

문서유출탐지프로그램(DocuMon) 관련사항 안내

DocuMon은 공유 또는 해킹프로그램(Peep과 같이 외부에서 접근하였을 경우)을 통하여 외부에서 사용자의 PC에 접근하여 hwp, xls, ppt, doc와 같은 문서에 마우스를 클릭하거나, 파일을 열었을 경우에 경고창이 뜨게 되어 사용자가 자신도 모르는 사이에 중요 문서가 유출되는 것을 탐지하는 기능을 수행하도록 하였습니다.

단, DocuMon은 외부에서 중요 문서에 접근했을 경우, 사용자에게 이를 사전에 알려 중요 파일의 외부유출에 대비하는 기능을 할뿐, 원천적으로 파일 읽기를 막거나 유출을 방지할 수 없음을 유념해야 합니다.

인스톨파일을 실행하면 C:\Program Files\WormCheck\DocuMon 폴더에 설치가 된다. 3개의 파일이 이 디렉토리에 설치됩니다. Filem.sys 등이 손상되었거나 이 디렉토리에 없으면 프로그램 자체가 실행되지 않습니다.

DocuMon.exe : DocuMon 실행파일

DucuMon.sys : DocuMon 시스템 파일

DocuMon.log : 탐지 로그 기록

DocuMon.exe를 실행하면, 윈도우 우측하단 (윈도우 시계가 위치한 곳)에 아이콘이 생성됩니다. 이 아이콘을 우클릭하면

- 로그 창 보기
- 모니터링 중지
- About
- 종료

4가지의 기능을 사용할 수 있습니다. 이 중에서 모니터링 중지기능은 파일 찾기, 하드디스크 정리, 에드웨어 탐지 프로그램, 백신 검사(실시간 감시는 상관없음) 등을 작동시킬 때 등 여러 파일을 접근하는 프로그램을 구동할 경우에는 모니터링 중지 기능을 사용하여 불필요한 경고창이 뜨거나 시스템에 과부하를 주지 않도록 하시기 바랍니다.

위와 같은 사항을 유념하시어 사용하시기 바랍니다.

이 프로그램은 윈도우 XP, 2000 버전에 최적화 되어 있으며, 98, Me 버전에서는 작동되지 않습니다.

또한, 특정 프로그램을 설치할 동안에 경고창이 뜰 수 있으므로 DocuMon을 일시 중지 시켜 주시기 바랍니다.

프로그램 버그, 개선사항이 있으면 국가사이버안전센터의 아래 주소로 메일 보내시기 바랍니다.

E-mail: analysis@ncsc.go.kr