

알기쉬운 무선랜 보안 안내서

제 · 개정 이력

순번	제 · 개정일	변경내용	발간팀	연락처
1	2010. 10.	제정	무선인터넷팀	국번없이 118
2				
3				
4				

CONTENTS



1. 무선랜 사용하기	04
2. 무선랜 보안이 중요해요	06
3. 무선랜 안전 이용 수칙	08
4. 무선랜 안전 이용 수칙 따라하기	09
[부록] 1. 무선랜 관련 사업자 · 제조사 문의처	22
2. 무선랜 기술 표준	24
3. 스마트폰 안전하게 사용하기	26

1 무선랜 사용하기



무선랜이란?

선 연결없이 인터넷을 이용할 수 있게 해주는 무선인터넷 이용환경을 의미하며, 흔히 와이파이(Wi-Fi)라고도 합니다.

※ 무선인터넷 기술은 와이브로, 3G 휴대폰(HSDPA 등), WLAN(Wireless LAN) 등이 있으며, 무선랜은 WLAN 기술을 이용한 서비스를 지칭합니다.



와이파이(Wi-Fi) : 국제 비영리단체인 WiFi Alliance에서 무선랜 표준인 802.11x 규약을 준수하여 무선랜 관련 장치와 연동됨을 보증함을 의미하는 인증마크를 의미합니다.

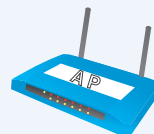


무선랜을 만들거나 사용하려면 무엇이 필요한가요?

무선랜을 사용하기 위해서는 기본적으로 무선 AP와 무선 단말기(노트북, 스마트폰 등)가 필요합니다.



무선 AP(Access Point) : 무선공유기라고도 불리는 무선 AP는 인터넷 회선(유선랜, 와이브로 등)과 연결하여 무선랜 환경을 만들어주는 장치입니다.



●●● [무선공유기를 이용한 무선랜 환경의 예]





무선랜은 어디에 있나요?

우리 주변에서는 다음과 같은 무선랜 환경을 흔히 볼 수 있습니다.



개인이 구매·설치하여 이용하는 무선랜



인터넷 전화 설치시 제공되는 무선랜



공공시설에서 고객편의 제공을 위해 운영하는 무선랜



통신 사업자가 서비스 제공을 위해 구축한 무선랜

! 위와 같이 일반 이용자를 대상으로 하는 무선랜 환경 외에도 기업 등에서 내부 업무용으로 사용하기 위해 구축하는 무선랜도 있습니다.

2 무선랜 보안이 중요해요

 무선랜은 선 연결 없이 자유롭게 접속할 수 있으므로 악의적인 목적을 가진 사용자가 접속하여 개인정보 유출 등 다양한 보안 위협을 발생시킬 수 있습니다.

 **무선랜 이용자의 중요한 정보가 유출될 수 있습니다.**

- 보안이 설정되지 않은 무선랜으로 인터넷을 이용할 경우 악의적인 목적의 사용자가 접속하여 비밀번호 등 개인의 중요한 정보를 유출할 수 있습니다.

●●● [무선랜을 통한 개인정보 유출]



 **인터넷전화도 도청될 수 있습니다.**

- 보안이 설정되어 있지 않거나 취약한 무선 AP에 접속하여 인터넷전화를 이용할 경우 통화내용이 도청될 수 있습니다.

●●● [무선랜을 통한 도청]

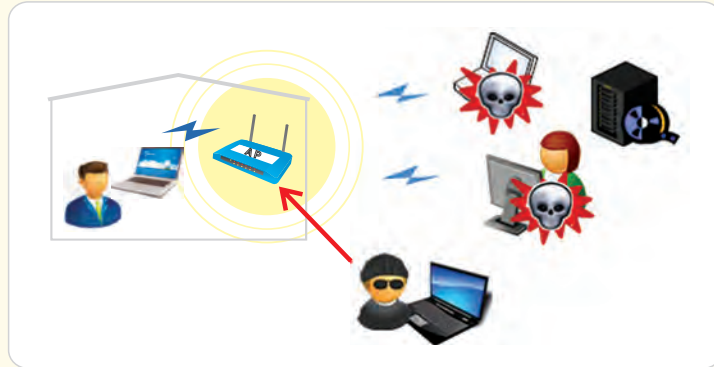




자신의 무선 AP가 악의적으로 이용될 수 있습니다.

- 보안설정이 되어 있지 않거나 미흡한 경우 자신의 무선 AP가 해킹, 불법 다운로드 등에 악용될 수 있습니다.
- 또한, 바이러스, 악성코드 등을 유포하는 경유지로 활용될 수 있습니다.

●●● [무선랜을 통한 불법다운로드, 악성코드 유포]



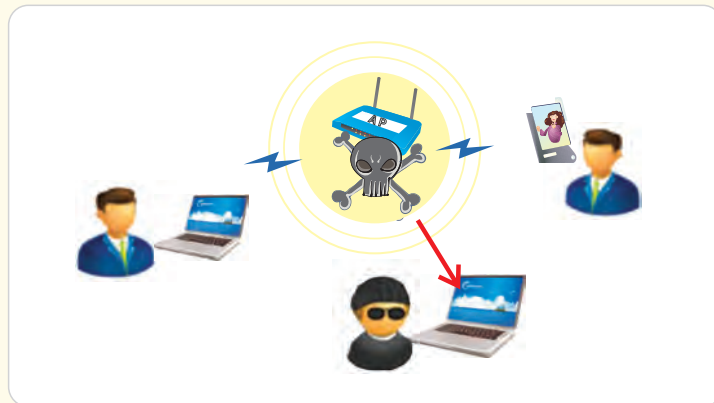
악의적인 목적으로 설치된 무선랜에 접속되어 개인정보가 유출될 수 있습니다.

- 해커가 개인정보 탈취등을 목적으로 구축한 무선랜에 접속할 경우 사용자의 개인정보가 유출될 수 있습니다.



Evil Twin : 이용자의 개인 정보를 수집하기 위해 정상 무선랜으로 위장 설치된 무선 AP

●●● [불법 무선랜 이용에 따른 개인정보 유출]



3 무선랜 안전 이용 수칙



무선랜 안전 이용 수칙을 준수하여 안전하게 무선랜을 이용할 수 있습니다.



- 1 무선공유기 사용시 보안기능 설정하기
- 2 무선공유기 패스워드 안전하게 관리하기
- 3 사용하지 않는 무선공유기는 꺼놓기
- 4 제공자가 불분명한 무선랜 이용하지 않기
- 5 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기
- 6 무선랜에 자동 접속 기능 사용하지 않기
- 7 무선공유기의 SSID를 변경하고 숨김 기능 설정하기



4 무선랜 안전 이용 수칙 따라하기



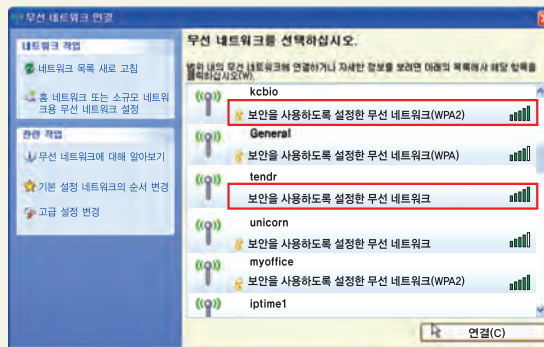
무선랜 안전 이용 수칙은 어떻게 사용할까요? 아래의 방법대로 따라하면 손쉽고도 안전하게 무선랜을 이용할 수 있습니다.

수칙 ① 무선공유기 사용시 보안기능 설정하기

무선공유기 사용 시 암호화/인증 등 보안기능을 설정하지 않으면 외부인이 무단으로 본인의 무선랜을 사용할 수 있으며, 이러한 경우 인터넷 속도가 느려지거나 개인정보 유출 등 해킹사고가 발생할 수 있습니다. 또한, 기업 내에서 보안기능 없는 무선랜을 사용하는 경우 사내 네트워크에 접근경로를 제공하여 해킹 등에 악용될 수 있습니다.

노트북에서 무선랜 보안설정 확인하는 방법

●●● [windows XP]



●●● [window 7]

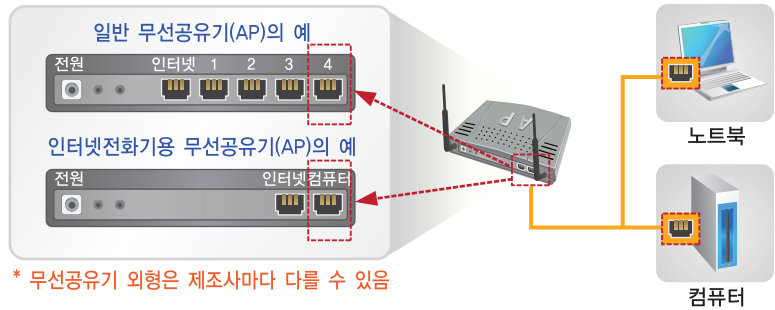


무선공유기 사용 시
암호화/인증 등 보안기능을
설정하지 않으면
해킹 대상이 됩니다.



① 노트북에서 무선랜 보안설정 확인하는 방법

① 무선공유기와 컴퓨터 또는 노트북을 연결합니다.



② 무선공유기 관리화면으로 접속합니다.

1 바탕화면의 웹 브라우저(ex.인터넷 익스플로러 실행)



2 http://192.168.?? 입력 (설정화면 IP주소)

※ 설정화면IP주소는 제품마다 다를 수 있습니다. 상세내용은 제품 메뉴얼을 참고하세요.

디링크	192.168.0.1
링크시스	192.168.1.1
아이피타임	192.168.0.1
유니콘정보시스템	192.168.123.254
애니게이트	192.168.10.1
한국쓰리콤	192.168.1.1

3 무선공유기 설정 초기화면 접속

기본정보	
인터넷 정보	
인터넷 연결상태	정상적으로 연결됨
인터넷 연결방식	고정 IP 연결
네트워크 정보	
내부 IP 주소	192.168.0.2 ~ 192.168.0.254
DHCP	DHCP 동작 중
무선 서비스 정보	
SSID	HomeAP
보안설정	암호화 미사용



③ 무선공유기 관리화면에서 보안기능을 설정 합니다.

1 무선보안설정

기본 설정
▶ 상태 보기
▶ 자동 설정
▶ 수동 설정

고급 설정
▶ ID 선택
▶ 무선보안설정
▶ 무선 고급 설정
▶ WPS
▶ 트래픽 제어
▶ 보안 설정
▶ 부가 기능
▶ 관리자
▶ 상태 정보

2 암호를 통한 보안 설정을 선택

보안 설정 ☒ 암호를 통한 보안설정

3 암호는 WPA2를 선택

암호 설정 ☐ WEP ☐ WPA ☒ WPA2

※ 제품에 따라
WPA는 WPAPSK,
WPA2는 WPAPSK2로
표기될 수 있습니다.

보안설정	암호알고리즘	보안강도
WEP	RC4	낮음
WPA	RC4(TKIP)	보통
WPA2	AES	높음

4 암호알고리즘은 AES를 선택한 후 비밀번호를 입력

Algorithms ☐ TKIP ☒ AES

공유키(비밀번호)

확인 취소

👉 무선 AP에서 제공하는 인증/암호 기술은 보안 강도에 따라 WEP, WPA, WPA2가 있으며, 안전한 이용을 위해 WPA2 설정을 권고합니다.



알기쉬운

무선랜 보안

안내서 <<>>

수칙 ② 무선공유기 비밀번호 안전하게 관리하기

무선공유기에 설치된 초기 비밀번호는 공개되어 있어 타인이 쉽게 접속할 수 있으므로 반드시 변경 후 사용해야 합니다. 또한, 설정한 비밀번호는 주기적으로 변경하고 추측하기 쉽거나 7자리 이하의 짧은 비밀번호는 사용하지 않아야 합니다.

● 안전한 비밀번호 관리 방법

- ▶ 무선AP의 비밀번호는 안전한 비밀번호 생성방법에 따라 생성합니다.
- ▶ 초기 설정된 무선 AP의 비밀번호는 빠른 시간 내에 새로운 비밀번호로 변경합니다.
- ▶ 무선 AP의 비밀번호는 주기적으로 변경합니다.
- ▶ 비밀번호 변경은 이전에 사용하지 않은 새로운 문자열로 변경합니다.
- ▶ 무선랜의 비밀번호가 제3자에게 노출되지 않도록 합니다.
- ▶ 제 3자에게 비밀번호를 유추할수 있는 정보, 힌트를 제공하지 않습니다.
- ▶ 제 3자에게 비밀번호가 노출된 경우, 즉시 새로운 비밀번호로 변경합니다.

※ 안전한 비밀번호 생성방법은 “비밀번호 선택 및 이용 안내서”를 참조하세요
(<http://www.118.or.kr> 의 자료실 참조)





수칙 ③ 사용하지 않는 무선공유기는 꺼놓기

사용하지 않는 무선공유기를 켜 놓을 경우 외부인이 불법다운로드, 해킹등에 악용할 수 있고 전력이 낭비될 수 있으므로, 사용하지 않는 무선공유기는 꺼놓아야 합니다.

● 무선공유기의 전원을 끄는 방법

●●● [무선공유기 전원을 끄거나 케이블을 분리합니다.]

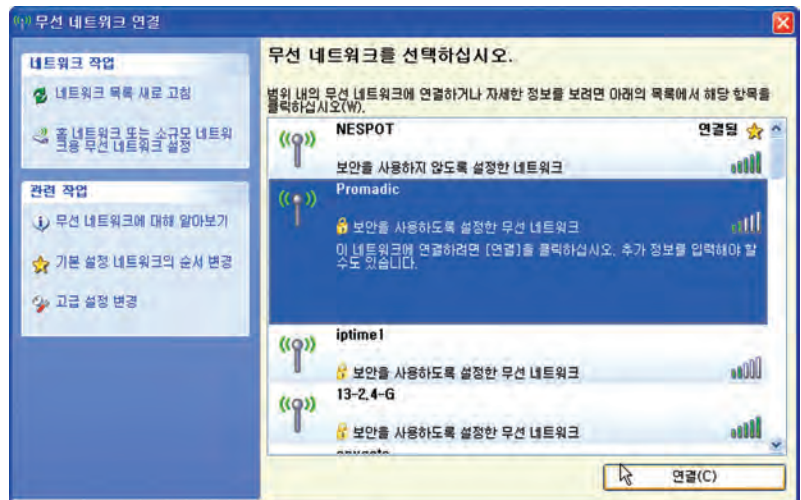


알기쉬운 무선랜 보안 안내서 <<>>

수칙 ④ 제공자가 불분명한 무선랜 이용하지 않기

개인정보 유출 등을 위해 악의적인 목적으로 설치한 무선공유기를 이용할 경우 개인정보가 쉽게 유출될 수 있습니다. 부득이 외부에서 무선랜 이용이 필요할 경우 본인이 잘 알고 있거나, 무선랜 이용 장소에서 제공자가 확인된 무선랜 만을 이용해야 합니다.

무선네트워크 연결 화면에서 무선랜 이름(SSID)으로 자신이 알고있는 무선랜인지 여부를 확인할 수 있습니다.



제공자가 분명한 무선랜의 예

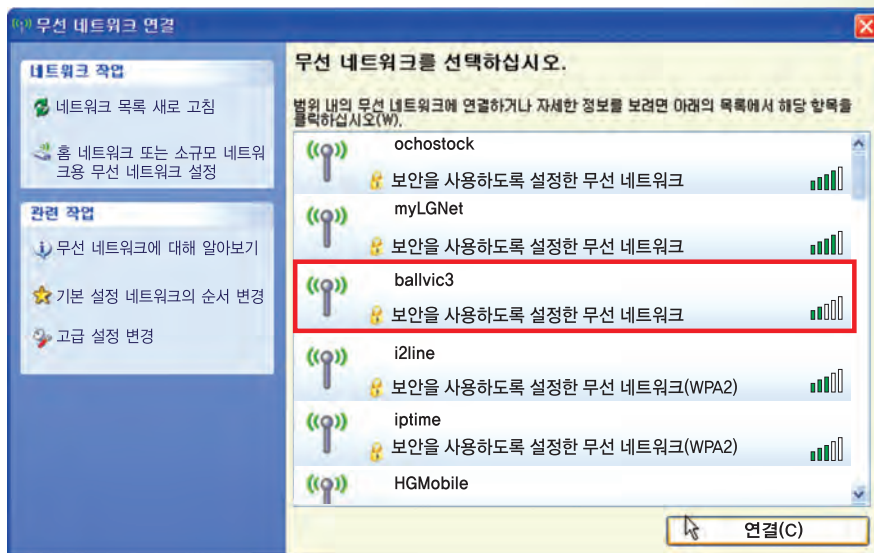
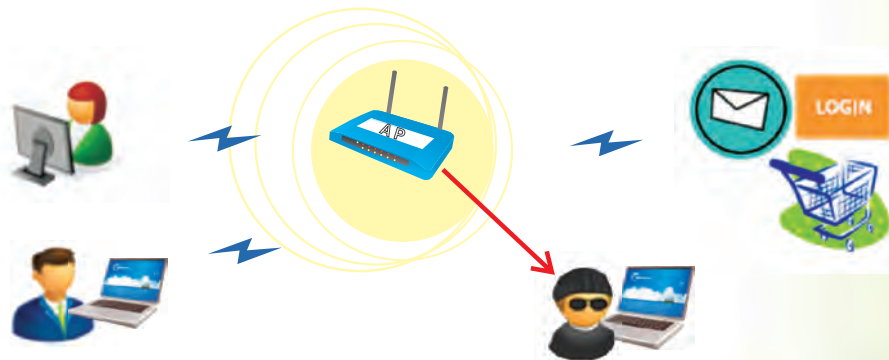
- ① 통신사, 지자체에서 제공하는 무료 와이파이존
예) KT의 QOOKnSHOW, ollehWiFi, SKT의 SKT-Tspot, LGU+의 U+ Wi-Fi100 등
- ② 커피숍 호텔 등에서 제공하는 무선랜
예) 커피숍, 호텔 등에서 유료 또는 무료로 제공하는 무선랜
- ③ 자신의 집에 설치된 인터넷전화기용 무선랜
예) KT_WLAN, myLGnet-xxx, 등
- ④ 자신이 설치했거나 기업에 설치된 사설 무선랜



수칙 ⑤ 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기

보안설정이 없는 무선랜의 경우 이용자의 접속행위, 개인정보 등이 유출될 수 있습니다. 부득이 무선랜 이용이 필요할 경우 금융거래, 기업업무, 로그인에 필요한 서비스, 개인정보를 입력하는 서비스 등 민감한 서비스는 가급적 사용하지 않아야 합니다.

● 보안이 설정되지 않은 무선랜 이용에 따른 개인정보 유출 화면



알기쉬운

무선랜 보안

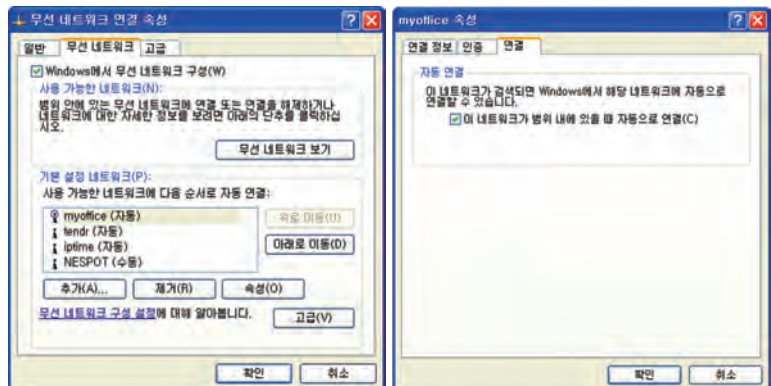
안내서 <<>>

수칙 ⑥ 무선랜에 자동 접속 기능 사용하지 않기

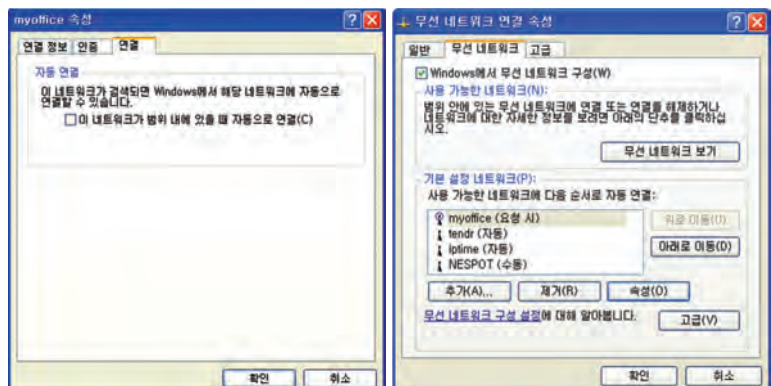
무선단말기에는 한번 접속한 무선랜에 자동으로 접속하는 기능이 있습니다. 무선랜 이름은 관리자가 임의로 변경가능하기 때문에, 해커가 잘 알려진 무선랜을 가장하여 자동접속 기능을 통해 이용자의 접속을 유도할 경우 개인정보 유출 등의 위험에 노출될 수 있습니다. 따라서, 무선랜의 자동접속기능은 끄고, 기존 접속한 무선랜 리스트는 주기적으로 지워야 합니다.

Windows XP에서 자동접속 해지 및 접속리스트 삭제

- ▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [무선 네트워크] → [속성] → [연결] → 자동연결 체크해제



- ▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [무선 네트워크] → 해당 무선랜 선택 → [제거]

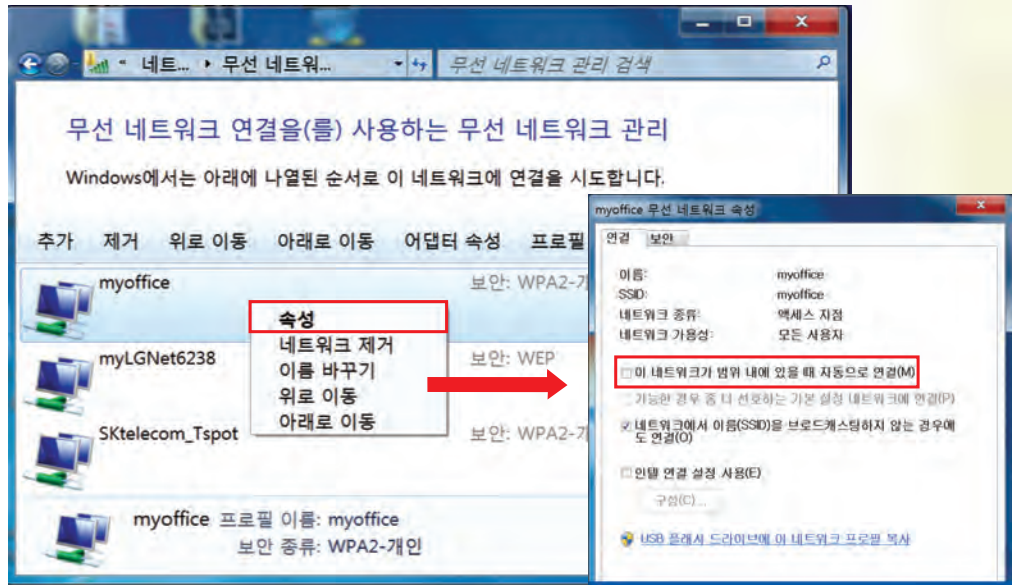




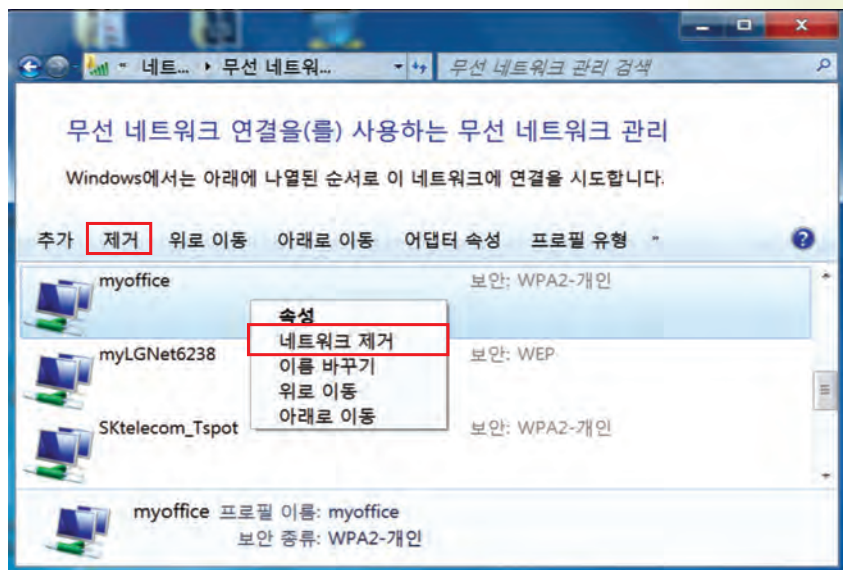
Windows 7에서 자동접속 해지 및 접속리스트 삭제



- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → 해당 무선랜 우클릭 → [속성] → 자동연결 체크 해제



- ▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → 해당 무선랜 선택 → 제거



알기쉬운

무선랜 보안

안내서 <<>>

수칙 ⑦ 무선공유기의 SSID를 변경하고 숨김 기능 설정하기

SSID(Service Set IDentification)란 무선랜을 구분하기 위한 이름입니다. SSID 숨김은 SSID 보안설정과 함께 사용 되어 보안성을 높이는 기능입니다. SSID를 숨김으로 할 경우 외부인은 해당 무선랜이 존재하는 지 알 수 없으므로 무선랜을 이용할 수 없어 해킹, 정보유출을 예방할 수 있습니다.

무선네트워크 이름(SSID) 변경 및 숨김 기능 설정 방법

① 무선공유기의 관리화면에 접속합니다.

※ 무선공유기 관리화면에 접속하는 방법은 “수칙①, 무선공유기 사용시 보안기능 설정하기” 를 참조하세요

② 무선 네트워크 설정 화면에서 SSID를 변경하고, 숨김기능을 체크 합니다.

●●● [무선 네트워크 SSID 이름변경 및 숨김기능 설정화면]



무선 네트워크 설정

기본설정

- ▶ 상태 보기
- ▶ 자동 설정
- ▶ 수동 설정

무선 대역 2.4GHz 대역

무선 활성화 ☒ Always **신규 추가**

무선 네트워크 이름 : HongGilDong_WLAN (SSID로 불림)

802.11 Mode Mixed 802.11n, 802.11g and 802.11b

자동 채널 스캔 설정 ☒

무선 채널 2,437 GHz - CH 6

채널 간격 20 MHz

무선 네트워크 이름 숨김 : ☐ 사용안함 ☒ 사용

확인 **취소**



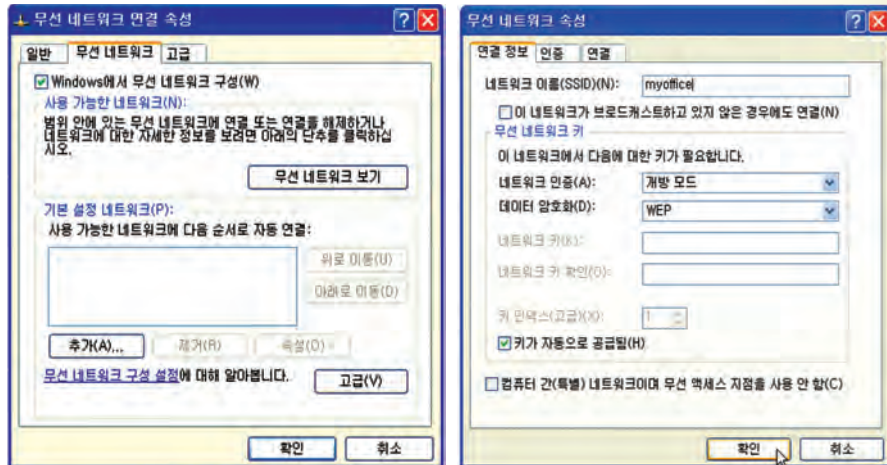
SSID가 숨김으로 설정된 경우 접속 방법

- ▶ SSID가 숨겨져 있는 경우, 직접 SSID를 입력해야 합니다.

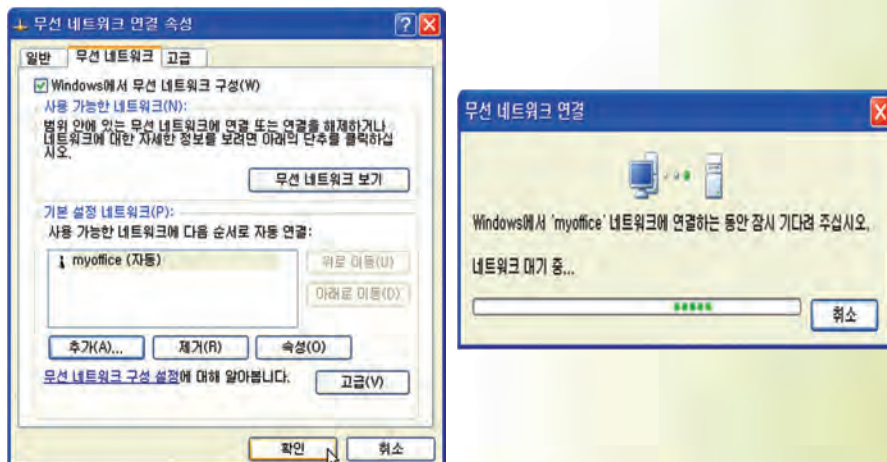
① Windows XP

- ▶ [시작] → [설정] → [네트워크 연결] → [무선네트워크 연결] → [고급 설정 변경] → [무선네트워크 탭] → [추가]
- ▶ [네트워크 이름(SSID)] 입력 및 [이 네트워크가 브로드캐스트 하고 있지 않은 경우에도 연결] 클릭, 인증/암호화, 암호키 입력

●●● [숨김 설정된 무선랜에 접속하기 위한 화면]



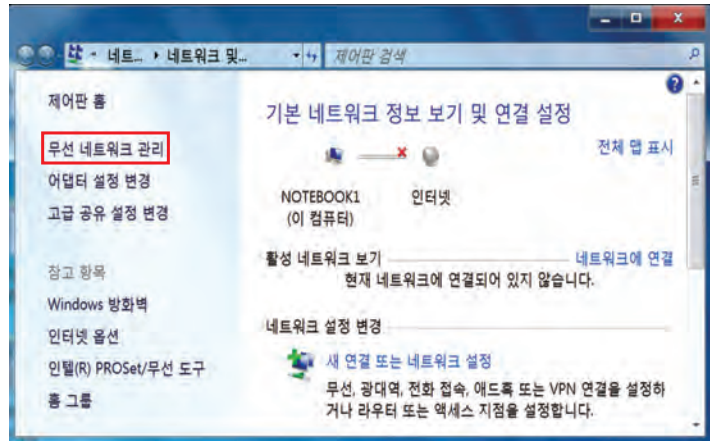
●●● [무선 네트워크 추가 화면, 접속되는 화면]



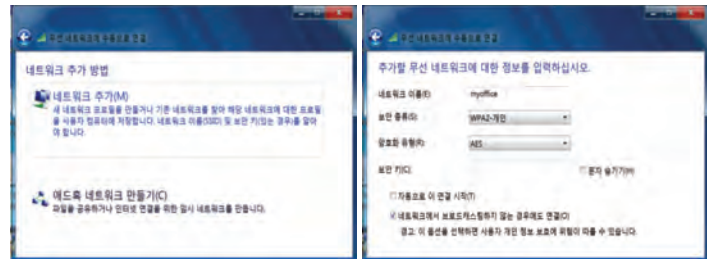
알기쉬운
무선랜 보안
안내서 <<>>

② Windows 7

▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] → [무선 네트워크 관리] → [추가]



▶ [시작] → [제어판] → [네트워크 및 인터넷] → [네트워크 및 공유센터] →





③ 스마트폰

- [숨김 설정된 무선랜에 접속하기 위한 화면]



- [아이폰에서 수동으로 무선랜 설정하는 화면]



[부록 1] 무선랜 관련 사업자 · 제조사 문의처



무선랜 관련 서비스를 제공하는 통신사업자

사업자	홈페이지	연락처	주요서비스
KT	http://www.kt.com	100	Qook-허브, Qook-인터넷전화, 네스팟, QOOKnSHOW, KT-에그 등
SKB	http://www.skbbroadband.com	106	anyway, SK_WLAN 등
SKT	http://www.sktelecom.com	02-1599-0011	T 와이파이존 등
LGU+	http://www.lguplus.com	02-1544-0010	LG U+ ACN, LG U+ 070 등

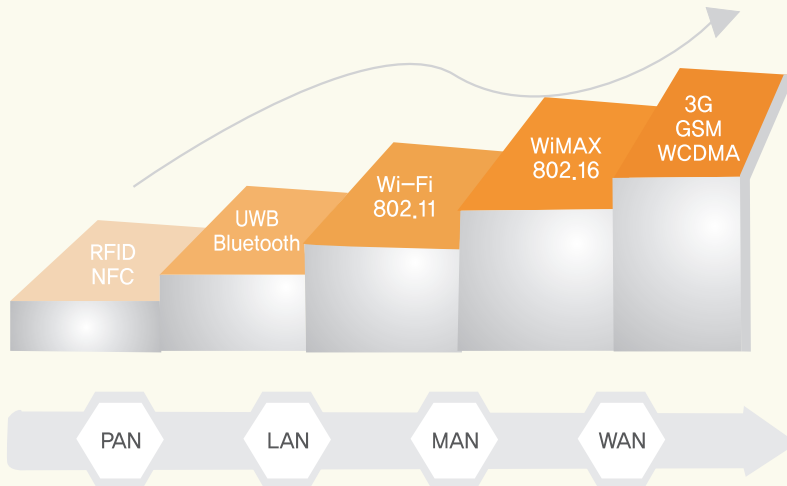
무선공유기를 제조하는 제조사



	제조사	홈페이지	연락처	주요모델
국내	Airband	http://www.airband.co.kr	070-7759-8555	AWR-11N, AWR-MIMO, AWR-54G
	AnyGate	http://www.anygate.co.kr	02-566-3879	RG-5300A, RG-5500A, RG-5300N, RG-5500N, XM-3100N, XM-3300N, 등
	엑슬러	http://www.axler.co.kr	02-703-1303	LGI-IP10000N, LGI-IP10000N PLUS, LGI-IP9500S, LGI-IP6000T, 등
	CREWAVE	http://www.crewave.com	031-420-0990~2	CW-1100AP 등
	Danbi	http://www.dan-bi.com	1588-6076	Danbi
	FREEO	http://www.freeo.co.kr	1577-7107	FN151, FN301, FL15U, FR101
	iptime	http://iptime.co.kr	1544-8695	N1, N608, N6004, N104M, N604M, N6004M, G104i 등
	MODAFUN	http://www.modafun.com	0505-656-1380	PWR MD-760NI
	NEPLE	http://www.neple.co.kr	1544-9586	G101, G101Y, N101, N202
	NetTop	http://www.nettop.co.kr	1577-2940	NTP-N4, NTP-N6, NTP-NP 150, NTP-NV120, NTP-NV150
	NEXT	http://www.ez-net.co.kr	02-715-0372	NEXT-N1104, NEXT-640MIMO, NEXT-1004N 11N, NEXT-WR54G 등
	UNICORN	http://www.eunicorn.co.kr	1588-2713	AP-150R, DW-2200N, WB-1100NR, WB-3300NR, MW-9000N 등
	Windy31	http://www.windy31.co.kr	070-7018-0024	windy31
국외	ZIO	http://www.izio.co.kr	1588-1696	ZIO-1500N, FX11s, V11, Q11, Z11 등
	3COM	http://www.hp.com	080-698-0880	A7700, A8700, A9100, A9500 등
	ASUS	http://support.asus.com	02-718-0164	RT-N11
	BELKIN	http://www.belkin.com/kr	00798-8521-9469	N+_F5D8232-4, N+_F5D8235-4
	BUFFALO	http://www.buffalotech.co.kr	02-2057-2094~5	WCR-GN, WHR-G300N, WHR-G300N V2 등
	D-Link	http://www.d-link.co.kr	02-890-3540~4	DWL-3200AP, DWL-8200AP, DWL-8500AP, DWL-8600AP 등
	imation	http://www.imation.co.kr/imation.php	1544-9152	R104G, R104N
	levelone	http://global.level1.com	080-087-0001	WAP-3010, WAP-3100
	CISCO	http://cisco.com/kr	080-808-8082	WRT110, WRT120N, WRT160N, WRT160NL, WRT320N, WRT610N 등
	NETGEAR	http://www.netgear.co.kr	080-638-4327	WG 602

[부 록]

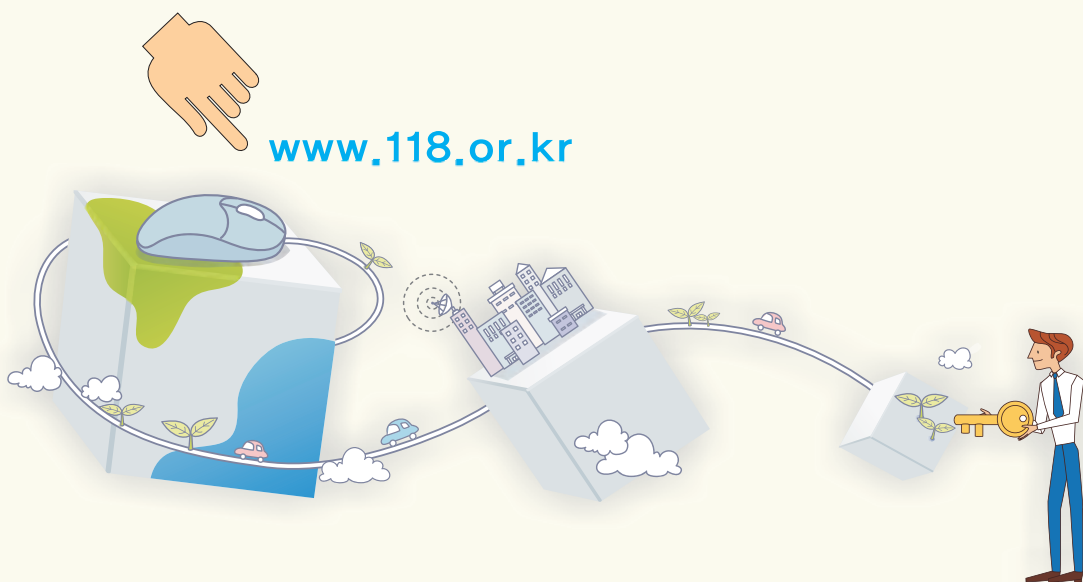
[부록 2] 무선랜 기술 표준



- PAN : Personal-area networks
- LAN : Local-area networks
- MAN : Metropolitan-area networks
- WAN : Wide-area networks

무선랜 기술 표준

무선랜 표준	표준 제정시기	주파수대역	데이터속도(최대)	서비스 범위(실내)
802.11	1997	2.4GHz	2 Mbps	20M
802.11a	1999	5GHz	54 Mbps	35M
802.11b	1999	2.4GHz	11 Mbps	38M
802.11g	2003	2.4GHz	54 Mbps	38M
802.11n	2009	2.4 / 5GHz	600 Mbps	70M

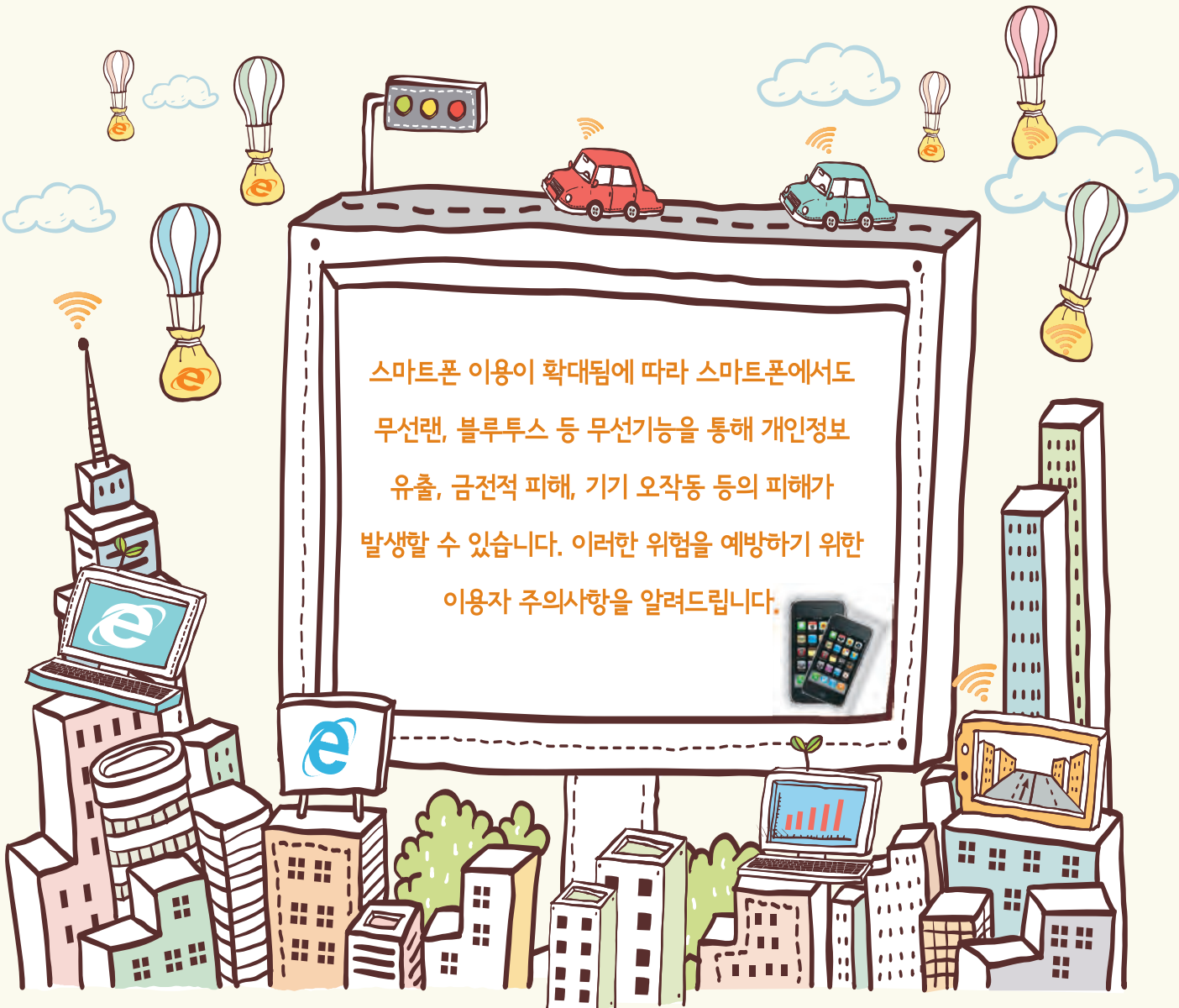


무선랜 보안기술 표준

설정 방식	보안기술	인증	암호화
개인 모드 (Personal-mode)	WEP	PSK	RC4 (64bit/128bit)
	WPA	PSK	RC4-TKIP
	WPA2	PSK	AES-CCMP
엔터프라이즈 모드 (Enterprise-mode)	WPA	IEEE 802.1X/EAP	RC4-TKIP
	WPA2	IEEE 802.1X/EAP	AES-CCMP

[부 록]

[부록 3] 스마트폰 안전하게 이용하기



※ 안전한 스마트폰 이용에 대한 세부 내용은 “**스마트폰 안전이용 수칙**”을 참조하세요
(<http://www.118.or.kr> 의 자료실 참조)



의심스러운 애플리케이션은 다운로드하지 않습니다.

신뢰할 수 없는 사이트는 방문하지 않습니다.

발신인이 불명확하거나 의심스러운 메시지 및 메일은 삭제합니다.

비밀번호 설정 기능을 이용하고 정기적으로 비밀번호를 변경합니다.

블루투스 기능 등 무선인터페이스는 사용 시에만 켜놓습니다.

이상증상이 지속될 경우 악성코드 감염여부를 확인합니다.

다운로드한 파일은 바이러스 유무를 검사한 후 사용합니다.

PC에도 백신 프로그램을 설치하고 정기적으로 바이러스를 검사합니다.

스마트폰 플랫폼의 구조를 임의로 변경하지 않습니다.

운영체제 및 백신 프로그램을 항상 최신 버전으로 업데이트 합니다.

한국인터넷진흥원(KISA) 안내서 · 해설서 시리즈

분류	안내서 · 해설서	해당팀명	발간년월	대상	수준
인터넷 진흥	DNS 설정 안내서	시스템관리팀	'09.	IT시스템관리자	중급
	인터넷주소분쟁해결 안내서	도메인팀	연간지	일반	초급
	모바일 RFID코드 및 OID기반 RFID코드 적용 안내서	무선인터넷팀	'09.8	IT기업개발자	중급
	13.56MHz대역의 OID적용을 위한 미들웨어 개발 안내서	무선인터넷팀	'09.12	IT기업개발자	중급
	공공기관 IPv6 적용 안내서	IP팀	'08.12	IT시스템관리자	중급
인터넷이용 활성화	본인확인제 안내서	인터넷윤리팀	'09.2	일반,업무관계자	중급
	본인확인제 만화 안내서	인터넷윤리팀	'09.	일반	초급
정보보호 시스템 관리	BcN 정보보호 안내서	인터넷서비스보호팀	'07./'10.1	IT시스템관리자	중급
	침해사고 분석절차 안내서	해킹대응팀	'10.1	IT시스템관리자	고급
	웹서버구축 보안점검 안내서	웹보안지원팀	'10.1	IT시스템관리자	고급
	웹어플리케이션 보안 안내서				
	홈페이지 개발보안 안내서				
	무선랜 보안 안내서	해킹대응팀	'10.1	일반	중급
	침해사고대응팀(CERT) 구축/운영 안내서	침해사고대응기획팀	'07.9	업무관계자	중급
	WebKnight를 활용한 IIS 웹서버 보안 강화 안내서	웹보안지원팀	'09.6	IT시스템관리자	중급
	WebKnight 로그 분석 안내서				
	ModSecurity를 활용한 아파치 웹서버 보안 강화 안내서				
정보보호인증	보안서버구축 안내서	개인정보보호기술팀	'08.7	IT시스템관리자	중급
	IT보안성 평가 · 인증 안내서	공공서비스보호팀	'09.12	일반, 업무관계자	초급
기업 정보보호	정보보호 안전진단 해설서	기업보안관리팀	'08.4/'10.1	업무관계자	초급
	정보보호 안전진단 업무 안내서	기업보안관리팀	'10.1	업무관계자	초급
	정보보호관리체계 안내서	기업보안관리팀	'09.12	일반	초급
신규 서비스 정보보호	패스워드 선택 및 이용 안내서	융합보호R&D팀	'10.1	일반	초급
	암호이용 안내서	융합보호R&D팀	'07./'10.1	일반	중급
	IPv6운영보안 안내서	융합보호R&D팀	'06.12	IT시스템관리자	중급
	IPv6보안기술 안내서	융합보호R&D팀	'05.	일반	초급
	와이브로 보안기술 안내서	융합보호R&D팀	'06.8	IT시스템관리자	중급
	암호 알고리즘 및 키 길이 이용 안내서	융합보호R&D팀	'07	IT시스템관리자	중급
	(기업 및 기관의 IT 정보자산 보호를 위한) 암호정책 수립 기준 안내서	융합보호R&D팀	'07	IT기업개발자	중급
	(정보의 안전한 저장과 관리를 위한) 보조기억매체 이용 안내서	융합보호R&D팀	'09	일반	초급
	웹사이트 회원탈퇴 기능 구현 안내서	융합보호R&D팀	'06	IT시스템관리자	중급
	개인정보	개인정보의 기술적 · 관리적 보호조치 기준 해설서	개인정보보호기획팀	'09.9	업무관계자
위치정보의 보호 및 이용 등에 관한 법률 해설서		개인정보보호기획팀	'08.12	업무관계자	중급
위치정보보호를 위한 관리적 · 기술적 보호조치 권고 해설서		개인정보보호기획팀	'08./'10.1	업무관계자	중급
웹사이트 개발 · 운영을 위한 개인정보 안내서		개인정보보호기술팀	'09.11	IT기업 개발자, 관리자	중급
I-PIN 2.0 도입 안내서		개인정보보호기술팀	'09.7	업무관계자	중급
김대리, 개인정보보호 달인되기		이용자권익보호팀	'09.8	업무관계자	중급
기업의 개인정보영향평가 수행을 위한 안내서		이용자권익보호팀	'09.1	업무관계자	중급
스팸	사법자를 위한 불법스팸 방지 안내서	스팸대응팀	'08.9	일반, 업무관계자	초급
인력양성	지식정보보안 신규일자리 창출사업 세부시행 안내서	KISA아카데미팀	'09.	업무관계자	초급

■ 본 안내서 · 해설서는 [한국인터넷진흥원 홈페이지\(www.kisa.or.kr\)](http://www.kisa.or.kr) 자료실에서 내려 받으실 수 있습니다.

알기쉬운 무선랜 보안 안내서

2010년 10월 인쇄

2010년 10월 발행

발행처: 방송통신위원회 · 한국인터넷진흥원

서울특별시 종로구 세종로 100번지
방송통신위원회
Tel: (02) 750-1114

서울특별시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-4118

인쇄처: 한울

Tel: (02) 2279-8494

(비매품)

■ 본 안내서 내용의 무단 전재를 금하며, 가공·인용할 때에는 반드시 방송통신위원회 · 한국인터넷진흥원 「알기쉬운 무선랜 보안 안내서」라고 출처를 밝혀야 합니다.



방송통신위원회

110-777 서울특별시 종로구 세종로 100번지
Tel: (02) 750-1114
www.kcc.go.kr

한국인터넷진흥원

138-950 서울특별시 중대로 109(가락동 79-3) 대동빌딩
Tel: (02) 405-4118 Fax: 405-5119
www.kisa.or.kr