** 국내 대표 포털 사이트 접속 시(네이버, 다음 등등) 파밍 사이트로 접속된다면 사용중인 공유기의 펌웨어 업그레이드 및 공장 초기화를 진행 하신 다음 공유기의 보안 강화 설정을 하여 주시기 바랍니다.

공유기의 보안 강화 설정은 다음과 같습니다.

첫번째 공유기 공장초기화 하기

두번째 공유기의 관리자 암호 설정 하기

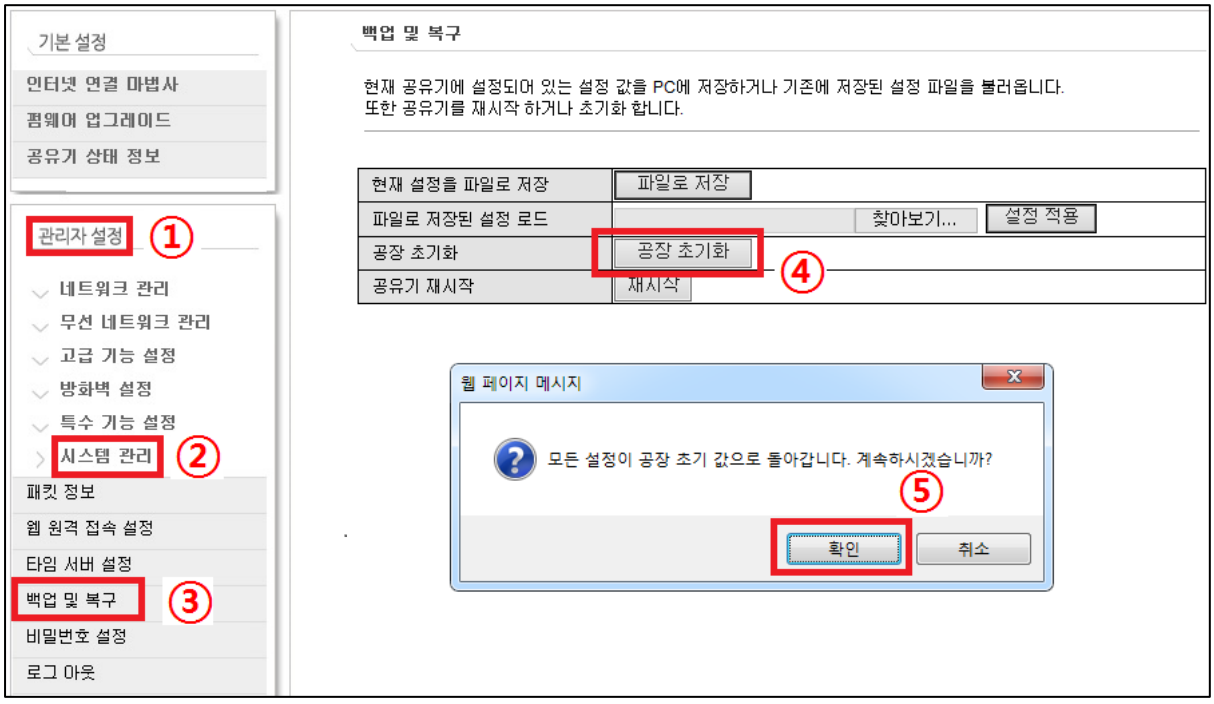
세번째 공유기의 원격 웹 접속 포트 설정 [사용 안함]으로 설정 하기

네번째 공유기의 무선 암호 설정 하기

☞ 공유기 공장초기화 절차

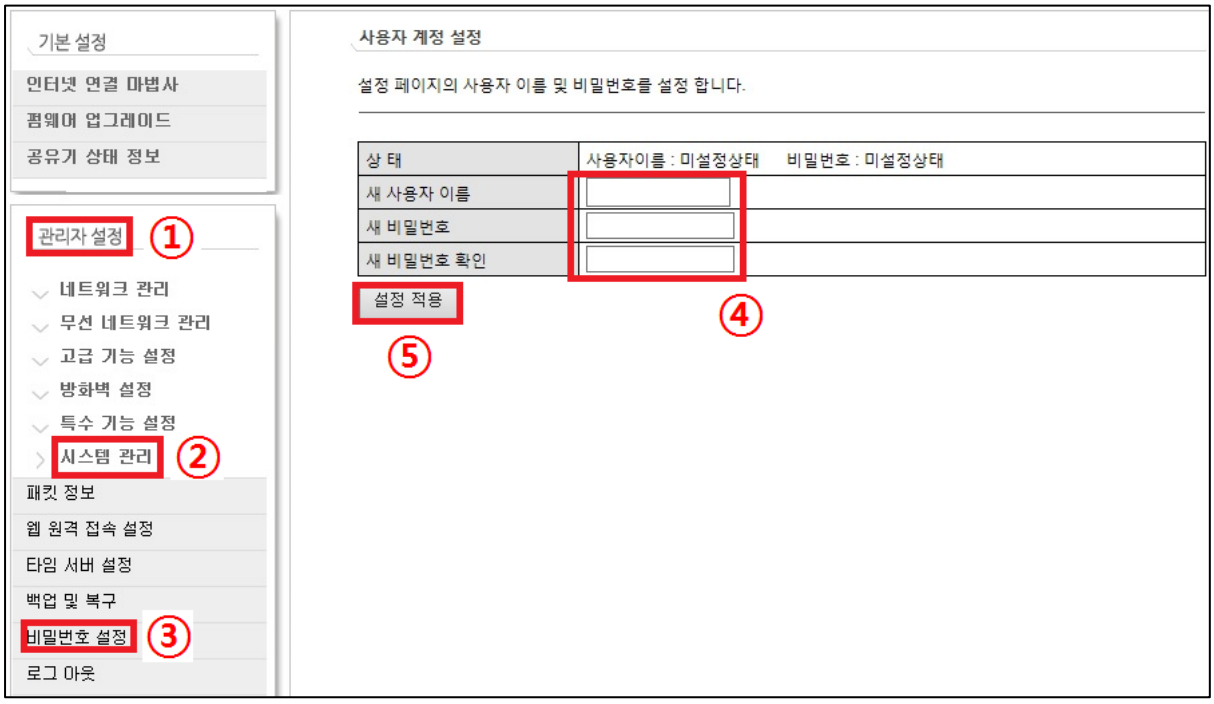
공유기 설정 페이지의 설정 메뉴 중 [관리자 설정] → [시스템 관리] → [백업 및 복구] → [공장초기화] 버튼을 누른 뒤 확인 버튼을 클릭 합니다.

(공장 초기화 시 기존의 설정 값이 지워지므로 이 점 유의하시기 바랍니다.)



☞ 관리자 암호 설정 절차

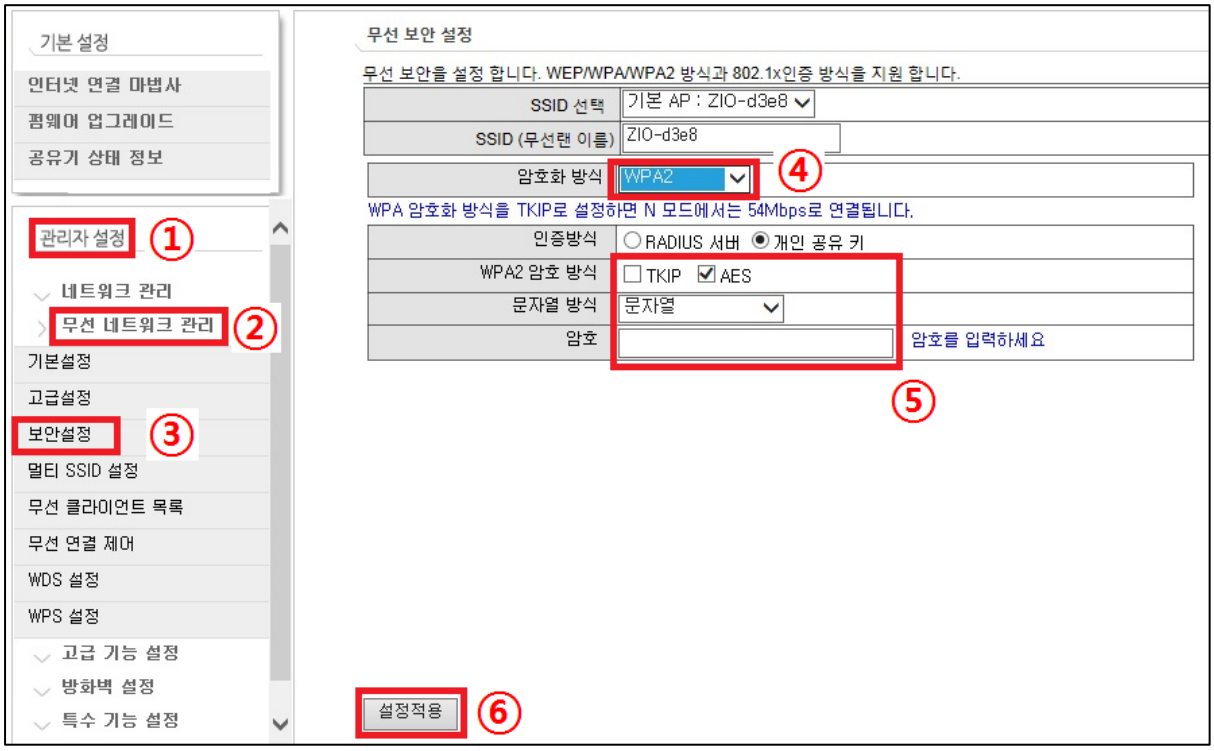
공유기 설정 페이지의 설정 메뉴 중 [관리자 설정] → [시스템 관리] → [비밀번호 설정] → [새 사용자 이름/새 비밀번호/ 새 비밀번호 확인]에 설정하고자 하는 사용자 이름과 비밀 번호 입력 → [설정 적용]버튼 클릭 합니다.



적용 후 설정페이지(192.168.10.1)에 재 접속 후 환경설정 선택을 하였을 때 아이디와 비밀번호 입력 창이 나오면 정상적 적용된 것입니다.

☞ **무선(WI-FI)암호 설정 하기**

공유기 설정 페이지의 설정 메뉴 중 [관리자 설정] → [무선 네트워크 관리] → [보안 설정]에서 무선 암호 설정 → [설정 적용]버튼 클릭 합니다.



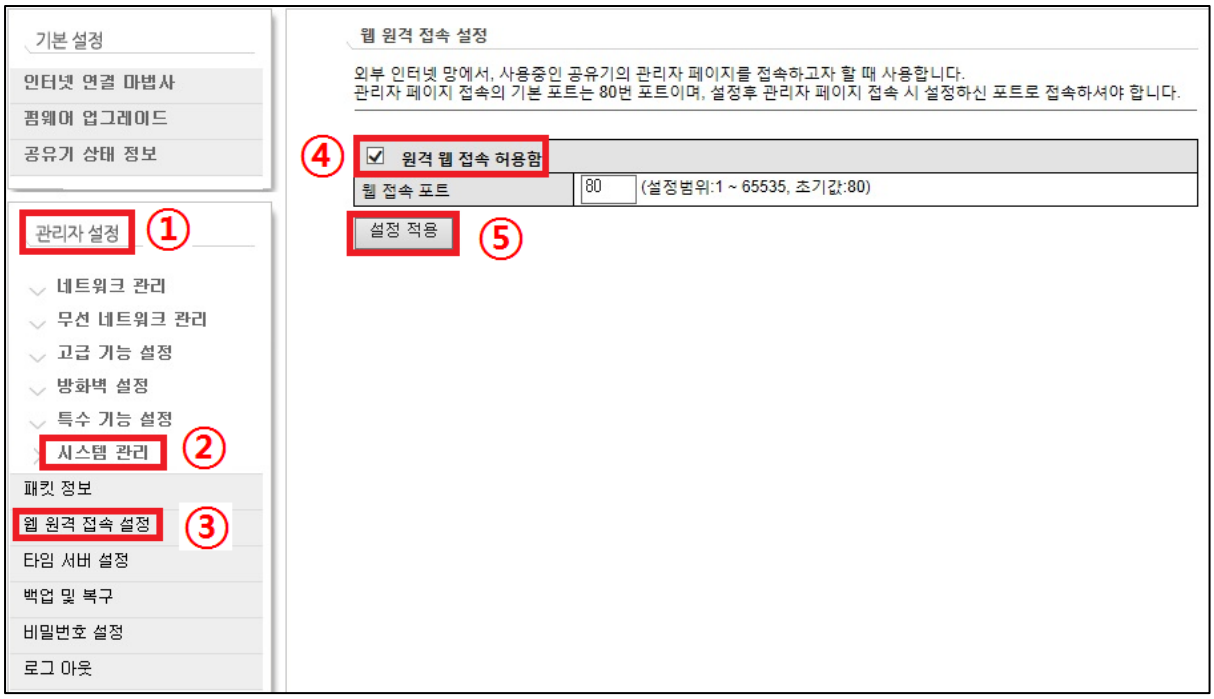
설정 내용

- 암호화 방식 : WPA2 방식 권장
- WPA2 암호 방식 : AES 권장
- 문자열 방식 : 문자열 권장
- 암호 : 8자리 이상의 영문 문자 및 숫자 권장

※ 설정 적용 후 기기에서 변경된 이름(SSID)를 선택 후 지정하신 비밀번호를 입력하시면 무선 사용이 가능합니다.

☞ **원격 웹 접속 설정 해제하기**

공유기 설정 페이지의 설정 메뉴 중 [관리자 설정] → [시스템 관리] → [웹 원격 접속 설정] → [원격 웹 접속 허용함]을 체크 해제→ [설정 적용]버튼 클릭 합니다.



위와 같이 설정을 하였음에도 계속 파밍 사이트로 접속이 된다면 PC 내에 있는 악성코드를 치료하시길 바랍니다.

악성코드 치료 방법 클릭 (KISA 보호나라 사이트)