즘의 고속 병렬 구현기술을 습득한다. 특히, 그래픽프로세서(GPU)를 이용한 고속구현 실습으로 암호알고리즘에 대한 이해와 함께 응용능력 향상을 도모한다.
- 암호모듈평가및검증(Evaluation and Validation Techniques for Cryptographic Modules)
  암호모듈 검증제도(CMVP)에 대한 정책적・제도적 이해를 바탕으로 암호모듈의 평가・검증을 위한 기준과 관련기술에 대한 이해와 적용방법을 습득한다. 각 검증기준에 대한 취지의 이해와 함께 평가기술의 적용방법에 대하여 학습한다.
- 부채널공격론(Side Channel Attacks)
  스마트디바이스의 물리적 취약성 분석기술을 다룬다.
- 부채널공격대응론(Countermeasures of Side Channel Attacks)
  부채널공격에 안정한 S/W 및 H/W 기반 대응방법의 설계 및 구현에 대하여 다룬다.
- 보안구현개발방법론(Security Implementation Methodology)
  정보보안에 필요한 암호기능을 구현하는 실무적인 방법을 익힌다. 안전한 코딩기술을 바탕으로 환경에 맞는 보안기능을 식별하고 구현할 수 있는 능력을 배양한다.

- 이동통신보안(Mobile Security)
  이동통신망의 최신 보안 구조 및 그 응용 기술을 다룬다.
- 무선보안특강(Wireless Security)
  최신의 무선통신 기술과 그 응용에 필요한 보안기술을 학습한다.
- 융합보안특강(IT Convergence and Security)
  IT와 타 산업의 융합기술을 배우고, 그 응용에 필요한 보안기술을 배운다.
- 금융정보보호정책(Financial Security Policy)
  정보보호정책과 관리에 대한 지식을 습득할 수 있도록 한다. 정보보호의 기술적 한계를 보완할 수 있는 관리적 대책 방안을 학습한다.
- 정보보호컨설팅(Information Security Consulting)
  정보보안제품 또는 정보보안 관련 조직의 정보 보호의 수준과 취약점 및 정보보호 정책, 표준 및 절차, 모니터링 과정 등을 평가하여 개선 방법을 제공하는 방법을 배운다.
- 정보보호시스템평가방법론(Information Security System Evaluation Methodology)
  IT제품 및 시스템의 보안성 평가를 위한 공통 평가 기준 (Common Criteria), CMVP(Cryptographic Module Validation Program), PIV(Personal Identity Verification) 등의 평가 방법론을 배운다.
- 보안기술표준분석및구현(Analysis and Implementation of Security Technical Standards)
  IETF(Internet Engineering Task Force), 국제표준화기구(ISO), 미 국가표준기술연구원(NIST)에서 발간하는 보안기술과련 표준을 이해하고 구현과 관련한 지식을 배운다. ISO/IEC, IETF 등의 국제표준기술에 대한 이해와 분석을 바탕으로 안전한 표준기술을 활용하여 보안시스템을 설계할 수 있는 능력을 배양한다.
- 디지털포렌식개론(Introduction to Digital Forensic)
  PC나 노트북, 휴대폰 등 각종 저장매체 또는 인터넷 상에 남아 있는 각종 디지털 정보를 분석해 의미있는 정보를 찾는 방법 및 기술에 대해 배운다.
- 디지털포렌식특수연구(Special Research of Digital Forensics)
  디지털포렌식 관련 최신 기술을 습득하고 연구한다.
- 금융디바이스공격론(Financial Device Attacks)
  개인PC, 스마트폰, 스마트카드, Micro-SD, OTP 등 다양한 금융디바이스에서 발생 가능한 보안 취약성을 찾고 이를 안전하게 대응하는 기술에 대해 배운다.
- 금융디바이스공격대응론(Countermeasures against Financial Device Attacks)
  금융장비 공격에 안전하도록 S/W와 H/W를 기반으로 한 대응 기법을 다룬다.
- 금융키관리시스템(Financial Key Management System)
  금융정보 보호 시스템에 사용되는 키를 생성·분배·복구하는 제반 기술을 다룬다.
- 금융네트워크보안(Financial Networks Security)
  금융통신망 시대에 필요한 데이터 보호 기술을 다룬다. 금융 통신망의 구조와 특성을 분석하고 가상사설망(VPN), IPsec, SSL, TLS 등을 다룬다.

- 전자상거래(Electronic Commerce Security)
  전자쇼핑몰을 이용한 전자상거래 시 필요로 하는 각종 보안 기법 및 문제점을 다룬다. 신용카드나 전자 수표, 전자 화폐를 이용하는 각종 지불 수단에 대해서 다룬다. 전자지불 시스템이 장단점과 보안상의 문제 등을 학습한다.

- 증명가능안전성론(Provable Security)
  seudo-randomness, 정보이론 관점의 안전성, 계산 복잡도 측면의 안전성 등 암호 알고리즘 및 프로토콜에 대한 증명가능 안전성 이론을 다룬다.

- 암호소프트웨어구현(Implementation of Cryptographic S/W)
  국제표준 대칭키 암호 및 공개키 암호의 소프트웨어 구현기술을 습득한다.

- 난수성분석론(Analysis of Randomness)
  정보보안 프로토콜 및 암호 알고리즘에 필수적으로 사용되는 난수발생기의 설계와 안전성 분석을 다룬다.

- 인공지능과보안이론(AI and Security)
  인공지능을 활용한 보안 기술 및 인공지능의 허점을 분석하기 위한 개념 및 이론을 학습한다.

- 자율성장인공지능특론(Advanced Self-supervised AI)
  자율성장 인공지능에 필요한 기본 개념과 모델을 분석하고 다양한 데이터 기반 문제 해결 능력방법에 대하여 학습한다.

- 인공지능융합기술특강(AI Convergence)
  인공지능 및 보안 기술과 관련된 다양한 분야에서의 활용 및 융합 연구에 대한 전문가 특강을 통해 새로운 연구동향을 학습한다.

- 사물지능망특론(Advanced Internet of Things)
  이 수업을 통해 service, platform, network(connectivity) 및 smart device로 구성되는 사물 공간 연결망 Internet of Things (IoT) / Internet of Service (IoS)에 대하여 학습한다. 나아가 인공지능과 결합된 시뮬레이션 및 Cyber Physical System, Digital Twin 등에 대하여 학습한다.

- 무선이동통신네트워크(Wireless Cellular Network)
  본 수업을 통해 무선이동 셀룰라통신 1세대 AMPS (Advanced Mobile Phone System)부터 4G LTE-A (Long Term Evolution - Advanced)까지의 무선 이동통신 기술 및 역사에 대하여 학습한다. 5G 및 5G+ 이동통신 시스템을 Network slicing, eMBB(Enhanced Mobile Broadband), URLLC(Ultra-Reliable Low Latency Communication), mMTC(Massive Machine Type Communication) 등의 핵심기술을 중심으로 살펴본다. 또한 무선 액세스 모바일 인터넷, D2D, 5G 코어 네트워크 기술 및 인공지능 기반 서비스 플랫폼 등에 대하여도 학습한다. 2030년부터 서비스가 시작될 것으로 예측하는 6G네트워크 요구사항 및 망 확장성에 대하여 학습한다.

○ 금융보안 전공(Financial Security Major Courses)

- 고급정보통신론(Advanced Information Communication Theory)
  Core / Edge 네트워크 및 컴퓨팅의 핵심기술인 상황인지 및 위치인식에 대하여 학습한다. 상황인지(context-awareness) / 위치인식(localization) 및 차세대 네트워크 아키텍처, 요구사항 등 다양한 응용

시스템에 대하여 학습을 진행한다.

- 모델기반시스템설계(Model-based System Design)
  소프트웨어 설계 및 구현 패턴에 대한 기본적인 개론을 포함하여 일반적인 이해를 습득하며, Java와 같은 객체지향 프로그램 언어를 이용하여 디자인 패턴을 소프트웨어 시스템 설계에 적용 하는 다양한 작업들과 종류별 패턴들을 학습한다. 소프트웨어 디자인 패턴에서의 Creational Patterns, Structural Patterns, Behavioral Patterns의 다양한 세부 패턴들을 습득하며, 실제 시스템 설계에 적용하며 학생들의 설계 및 구현 능력을 함양한다.

- 데이터마이닝(Data Mining)
  데이터 마이닝의 기본 개념 학습, 실습을 통한 사례 학습을 진행한다. Association, Clustering, Classification 등 데이터 마이닝을 통해 발굴되는 지식의 패턴에 대해 배우고, 가장 널리 사용되고있는 도구인 SAS Enterprise Miner를 활용하여 실습 능력을 배양하도록 한다.

- IoT네트워크(IoT Network)
  지상 IoT(Internet of Things), M2M(Machine to Machine Communication), WoT(Web of Things), UIoT (Underwater IoT)와 같은 사물 인터넷 개념 대해서 학습한다. 뿐만 아니라 관련 국제 표준에 대해서도 학습한다.

- 임베디드시스템(Embedded System)
  ARM 아키텍처에 대한 이해 및 펌웨어 기반의 임베디드 시스템 설계 및 구현 능력을 함양한다.

- 실시간시스템(Real-time System)
  실시간 시스템에 대한 이해 및 실시간운영체제 기반의 임베디드 시스템의 설계 및 구현 능력을 함양한다.

- 정보시스템개발방법론(Information System Development Methodology)
  임베디드 시스템과 관련된 정보시스템 개발 방법론에 대해서 학습한다. 따라서 자료 구조와 알고리즘, 임베디드 시스템의 설계 및 구현에 대한 전반적인 과정 등에 대하여 학습한다.

- 비즈니스정보통신(Business Data Communication)
  비즈니스정보통신의 개념에 대하여 학습한다. 데이터통신 및 네트워킹의 기본 개념에 대하여 학습을 진행 후 실제로 비즈니스 응용분야에 어떻게 적응할 것인지에 대하여 사례를 통하여 학습을 진행한다. 데이터통신의 기본개념의 이해를 돕는 예제를 중심으로 실습 및 정보통신기술이 실제 비즈니스 분야 적용되는 사례를 조사한다.

- 클라우드컴퓨팅(Cloud Computing)
  기업의 비즈니스 활동을 지원하고, 소비자들의 편익을 증대시켜 주는 클라우드 컴퓨팅 및 응용 서비스에 대한 일반적인 개념을 이해한다. 본 과목에서는 클라우드 컴퓨팅 환경 하에서 요구되는 핵심기술 및 이슈들에 대해 다루며, 서비스 대상에 따라 구분되는 SaaS, PaaS, IaaS 과 혼합된 형태의 서비스들에 대해 공부한다. 더불어, 분산 시스템, 미들웨어, 어플리케이션 통합 등 클라우드 서비스를 형성하는데 필요한 다양한 개념들, VM 관련 기술과 Public Cloud 의 사용 및 Open-source cloud에 대하여 함께 습득한다.