# APT대응시스템 Agent 배포 안내

## ○ 목적

- 신·변종 악성코드 및 악성파일 등 위협트래픽으로부터 캠퍼스전산망의 안정성을 높이고 사용자 PC의 보안을 강화하고자 함

**※ APT(Advanced Persistent Threat) : 지능적이고 지속적인 해킹 위협, 백신이나 방화벽 같은 보안체계를 우회하는 사례가 많아 지능적이라고 평가됨**

## ○ 운영방식

- 알려진 악성코드 및 악성파일 탐지/대응

· C&C서버 및 악성사이트 접속시 차단 → 안내페이지로 연결

· 악성파일 다운로드시 삭제(복원 가능) → 안내 팝업 표시

- 감염된 PC 시스템 격리

※ 알려지지 않은 악성코드 및 악성파일에 분석 실행하여 악성 여부 판별

## ○ 에이전트 사용 환경

- 대상 : 윈도우7, 8(8.1), 10
  윈도우서버 2003 SP2이상, 2008, 2012, 2016

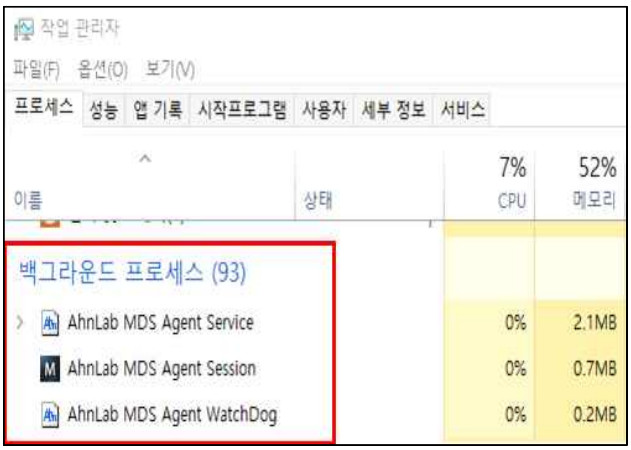
  ※ 32, 64bit 지원

## ○ 추진 일정

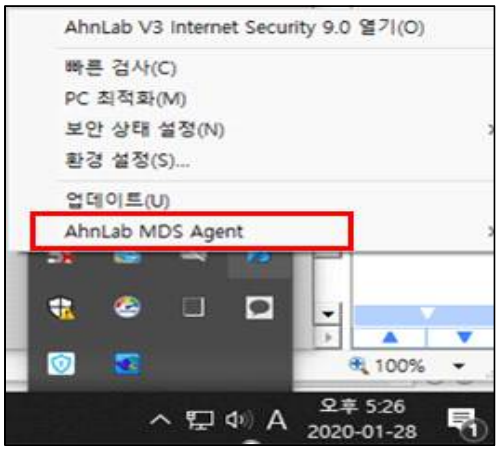
- 배포 일정 : 2020.2.3. ~
- 배포 방법 : 학내 PC에 설치된 V3나 컴보이 서버를 통해 자동 배포
  (※수동설치 : 포털의 게시판에서 설치파일 다운로드)

- 설치된 프로세스 확인 방법

① 작업관리자




② V3아이콘(트레이) 클릭 후 오른쪽 마우스 클릭




- 수동설치 방법

· 포털에 로그인한 후 스누인 지원 클릭 > 캠퍼스라이선스SW다운 > 게시물 3번 “PC보안 (MDS Agent, 구 좀비PC탐지)” 참고

## ○ 기타

- 백그라운드 프로세스로 설치되어 해당 PC사용자가 설치과정을 인지하지 못함
- 에이전트 프로세스의 성능을 최적화하여 시스템의 부하를 최소화함
- C&C서버나 악성URL접속시 차단됨(안내페이지로 자동 연결)