[붙임1]

유무선 공유기 보안가이드

2018년 5월

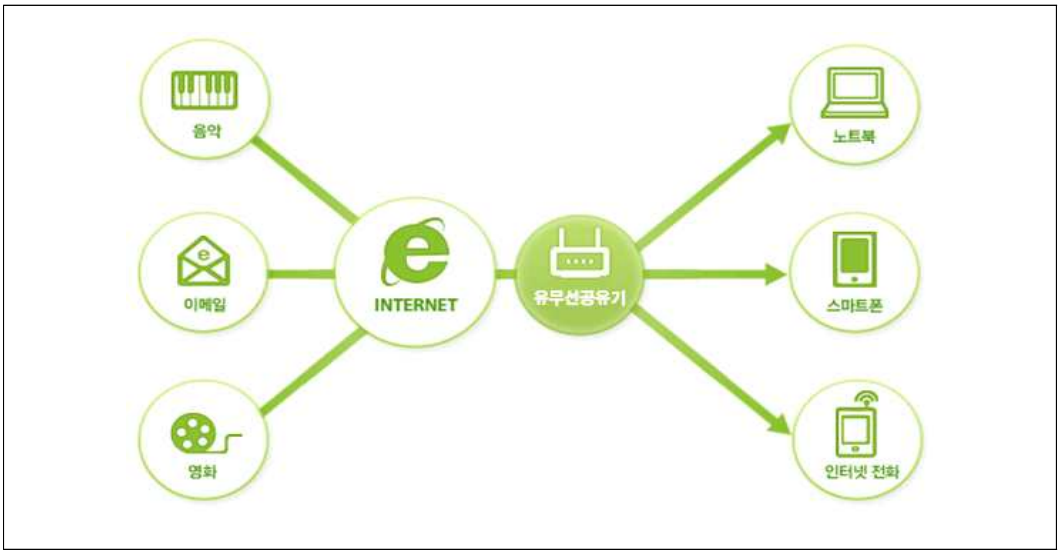
서울대학교 정보화본부
Information Systems & Technology

<목 차>

I. 공유기 보안

□ 유무선 공유기란?

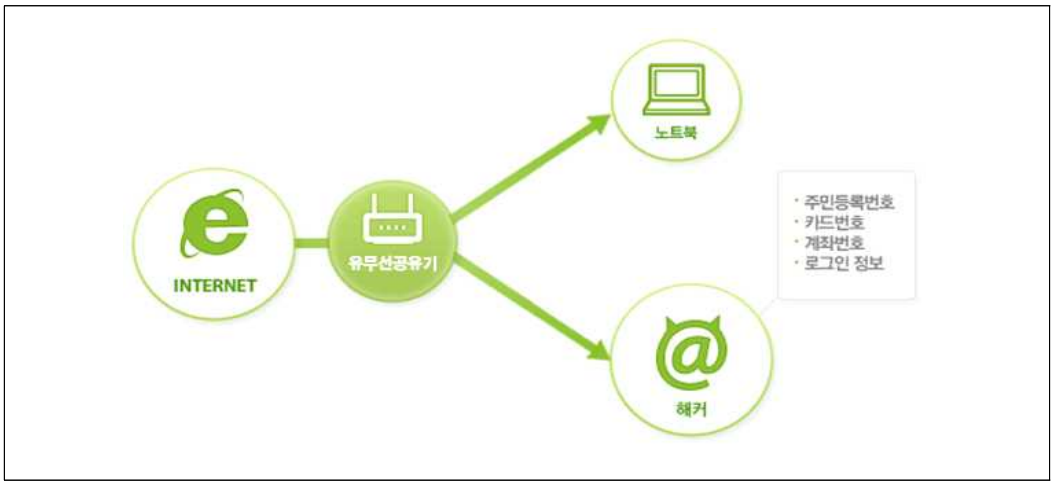
- PC, 스마트폰 등 다양한 기기를 인터넷에 접속할 수 있도록 연결해주는 중간 매개체
- 유무선공유기를 통해 선 없이 인터넷에 접속할 수 있는 무선랜 환경 구축이 가능하여 널리 사용됨



[그림1] 유무선 공유기 사용 환경

□ 공유기 보안의 필요성

- 보안을 설정하지 않은 경우, 외부인이 공유기를 무단으로 사용 가능
- 해커가 접속하여 해킹, 개인정보유출 등 다양한 보안사고 발생 가능



[그림2] 공유기 보안의 필요성

□ 공유기 환경에서의 해킹 유형

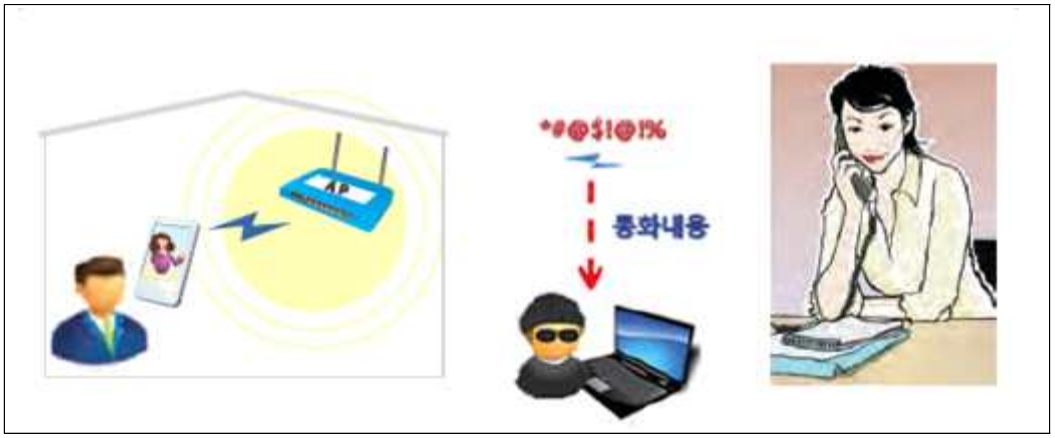
(1) 이용자의 중요한 정보 유출

- 보안이 설정되지 않은 무선랜으로 인터넷을 이용할 경우 악의적인 목적의 사용자가 접속하여 비밀번호 등 개인의 중요한 정보를 유출

[그림3] 무선랜을 통한 개인정보 유출

(2) 인터넷전화 도청 위험

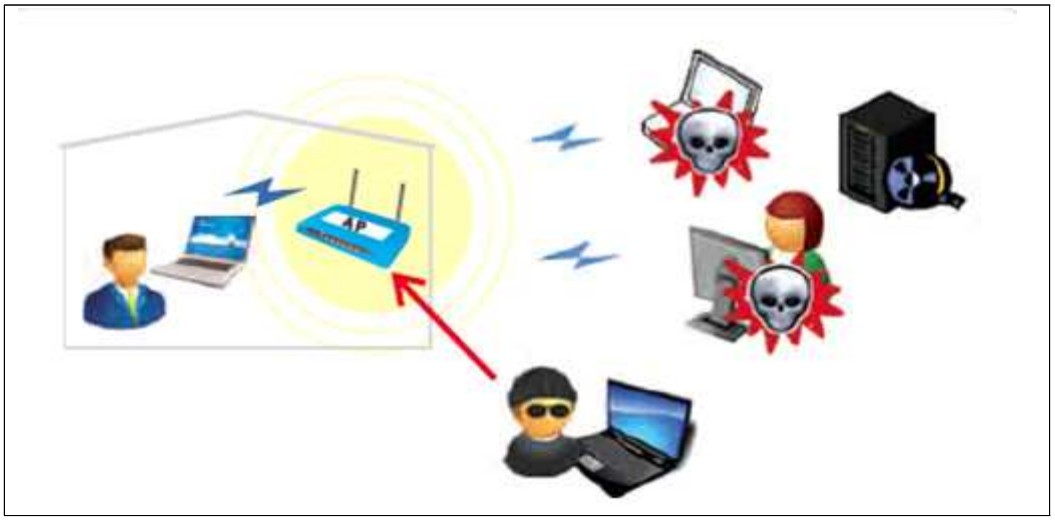
- 보안이 설정되어 있지 않거나 취약한 유무선 공유기에 접속하여 인터넷 전화를 이용할 경우 통화내용이 도청이 가능



[그림4] 무선랜을 통한 통화내용 도청

(3) 자신의 유무선 공유기가 악의적으로 이용될 위험

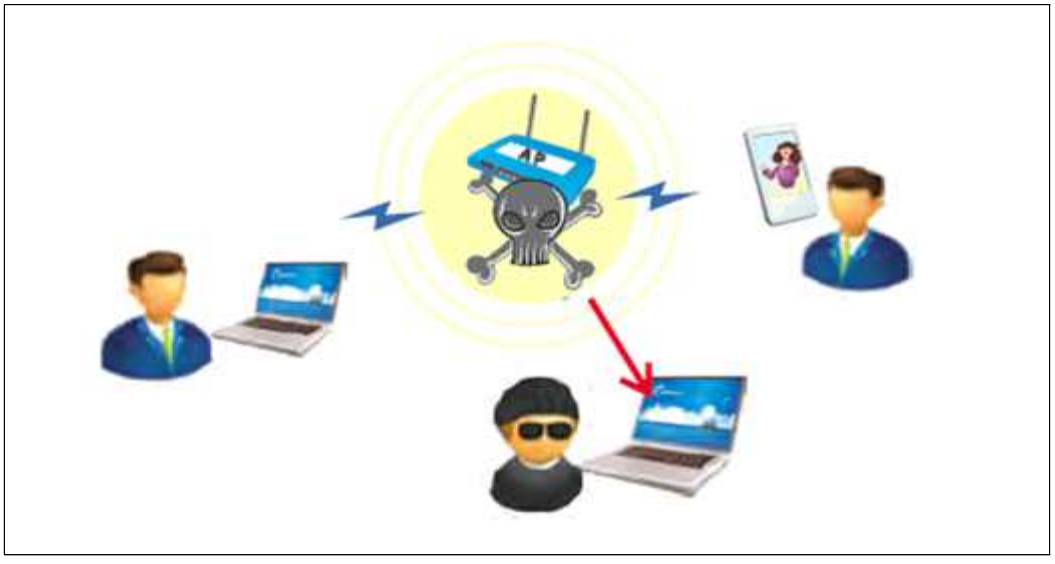
- 보안이 설정되지 않은 유무선 공유기는 해킹, 불법 다운로드등에 악용되거나, 바이러스, 악성코드 등을 유포하는 경유지로 활용



[그림5] 무선랜을 통한 불법다운로드, 악성코드 유포

(4) 악의적으로 설치된 무선랜에 접속되어 개인정보 탈취

- 해커가 개인정보 탈취 등의 목적으로 구축한 무선랜에 접속할 경우 사용자의 개인정보가 유출될 수 있음



[그림6] 불법 무선랜 이용에 따른 개인정보 유출

Ⅱ. 공유기 보안관리 방법

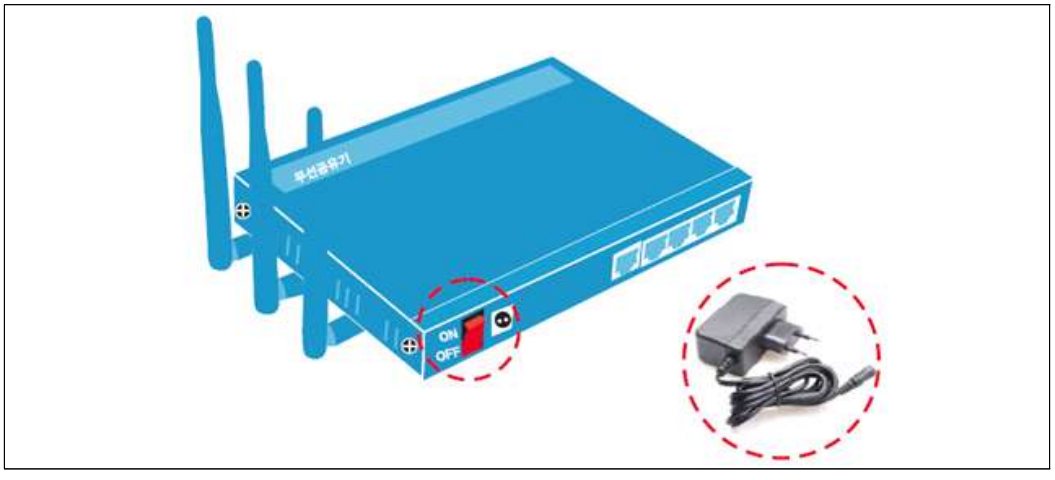
□ 보안 항목

번호	내용	비고
1	공유기 물리적 보호하기	권고
2	공유기 관리자 모드 접속 암호 변경하기	필수
3	SSID 이름변경 및 숨김 기능 설정하기 ※ SSID(Service Set IDentification)	권고
4	유무선공유기 전파출력 조정하기	권고
5	유무선공유기 암호화 설정하기	필수
6	주기적인 공유기 펌웨어 업그레이드	권고
7	외부접속 포트, Telnet, uPnP, 등의 불필요 서비스는 비활성화	권고

□ 보안 항목별 조치 방법

(1) 공유기 물리적 보호하기

- 유무선 공유기의 경우 무선 서비스를 위해서 장비가 외부에 노출될 수밖에 없음
- 공유기의 설정을 초기화하는 Reset스위치가 노출되어, 무단 설정 변경 위함 발생
- 별도의 수납공간 형태의 분리공간에 설치 및 추가 잠금장치 권고
- 사용하지 않는 무선공유기를 켜 놓을 경우 외부인이 불법다운로드, 해킹 등에 악용
- 전원케이블을 분리하거나, 스위치를 Off



[그림7] 유무선 공유기의 물리적 보호

(2) 공유기 관리자 모드 접속 암호 변경하기

- 유무선공유기에 설치된 초기 비밀번호는 공개되어 있어 타인이 쉽게 접속 할 수 있음
- 인터넷의 검색엔진에서 쉽게 제조사별 초기 비밀번호 확인 가능
- 암호설정 기준

① 9자리 이상 사용
② 숫자 및 영문자, 특수문자 혼용하여 사용
③ 일반 단어가 아닌 한글-영타 암호(예:암호-dkagh)의 사용
④ 주기적인 암호 변경

(3) SSID(Service Set IDentification) 이름변경 및 숨김기능 설정하기

- SSID(Service Set IDentification)은 무선랜을 구분하기 위한 이름
- SSID 이름을 외부인이 쉽게 추측하기 어렵게 변경하여 사용
- SSID 숨김은 SSID 보안설정과 함께 보안성을 높이는 기능
- SSID를 숨김으로서 외부인이 자신의 공유기를 사용하지 못하도록 방어

[그림8] 무선공유기 SSID 보안설정

(4) 공유기 전파출력 조정하기

- 무선공유기의 전파 출력을 조정하지 않아서 사용범위 밖에서 쉽게 접속하는 위험
- 강의실 또는 연구실 밖에서 무단 접속의 위험(복도 또는 건물밖에서 접속)
- 무선공유기를 개인적으로 사용할 경우 무선전파의 출력을 조정하여 사용

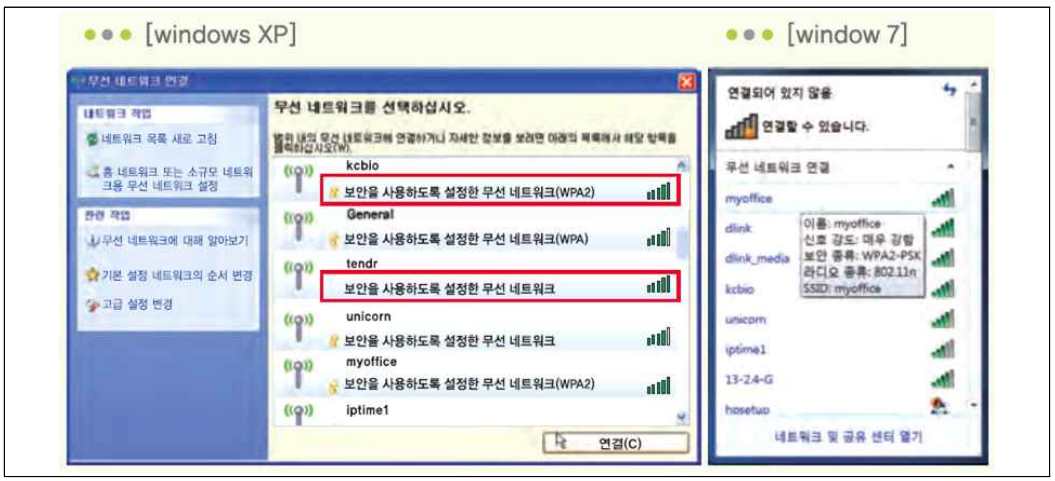
(5) 공유기 암호화 설정하기

- 무선공유기 사용시 암호화/인증 등 보안기능 미설정시 외부인이 무단 사용 가능
- 피해사항은 인터넷이 느려지거나, 개인정보 유출 등의 해킹사고 발생
- 무선공유기의 인증/암호 종류 : WPA2 필수 사용

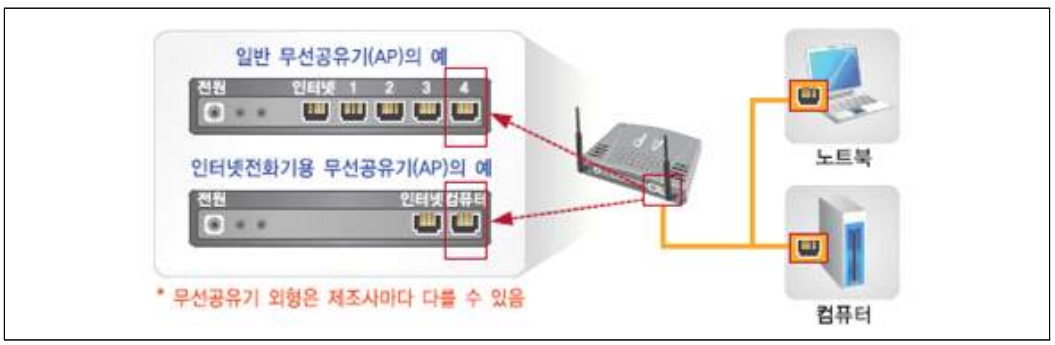
구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인증	사전 공유된 비밀키 사용 (64비트, 128비트)	사전에 공유된 비밀키를 사용하거나 별도의 인증서버 사용	사전에 공유된 비밀키를 사용하거나 별도의 인증서버 사용
암호방법	고정 암호키 사용 RC4 알고리즘 사용	암호키 동적 변경(TKIP) RC4 알고리즘 사용	암호키 동적변경 AES 등 강력한 아호 알고리즘 사용
보안성	가장 취약하여 널리 사용되지 않음	WEP 방식보다 안전하나 불안전한 RC4 알고리즘 사용	가장 강력한 보안 기능 제공

※ 제조사별 암호/인증 설정 방법은 Ⅲ.제조사별 공유기 보안설정 참고

① OS별 공유기 보안설정 상태 확인 방법 : 보안종류 확인



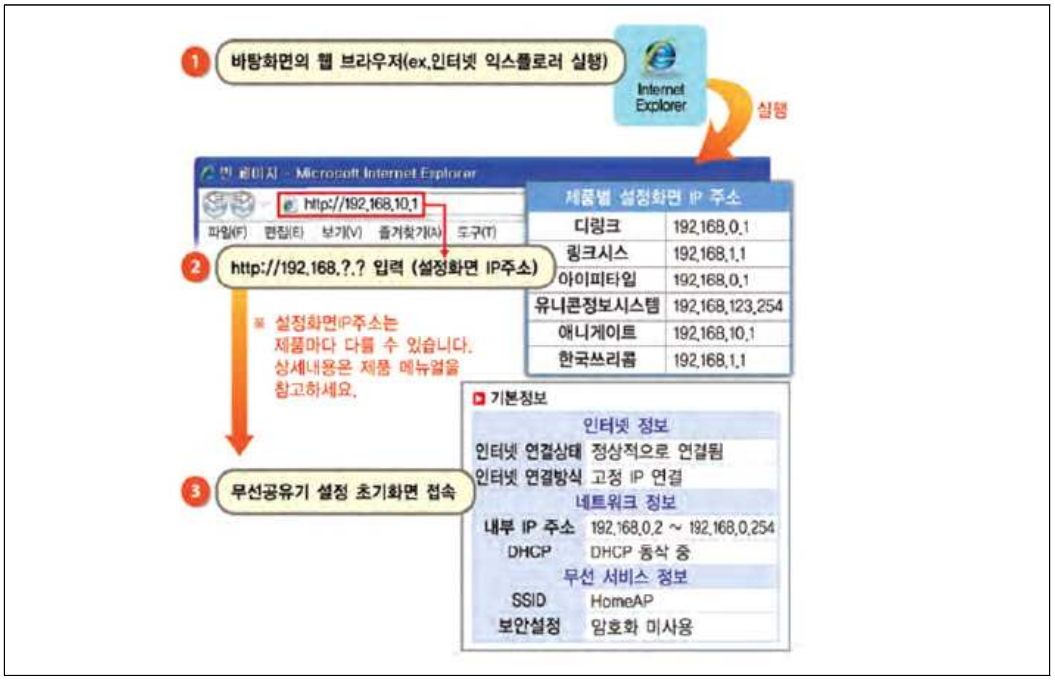
[그림9] 무선네트워크 공유기 보안설정 상태 확인



[그림10] 무선공유기 연결 방법

② 공유기 관리화면 접속

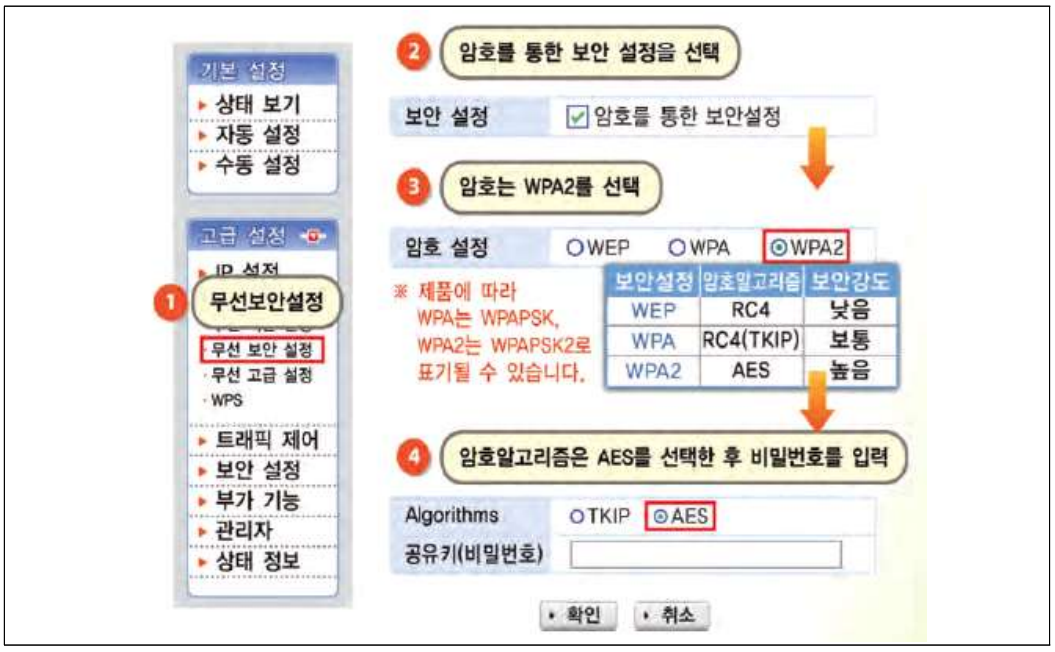
- 제조사별 접속IP를 확인 → 관리자 접속



[그림11] 무선공유기 관리화면 접속

③ 공유기의 인증/암호 설정

- 무선보안설정 → 암호를 통한 보안설정 선택 → 암호방법 선택



[그림12] 무선공유기 관리화면 접속

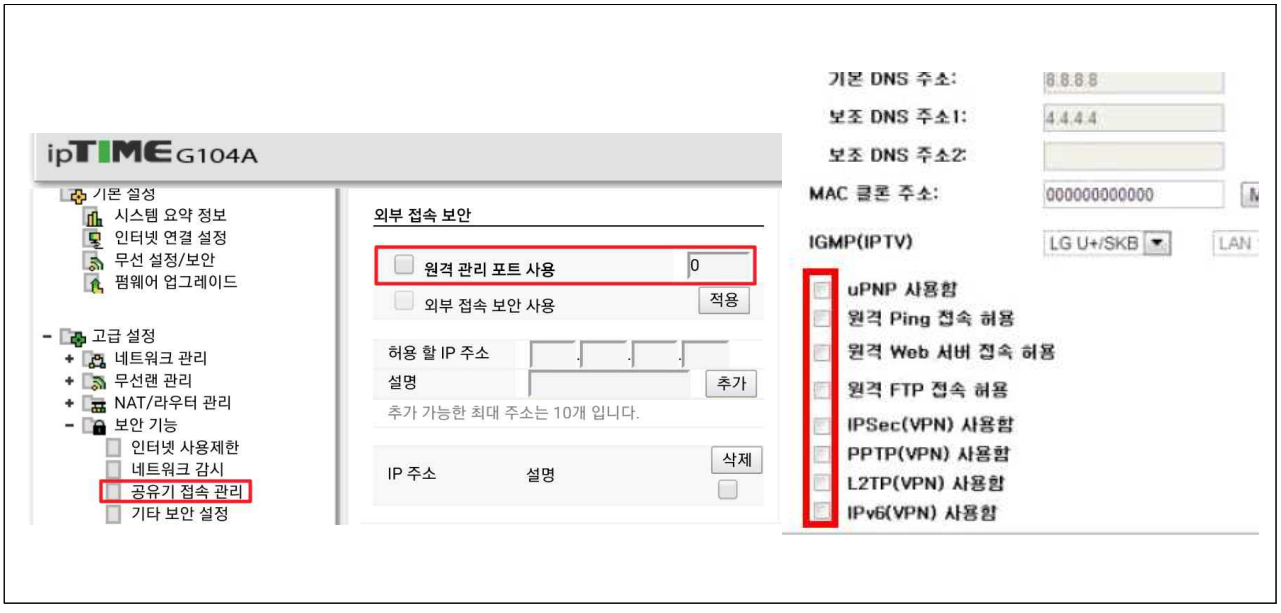
(6) 주기적인 무선공유기 펌웨어 업그레이드

- 지속적으로 발생하는 해킹에 대응하기 위해서 무선공유기 펌웨어 업그레이드 필요
- 제조사 홈페이지에서 최신 펌웨어를 다운로드 후 무선공유기에 설치

[그림13] 무선공유기 펌웨어 업그레이드 화면(ipTime)

(7) 외부접속 포트, Telnet, uPnP, 등의 불필요 서비스는 비활성화

- 외부 원격지에서 공유기 설정관리를 위한 원격접속 포트로 직접 불법 접근이 가능
- uPnP, Telnet, FTP 등 서비스 사용시 다수의 취약점으로 인한 공격이 발생 가능



[그림14] 무선공유기 불필요 서비스 설정 화면

Ⅲ. 제조사별 공유기 보안설정

1. ipTIME

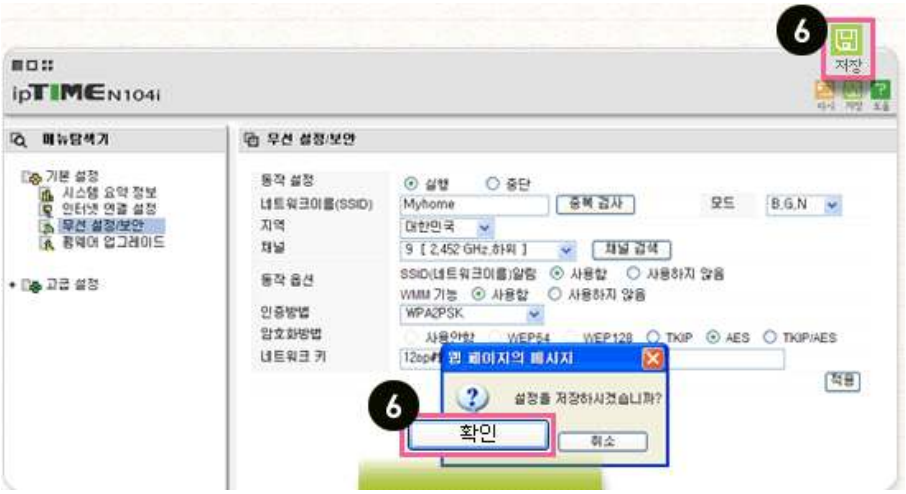
1) 보안설정 방법

(1) Internet Explorer를 실행한 후 주소창에 http://192.168.0.1를 입력한 후 다음과 같이 무선공유기 설정 초기화면에 접속합니다. 관리도구 아이콘을 클릭하여 설정을 진행합니다.

(2) 다음과 같이 무선공유기 설정 초기화면에 접속합니다. ① 관리도구 아이콘을 클릭하여 설정을 진행합니다.

(3) ②인증방법은 WPA2PSK를 선택합니다. (*WPA2PSK : 가장 안전한 보안을 제공)
③암호화방법은 AES를 선택합니다.
④네트워크 키를 입력합니다. (*영어, 숫자, 특수기호로 조합된 암호 8자리 이상)
⑤적용버튼을 클릭합니다.

(4) ⑥화면 우측 상단의 저장버튼 클릭 후 메시지 창의 확인버튼을 클릭합니다.



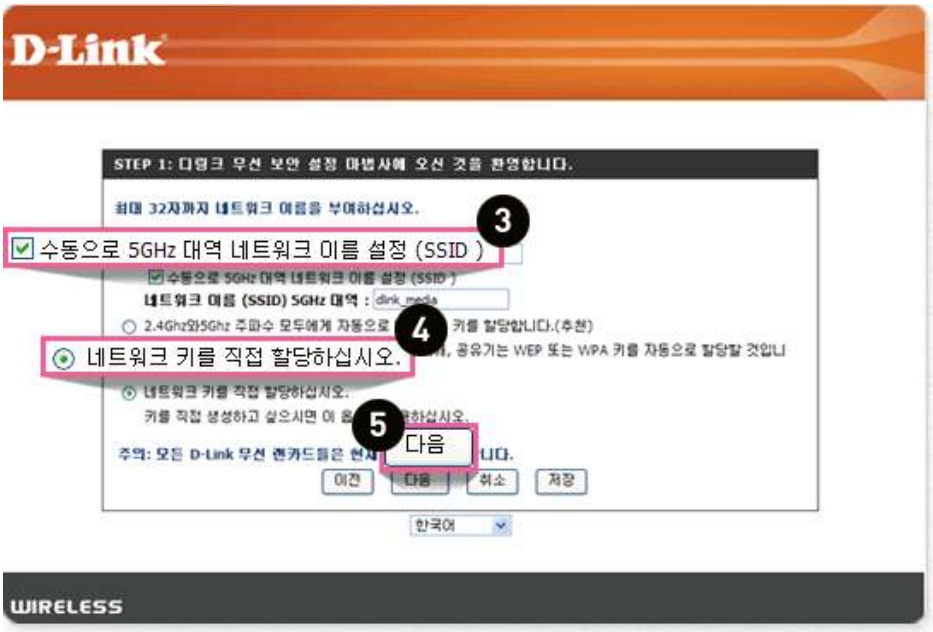
2. D-Link

1) 보안설정 방법

(1) Internet Explorer를 실행한 후 주소창에 http://192.168.0.1를 입력한 후 다음과 같이 무선공유기 설정 초기화면에 접속합니다.

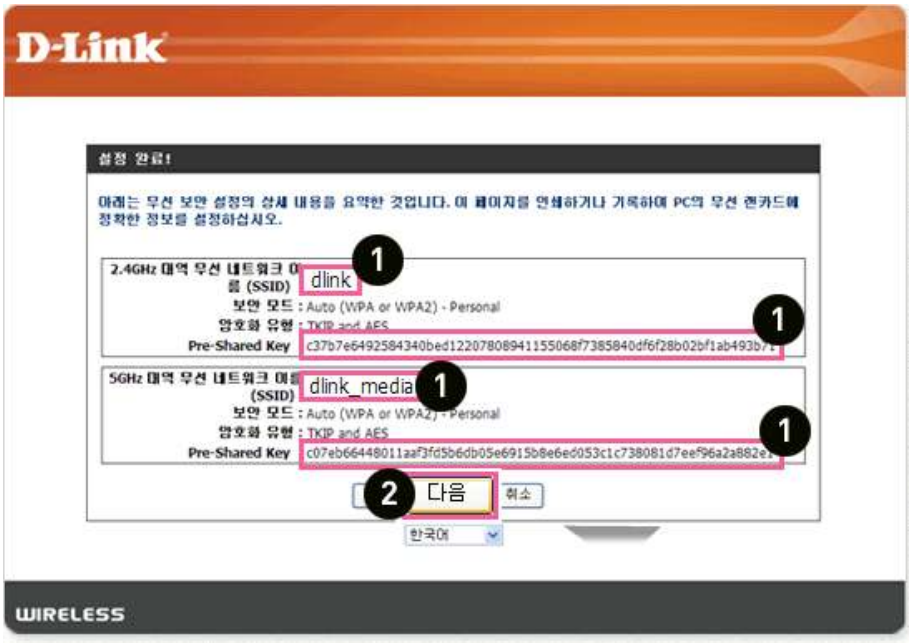
(2) 다음과 같이 무선 공유기에서 제공하는 보안기능을 설정합니다. ①좌측 메뉴부분의 무선설정 메뉴를 클릭합니다. ②무선 네트워크 설정 마법사 버튼을 클릭합니다.

(3) ③“수동으로 5GHz 대역 네트워크 이름 설정(SSID)“을 체크합니다.
④“네트워크 키를 직접 할당하십시오.“를 선택합니다.
⑤다음 버튼을 클릭합니다.
⑥비밀번호를 입력합니다. (*영어, 숫자, 특수기호로 조합된 암호 8자리 이상)
⑦다음 버튼을 클릭합니다.



(4) 설정이 완료되었으면 입력하신 정보를 확인합니다.
①입력하신 정보와 동일한 지 SSID와 Key를 확인합니다.

②다음 버튼을 클릭합니다.



3. ZIO

1) 보안설정 방법

(1) Internet Explorer를 실행한 후 주소창에 http://192.168.0.1를 입력한 후 다음과 같이 무선공유기 설정 초기화면에 접속합니다.

(2) 다음과 같이 무선 공유기에서 제공하는 보안기능을 설정합니다.

①좌측 메뉴부분의 무선설정 메뉴 클릭 후 상단의 암호화 탭을 클릭합니다.

②암호화 종류는 WPA2PSK를 선택합니다. (WPA2PSK : 가장 안전한 보안을 제공)

③WPA는 AES를 선택합니다.

④WPA 암호 KEY를 입력합니다. (*영어, 숫자, 특수기호로 조합된 암호 8자리 이상)

⑤적용버튼을 클릭합니다.

4. NetTop

1) 보안설정 방법

(1) Internet Explorer를 실행한 후 주소창에 http://192.168.0.1를 입력한 후 다음과 같이 무선공유기 설정 초기화면에 접속합니다.

(2) 다음과 같이 무선 공유기에서 제공하는 보안기능을 설정합니다.

①좌측 메뉴부분의 무선설정의 보안설정 메뉴를 클릭합니다.

②무선 보안 모드는 WPA2-PSK를 선택합니다. (WPA2PSK : 가장 안전한 보안을 제공)

③WPA는 AES를 선택합니다.

④암호 문자열에 암호를 입력합니다. (*영어, 숫자, 특수기호로 조합된 암호 8자리 이상)

⑤적용버튼을 클릭합니다.


NetTop
모두 보이기 | 모두 숨기기
메인(첫화면)
운영모드 설정
인터넷 설정
무선 설정
기본 설정
고급 설정
보안 설정
WPS 설정
무선사용자 목록
방화벽 설정
관리
무선 보안 / 암호 설정
비인가 접근 및 모니터링을 방지하기 위한 무선 보안과 암호를 설정해 주세요
무선 네트워크 이름(SSID) 선택
무선 네트워크 이름(SSID)
NETTOP_AP
"NETTOP_AP"
무선 보안 모드
3
AES
3
WPA 알고리즘
TKIP
AES
TKIP/AES
4
암호 문자열
4
QorTjf+7SksWkd
Key 갱신 간격
접근 정책
사용여부
사용안함
신규
5
적용
취소

[붙임#1]

□ 용어설명

구분	설명
중간자 공격 (MITM, MIMA)	Man In The Middle attack 또는 Man In the Middle Attack의 약어로 통신하고 있는 두 당사자 사이에 들키지 않게 끼어들어 당사자들이 교환하는 통신내용을 바꾸거나 도청하는 공격기법이다.
AES (Advanced Encryption Standard)	미국 국립 표준 기술연구소(NIST)가 데이터 암호화 표준(DES)의 차세대 국제 표준 암호로 대체하는 순서 공개형의 대칭 키 암호 방식이다. IEEE 802.11i에서 AES의 CCM 모드를 이용한 데이터 암호화 방식을 정의하고 있으며, 이는 하드웨어 암호기법을 사용하여 TKIP보다 안전하다.
EAP (Extensible Authentication Protocol)	IEEE 802.1x에서 사용자 인증을 위해 사용하는 프로토콜이다. EAP 자체는 실제 인증 프로토콜이 아니지만 확장성을 지원하여 내부적으로 MD5, 1회용 패스워드(One-Time Password), 스마트 카드, 전송 계층 보안(EAP-TLS), 터널 방식으로 개량된 TLS(EAP-TTLS)와 같은 인증 방식을 사용할 수 있게 되어 있다. 기업용 또는 공중 무선랜 환경 등 에서 인증서버를 이용한 인증에 사용된다.
SSID (Service Set IDentifier)	무선랜을 통해 전송되는 패킷 헤더에 붙는 고유 식별자로, 무선 장치들이 BSS(Basic Service Set)에 접속할 때 사용하는 텍스트 데이터로 무선랜 이름에 해당한다. SSID는 하나의 무선랜을 다른 무선랜으로부터 구분해주므로, 특정 무선랜에 접속하려는 모든 AP 나 무선 장치들은 반드시 일정한 SSID를 사용해야만 하며 SSID가 변경되면 해당 BSS에 접속할 수 없다.
TKIP (Temporal Key Integrity Protocol)	WEP 알고리즘의 취약성을 보완하기 위해 연구된 기술이다. 패킷당 키 할당, 키값 재설정 등 기존 WEP 방식에 소프트웨어 패치만으로 안전성을 개선한 보안 기술이다.
UTP (Unshielded Twisted Pair wire, 비차폐 연선)	차폐 연선과는 달리 외부의 전계, 자계 또는 다른 전송선에서 유도되는 전계, 자계로부터의 영향을 차단하기 위해 도전성 물질이 많은 피복(sheath)을 둘러싸지 않은 연선. 보통 의 구내 전화선이나 구내 정보 통신망(LAN)의 전송 매체로 사용된다. 전송 가능 대역에 따라 카테고리 1~5의 5종류로 분류되는데, LAN에서 널리 사용되는 것은 카테고리 3, 4, 5이다. 카테고리 3은 10Mbps, 카테고리 4는 16Mbps, 카테고리5는 100Mbps의 전송 속도를 보증한다. 비차폐 연선을 카테고리에 따라 흔히 UTP 3, UTP 4, UTP 5 등으로 부른다.
VLAN (Virtual LAN)	가상의 기능을 가진 근거리통신망(LAN) 스위치 혹은 비동기전송 방식의 스위치를 사용해서 물리적인 배선에 구애받지 않고 동보 패킷이 전달되는 범위를 임의로 나눈 가상의 근 거리 통신망이다.
WEP (Wired Equivalent Privacy)	초기 무선랜 보안설정 방법으로 유선랜과 동등한 수준의 보안성 제공의 목적으로 만들어진 보안 기술이다. 대칭키 기반 암호화 기법으로, 현재는 암호 알고리즘 자체의 취약성이 많이 알려져 있어 사용이 권고되지 않는다.
WPA (Wi-Fi Protected Access)	WEP의 취약성에 대한 대안으로 발표한 무선랜 보안 기술 규격으로 IEEE802.11i 표준이 완성되기 전에 단기간 보안 해결책으로 Wi-Fi alliance에서 제시한 표준이다. TKIP을 통한 암호화 향상, EAP를 통한 사용자 인증 등이 포함된다.
WPA2(Wi-Fi Protected Access 2	IEEE802.11i 규격의 완성에 따라, IEEE802.11i 규격을 완전히 수용하는 표준으로서 WPA와 구분하기 위해 WPA2로 불린다. AES-CCMP를 통한 암호화 기능 향상, EAP 사용자 인증 강화 등이 포함된다.