# AI Security
# Syllabus

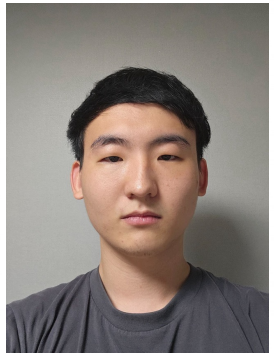
Artificial Intelligence Research (AIR) LAB
https://air.korea.ac.kr/
School of Cybersecurity
Korea University

Sangkyun Lee (이상근)

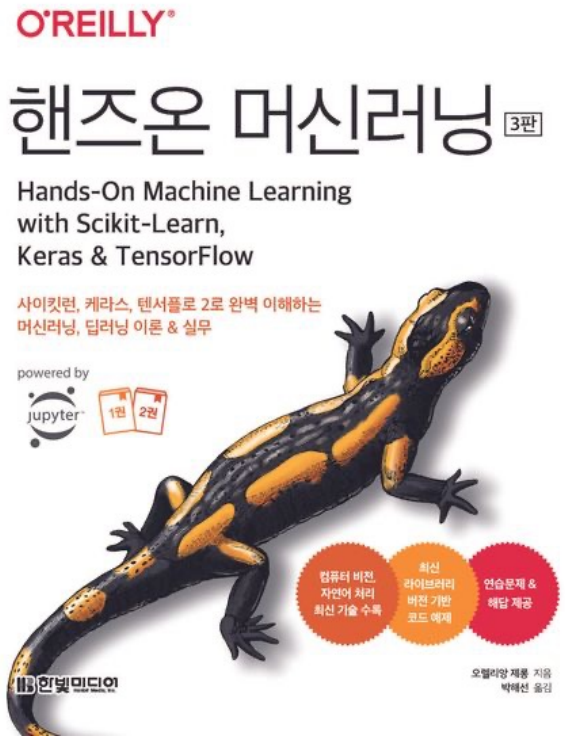
2025. Spring Semester

# AI보안 : 강의 개요

- 다양한 보안 분야의 문제 해결에 응용 가능한 기계학습과 딥러닝 방법에 대해 공부
- 이상근 교수: 정운오IT교양관 310호 (sangkyun@korea.ac.kr, air.korea.ac.kr)
- 조교: 박정환, 박성현



- 교재
  - 배포예정




- 강의노트: https://github.com/sanglee/SDS_AI_2025

# 세부 계획

- 총 12주 강의

- 시험
  - 중간고사 (6주차, TBD): 프로젝트 제안 발표
  - 기말고사 (12주차, 8월28일): 프로젝트 최종 발표

# 세부 계획

- 1주차: **Introduction to ML (ch1, 3)**
- 2주차: **로지스틱 회귀** (ch4), SVM (ch5)
- 3주차: decition tree (ch6), random forest / gradient boosting (ch7)
- 4주차: PCA (ch8), clustering (k-means/DBSCAN) (ch9)
- 5주차: anomaly detection (ch9), intro to deep neural nets (ch10)
- 6주차: **중간고사**
- 7주차: training dnns (ch11)
- 8주차: convolutional neural nets (ch14)
- 9주차: recurrent neural nets (ch15)
- 10주차: RNN with attention (ch16)
- 11주차: XAI (xx)
- 12주차: **기말고사**

# Thank You