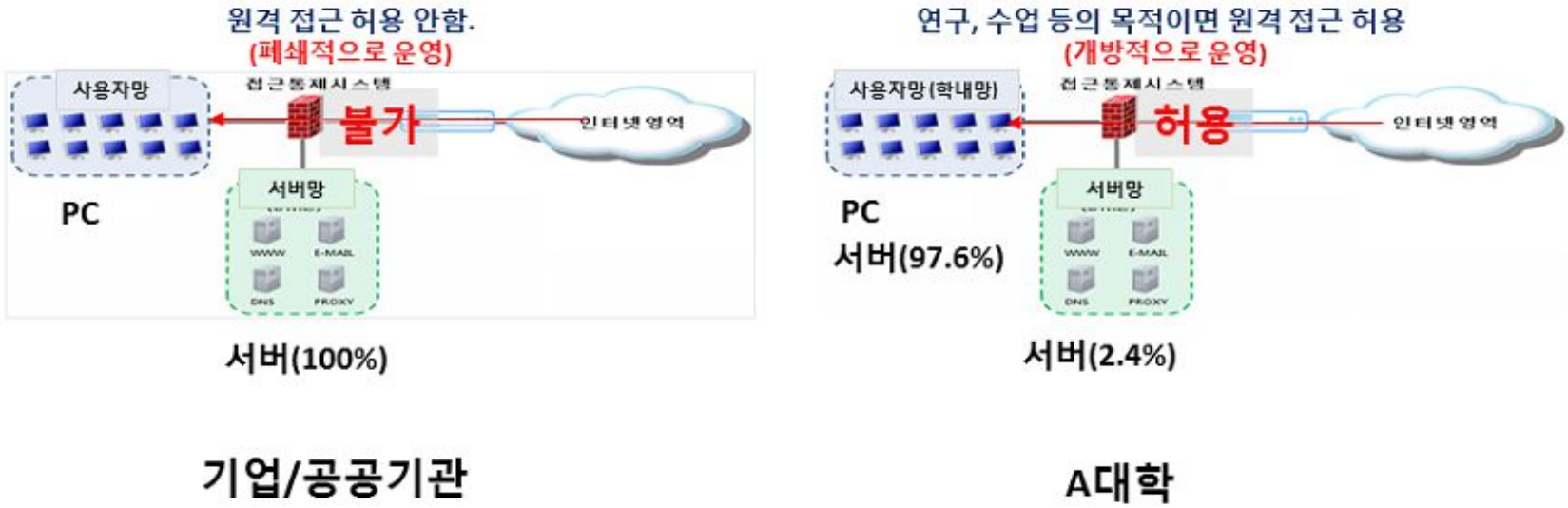
대학에서 왜 K-ISMS 의무인증에 대해 반대할까요?

- **ISMS의 실효성?**
  - 대학의 환경과 목적?
  - ISO27001 *vs* K-ISMS
- **의무인증?**
  - 공인인증서?
  - *Unknown Attack?*

☞ 대학의 학내망과 기업/공공기관 사용자망의 차이점

구분	기업/공공기관의 사용자망	대학의 사용자망(학내망)
운영방식	**폐쇄망** (원격으로 내부망에 접근 불가)	**공개망** (인터넷에서 서버,PC 등에 원격 접근 허용)
중점 보안	**기밀성, 무결성 보장**	**가용성 보장**
정보시스템	위치 할 수 없음.	**다수 위치** A대, 97.6%인 2,000대가 내부망에 위치 운영 주체 : 교원, 학생 등 다양
이용자 구분	직원(only)	**교원/학생/직원/방문객/지역주민 등**
물리적 환경	특정 건물에 이용자, 단말 밀집,	**캠퍼스 전역에 이용자, 정보시스템 등 전산 자원 산재** **(A대, 79개 건물, 1500개 이상의 연구실 등)**
단말 환경	표준화	**거의 모든 종류 단말 혼재**
보안정책	의무, 강제	**권고, 강제 불가한 영역**
특 징	폐쇄성, 기밀성, 무결성 보장	**학술, 연구, 교육활동이 최우선 보장되어야 하고, 이 가치가 훼손되지 않은 적정수준보안이 요구되는 공간, 빠르게 개방되고, 자원이 공유되는 영역**

사용자망 원격접속정책



A대는 운용하는 전체 서버의 97.6%(최소 2000대)가 사용자망에 위치하고, 연구 및 수업을 위해 사용자망으로의 원격 접속을 허용한다.

과연 대학에 K-ISMS 의무인증하는게 적절한가?

- **과연 대학에 ISMS 실효성?**
  - K-ISMS가 따른다는 ISO 27001에서조차 각 항목은 부록으로 선택사항으로 제안되고 있었으며 최근에는 기관에 따라 부록에 나와 있지 않은 항목에서도 자율적으로 설정해도 인증을 주는 것으로 바뀜: unknown attack에 대한 역량확보
  - 대학의 경우 '정보보안과 개인정보보호수준진단'을 통해 2011년부터 매년 교육부와 행정자치부를 통해 보안에 대한 노력: 새로운 보안위험에 대비해 매년 기준 업데이트
- **의무인증**: 자율적인 대학에 맞는 보안체계 마련 노력
  - 위기시 법적/경제적 책임을 미래부나 인터넷진흥원이 대신 해 줄 것인가?
  - 해커 입장에서는 기준이 모두 노출되고 unknown attack에 취약한 구조
  - ISO 27001과 상호인증 필수: 일본의 경우 상호인증을 통해 세계 최다 ISO27001 인증기관 (민간)
- **제안**: Education-Information Security Management System을 자율적으로 설정하여 대비하겠다.