

# 「랜섬웨어 예방 요령」

2017. 5. 14.



미래창조과학부



한국인터넷진흥원



## 1 랜섬웨어 방지 대국민 행동

### 1. PC를 켜기 전 네트워크 단절



※ 이미지 출처: Getty Images Bank

- 랜선 뽑기
- 와이파이 끄기

### 2. 감염 경로 차단



- 방화벽 설정 변경
- \* 붙임 참고

### 3. 인터넷 재연결 후 보안 업데이트



Windows Update

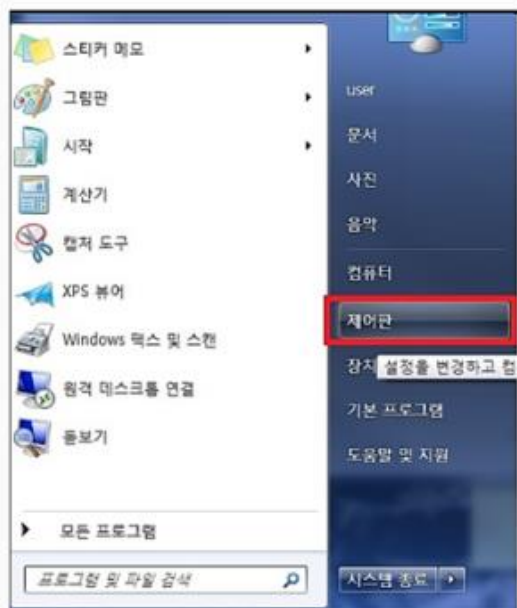


- 윈도우 보안 패치 실행
- 백신 프로그램 업데이트

## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

(1) [제어판] → [시스템 및 보안]

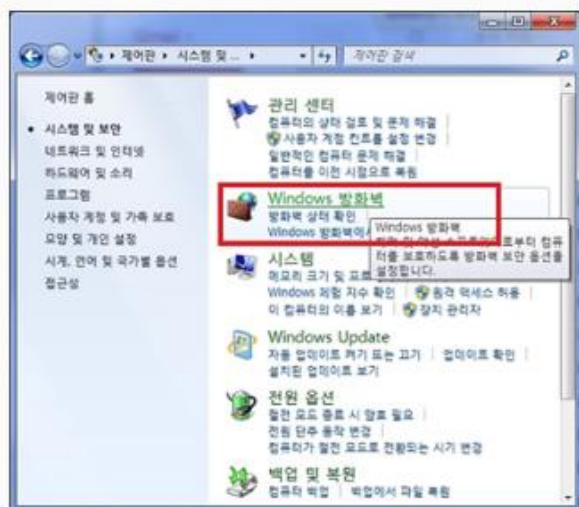


- 2 -

## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

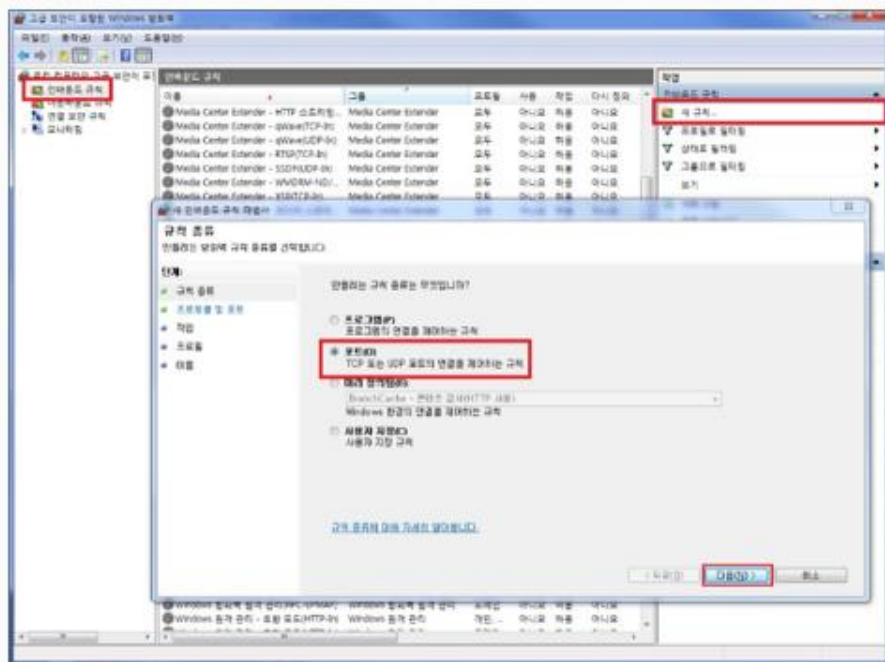
(2) [Windows 방화벽] → [고급 설정]



## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

(3) [인바운드 규칙] → [새규칙] → [포트] → [다음]



- 4 -

## 3 PC 보안설정 변경 - 파일 공유 기능 해제

Window 방화벽에서 SMB에 사용되는 포트 차단

(4) [TCP] → [특정 로컬 포트] → [139, 445] → [다음]



- 5 -

## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

(5) [연결 차단] → [다음]

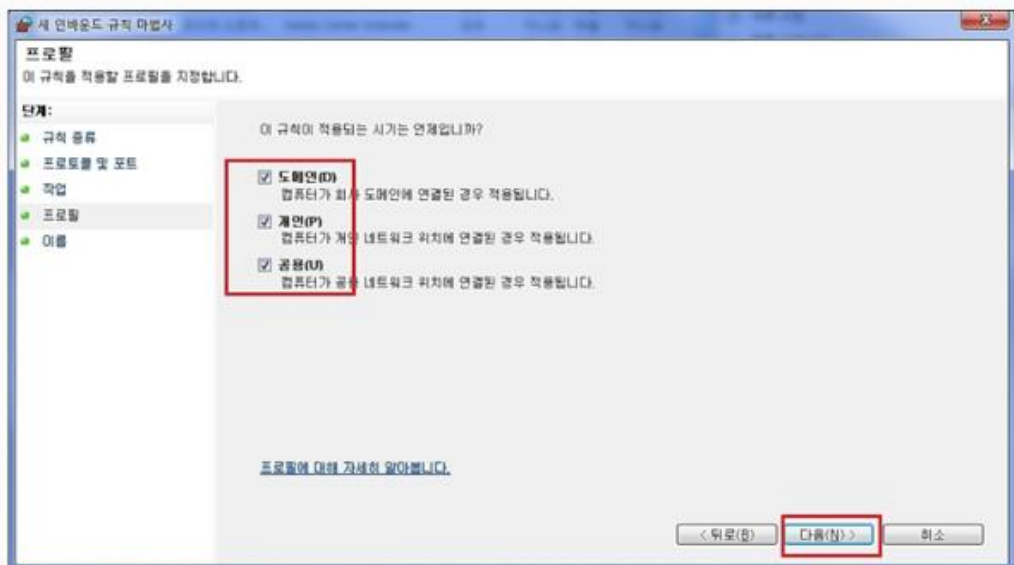


- 6 -

## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

(6) [도메인, 개인, 공용 체크 확인] → [다음]



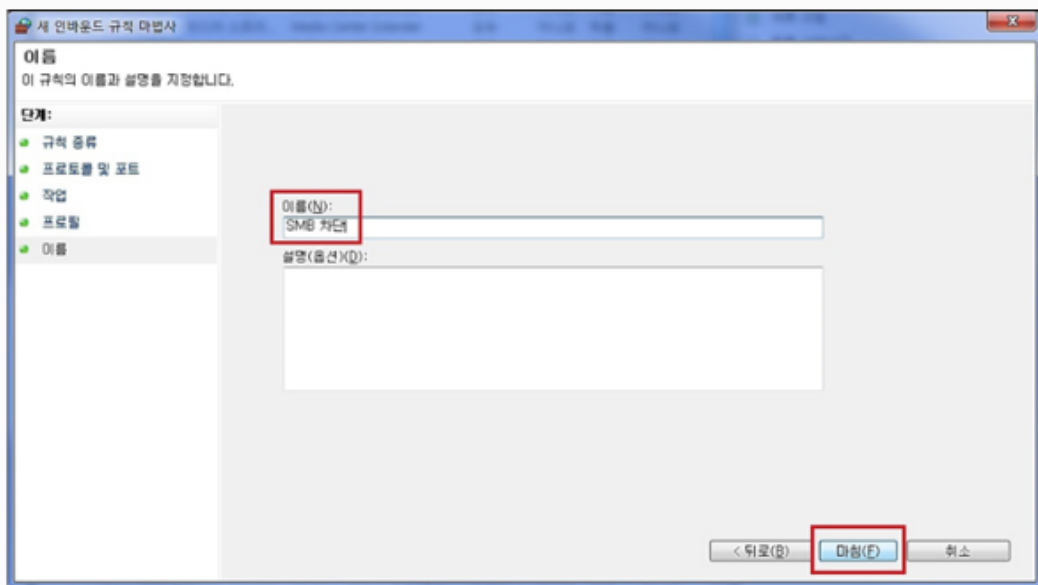
- 7 -



## 2 파일 공유 기능 해제 - 방화벽 설정

Window 방화벽에서 SMB에 사용되는 포트 차단

(7) [이름 설정] → [마침]



- 8 -

□ 기타 해결 방안(아래 버전을 사용하는 경우, 다음과 같은 방안으로도 해결 가능)

○ Windows Vista 또는 Windows Server 2008 이상 사용자

시작 -> 'Windows Powershell' 입력 -> 우클릭 -> 관리자 권한으로 실행 ->

① set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlset\Services\Lanmanserver\Parameters" SMB1 -Type DWORD -Value 0 -Force

② set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlset\Services\Lanmanserver\Parameters" SMB2 -Type DWORD -Value 0 -Force

○ Windows 8.1 또는 Windows Server 2012 R2 이상 사용자

클라이언트 운영체제 : 제어판 -> 프로그램 -> Windows 기능 설정 또는 해제

-> SMB1.0/CIFS 파일 공유 지원 체크해제 -> 시스템 재시작

서버 운영체제 : 서버 관리자 -> 관리 -> 역할 및 기능 -> SMB1.0/CIFS 파일 공유 지원 체크 해제

-> 확인 -> 시스템 재시작