랜섬웨어 대응 방법
매뉴얼
(공지용 자료)

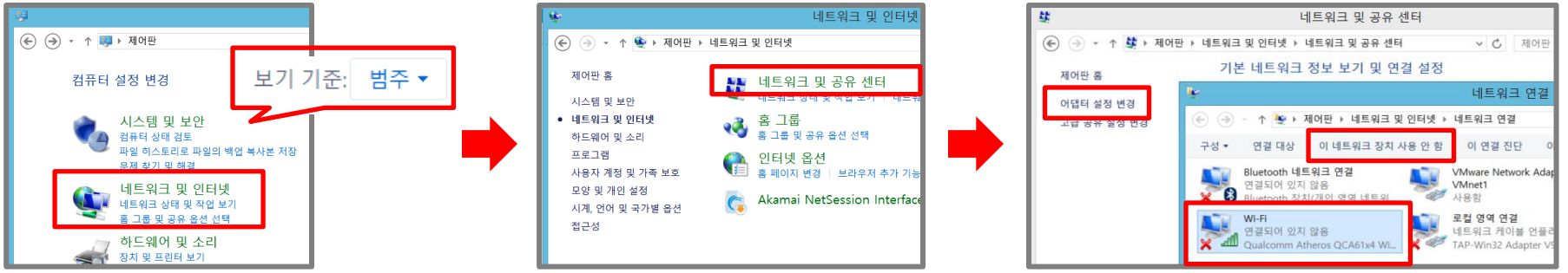
2017년 5월

이수시스템㈜

1. PC 방화벽 SMB 포트 차단 방법

(1) PC 켜기 전 네트워크 단절 (Windows 버전 전체 동일)

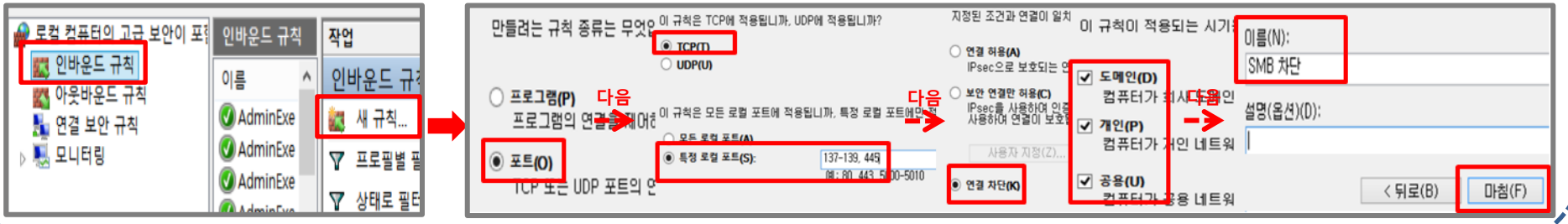
- 유선인 경우 : PC 본체에서 랜선 물리적 분리
- 무선인 경우 : [제어판] > [네트워크 및 인터넷] > [네트워크 및 공유 센터] > [어댑터 설정 변경] > [Wi-Fi] > [이 네트워크 장치 사용 안 함]



(2) PC 방화벽 SMB 포트(파일 공유 포트) 차단 (Windows 버전 전체 동일)

- [제어판] > [시스템 및 보안] > [windows 방화벽] > [고급 설정]

- [인바운드 규칙] > [새규칙] > [포트] > [특정 로컬 포트 : 137-139, 445] > [연결 차단] > [도메인, 개인, 공용] 체크 > [이름 설정 : SMB 차단(임의 설정)]



2. 윈도우 업데이트 방법

● 보안 업데이트 (Win 7, 8, 8.1 버전)

- [제어판] > [시스템 및 보안] > [Windows 업데이트] > [업데이트 확인] > [업데이트 진행]
- 보안 업데이트 자동 설치 설정 : [Winddows 업데이트] > [설정 변경] > [업데이트 자동 설치(권장)]

● 보안 업데이트 (Win 10 버전)

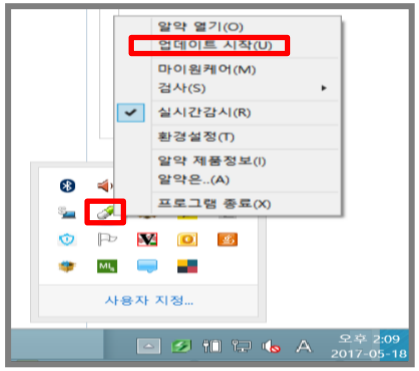
- [시작] > [설정] > [업데이트 및 복구] > [Windows 업데이트]
- 보안 업데이트 자동 설치 설정 : [Winddows 업데이트] > [고급 옵션] > [자동(권장)]

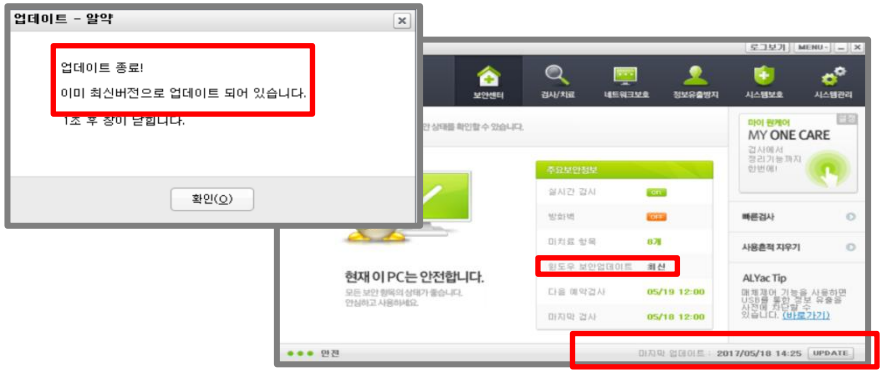
3. 백신 업데이트 및 시스템 보호 설정 방법

● 백신 보안 업데이트 최신 상태 유지 (Windows 버전 전체 동일)

- [알약] 우 클릭 > [업데이트 시작]

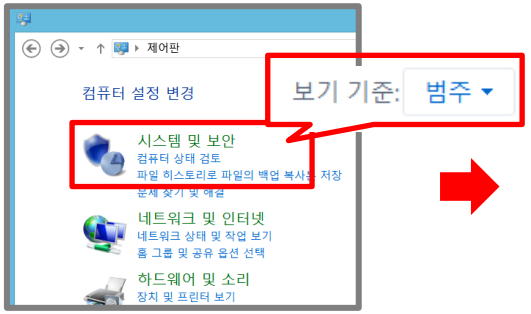
※ 정책 상 기본 검사(매일 12시) 및 자동 업데이트가 진행되므로 마지막 업데이트 일이 최신이 아닐 경우 실시

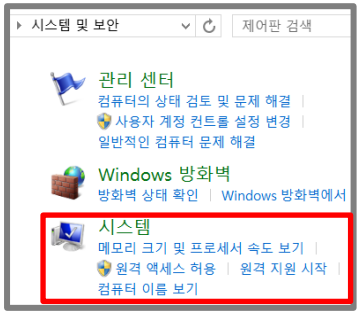


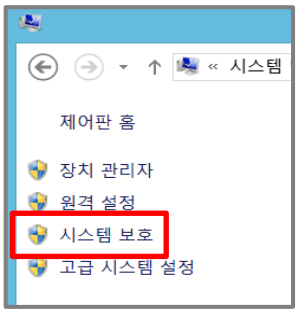


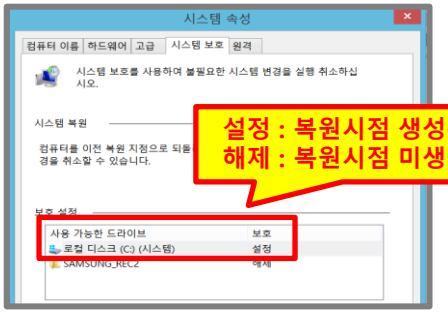
● 시스템 보호 설정 (Windows 버전 전체 동일)

- 사용 드라이브가 보호 설정되어있는지 확인 : [제어판] > [시스템 및 보안] > [시스템] > [시스템 보호]

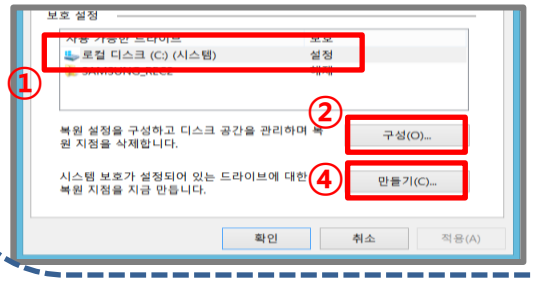


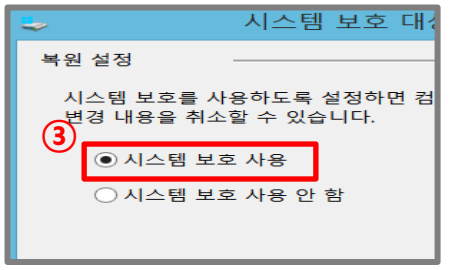


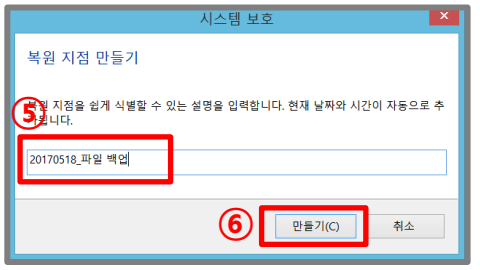




- 복원시점이 없는 경우 : 해당 드라이버 선택 > [구성] > [시스템 보호 사용] > [확인] > [만들기] > [임의 이름 설정] > [만들기]







- 그 외 행동요령
  - 발신자가 불명확한 메일 클릭 및 파일 다운로드 금지
  - 웹사이트 접속 주의 (국내외 포털 사이트 외 접속 자재)

    ※ 의심되는 사이트 및 파일 시 www.virustotal.com 에 접속하여 사이트의 안전상태 체크
  - 윈도우 XP 이하 버전일 경우 윈도우 7 이상으로 업그레이드

- 랜섬웨어(Ransomware) 감염 시 행동방안
  - 랜섬웨어 감염이 의심되는 PC의 네트워크를 즉시 차단하신 후 전산 담당 부서 혹은 이수시스템 담당자에게 연락

    - 담당자 연락처 : 02 – 590 - 6732 , 6769 , 6733 , 6756
  - 컴퓨터 확인 후 감염 확인 시 포맷 진행

End of Document