# Sentra

## 사용자 행동 기반
## 동적 네트워크 접근 제어 솔루션

**분과** 하드웨어/보안
**지도교수** 최윤호 교수님

201924524 이광훈
202155609 조유진
202255562 신해진

# 연구 목표

## 기존 문제점

현행 NAC (802.1X)

- 포트 기반 **사전** 인증으로 사용자·단말 검증
- 인증 **이후 행위**는 사각지대
- **"인증=안전" 가정**
  → 데이터 반출·이상 트래픽 **실시간 통제 불가**

사전 인증만으로는 내부자 위협 대응 불충분

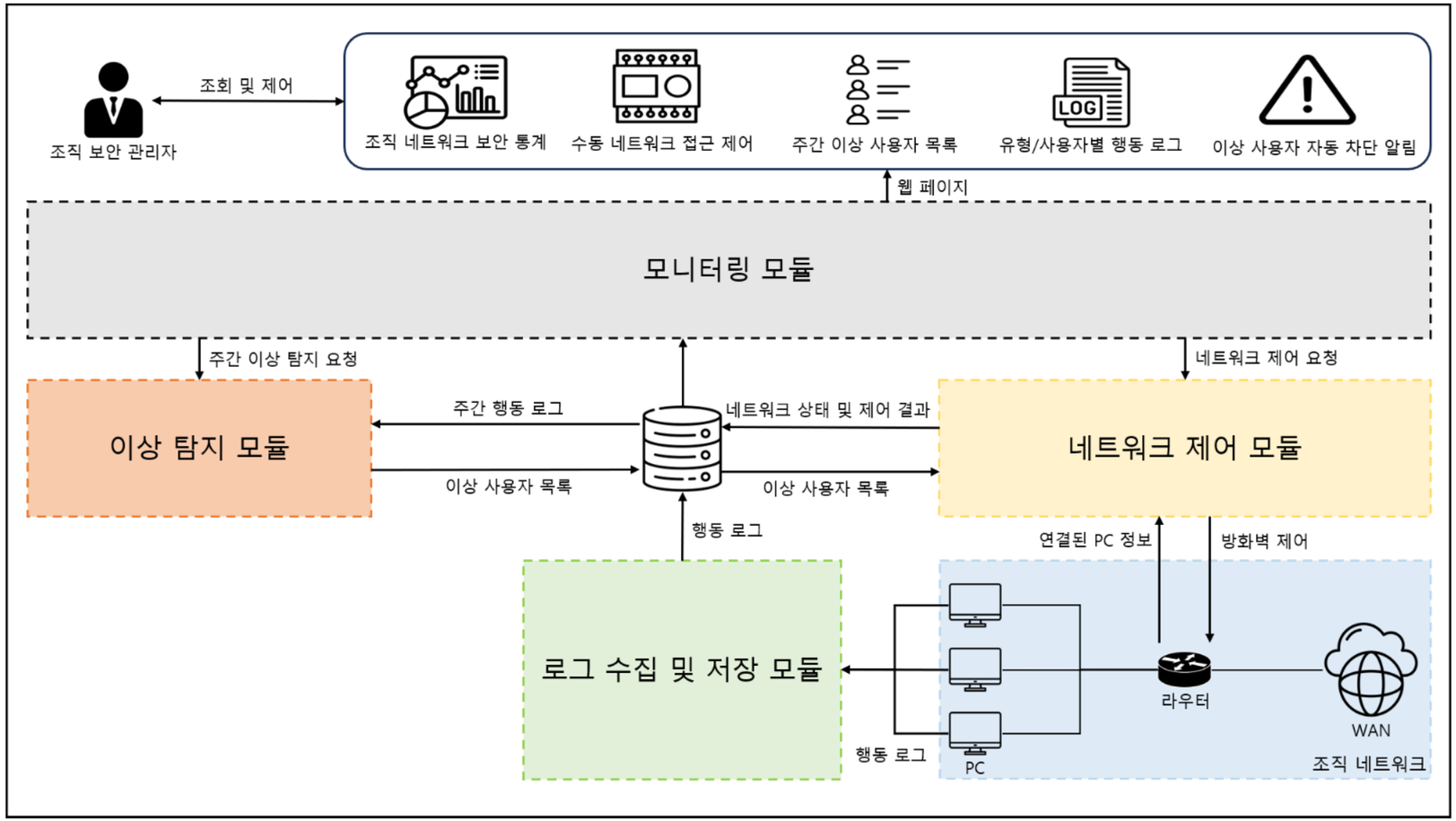
## 목표

사후 행동 기반 NAC

- 조직 내 사용자 **행동 로그** 실시간 수집·분석
- **이상 사용자 자동 식별**
- 탐지 즉시 **네트워크 격리** 자동화

사전 인증 중심 → 사후 행동 기반 통제로 확장

# 시스템 설계


조회 및 제어
조직 보안 관리자
조직 네트워크 보안 통계
수동 네트워크 접근 제어
주간 이상 사용자 목록
LOG
유형/사용자별 행동 로그
이상 사용자 자동 차단 알림
웹 페이지
모니터링 모듈
주간 이상 탐지 요청
네트워크 제어 요청
이상 탐지 모듈
주간 행동 로그
이상 사용자 목록
네트워크 상태 및 제어 결과
이상 사용자 목록
네트워크 제어 모듈
행동 로그
연결된 PC 정보
방화벽 제어
로그 수집 및 저장 모듈
행동 로그
PC
라우터
WAN
조직 네트워크

# 기능

## 로그 수집 및 저장

- 엔드포인트 에이전트가 **사용자 행동 로그** 실시간 수집
- Fluentd 파이프라인으로 원본 로그 전처리·필터링·정규화하여 중앙 수신 API로 전송

## 이상 탐지

- 데이터베이스에서 주 단위 사용자 활동 데이터 조회
- 전처리기가 로그 병합, 숫자 변환, 피처 추가 수행
- 사전 학습된 XGBoost 모델이 전처리된 데이터로 사용자의 이상 클래스별 확률 분포 반환
- 이상 확률이 임계값을 넘는 사용자는 탐지 목록에 추가 후 데이터베이스에 저장

## 네트워크 제어

- 이상 사용자 PC의 네트워크 연결 허용 및 차단
- 라우터에서 주기적으로 현재 연결된 PC의 목록을 스캔하여 메인 프레임에 보고
- 특정 PC에 대한 접근 제어 요청 발생 시 라우터의 SSH 서버에 접속하여 방화벽 규칙 자동 적용

## 모니터링

- 조직 네트워크 보안 상태를 웹 대시보드로 시각화
- 이상 탐지 결과·격리 현황·로그 흐름을 한눈에 보여주고 알림/감사 이력 제공

# 강점

# 감사합니다.