# 온라인 수업시의 시큐리티관련 주의사항

**1． Teams 또는 Zoom 으로 수업을 들을 경우**

① 시스템 업데이트 알림이 오면 바로 업데이트 할 것
② LMS(수업지원시템)를 통해서 전달받는 수업용 미팅 URL 이나 ID, 패스워드는 신중히 관리하도록 하고, 절대로 제 3 자에게 전달하거나 알리지 말 것
③ 수업 참가시 성명, 비디오, 마이크 등에 대한 룰에 대해서는 해당 수업 교수님의 지시에 따를 것
④ 수업을 녹화하거나 사진(스크린샷 포함) 찍지 말 것, 또한 수업에서 제공되는 영상자료를 포함한 모든 자료에 대해서는 어떠한 형태로든 공유하지말 것

※「요코하마국립대학교 정보 레벨관리 기준 및 정보 레벨 취급 가이드라인」에 의함

**2. 컴퓨터 보안관리에 대해서**

（１）백신 소프트 Apex One 은 항상 최신 버전으로 유지할 것. 교내 와이파이가 사용가능할 경우는 정보기반센터 홈페이지에서 무료로 다운로드 가능.

https://www.itsc.ynu.ac.jp/security/vb_haifu.html

① Apex One 에 예약검색 기능을 설정해 두어 정기적으로 스캔할 것
② 매달 10 일, 20 일, 30 일은 Malware 를 체크하도록 정해진 CheckDay 이므로 해당일에는 풀스캔 하도록 할 것
③ 해외에서 수업을 듣거나 캠퍼스에 들어 올 수 없는 학생의 경우는 각자 바이러스 백신 소프트를 준비하여 사용하시기 바랍니다.

（２）패스워드 관리

① 패스워드는 알파벳 대문자, 소문자, 숫자, 기호를 섞어서 강력한 것으로 설정 할 것
② 적어도 10 자 또는 그 이상으로 설정할 것
③ 패스워드 변경시 이전에 사용한 적이 있는 패스워드와 유사한 패스워드로 설정하지 말 것
④ 사용한 적이 있는 패스워드를 반복해서 사용하지 말 것

（３）OS/소프트웨어 관리

① OS/소프트웨어는 항상 최신버전으로 해 둘 것
② 제품 서포트가 중단된 OS/소프트웨어는 사용하지 말 것
③ 사용하지 않는 소프트웨어는 삭제할 것
④ 신뢰할 수 없는 프리소프트웨어는 인스톨하지 말 것