情 報 保 護 學 會 誌
第21卷 第1號, 2011. 2

국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향

백 종 현*, 박 순 태*

요 약

최근 폭발적인 스마트폰 이용 확산 및 다양한 태블릿 PC의 출시 등으로 언제 어디서나 저렴한 가격의 무선인터넷 이용 요구가 급증하고 있다. 그 중에서도 무선랜(WiFi)이 가격이나 속도 측면에서 이용자들의 요구를 충족시켜주고 있다. 무선랜 기술은 2000년대 초반부터 도입되기 시작하였으나 스마트폰이 출시된 2009년 말부터 본격적으로 보급이 확산되었다. 무선랜은 급격하게 증가하는 무선 데이터 트래픽에 대한 부하 분산 등을 위해 이통사를 중심으로 경쟁적으로 설치되고 있으며, 수도권을 중심으로 와이파이 존이 확산되고 있으며 점차적으로 전국으로 확대되고 있다. 이러한 무선랜 보급 확산에 따라 이에 대한 역기능 문제도 대두되고 있다. 구글의 스트리트뷰 서비스 관련한 개인정보 유출 문제나 무선랜 해킹 등이 최근 이슈가 되기도 하였다. 이에 따라 이용의 편리성과 동시에 무선랜 환경에 대한 보안 문제 해결도 시급하다고할 수 있다. 본 논고에서는 무선랜 기술, 국내 무선랜 환경 및 보안 운영 현황, 무선랜 보안 관련 정부정책 방향 및 대응방안 등을 제시한다.

Ⅰ. 서 론

최근 스마트폰 및 태블릿 PC 보급은 언제 어디서나 편리하게 인터넷을 할 수 있는 환경을 가져다줌에 따라 우리생활의 많은 부분을 바꾸어 놓았다. 이러한 무선인터넷 환경에서 부각된 중요 기술 중 하나가 무선랜(Wireless LAN) 기술이다.

기존 국내 무선인터넷은 이동통신사의 고비용 폐쇄적인 3G 네트워크를 이용한 데이터 통신 위주로 이루어져 왔다. 특히, 유선 인프라가 잘 갖추어진 국내에서는 내부 구조변경이 잦은 백화점, 일부 연구소 및 기업 환경 등에서 제한적으로 무선랜이 사용되어 왔다.

이러한 배경에서 스마트폰의 등장은 무선랜 확산을 가속화 시켰다. 스마트폰은 이동통신사의 네트워크와 무선랜을 모두 이용 가능하다. 상대적으로 저렴하고 빠른 통신 속도를 가진 무선랜이 선호됨에 따라 가정, 학교, 공중시설 등을 중심으로 무선랜이 널리 보급되는 동시에 다양한 무선랜 이용 환경이 만들어 졌다.

무선랜은 다양한 장점과 편의성을 가지고 있어 이용이 급증하고 있지만, 전파를 통신매개로 이용하는 특징에 따라 보안을 고려하지 않고 이용할 경우 일반적인 유선랜에 비해 더욱 취약하다. 특히, 공중 무선랜과 같이 일반 대중의 사용을 목적으로 개방된 환경의 경우 다양한 보안 사고를 유발할 수 있어 보안에 대한 고려가 필수적이다.

이 글에서는 국내 무선랜 이용환경 및 구축현황을 살펴보고 무선랜 환경별 보안위협을 분석한다. 또한 제시된 무선랜 환경별 보안위협에 따른 대응방안을 설명한다[1][2][3].

Ⅱ. 무선랜 기술 및 현황

2.1 무선랜 기술

무선랜이란 유선랜(LAN)과 대비되는 표현으로 무선으로 네트워크를 이용할 수 있도록 하는 기술을 통칭하며 국제 표준화 기구인 IEEE에서 802 위원회의 하부 그룹인 802.11 그룹에서 표준화를 진행 중이다. 현재까지 제정된 무선랜 관련 주요 표준은 [표 1]과 같다[4].

또한 국제 표준 인증 단체인 Wi-Fi Alliance 에서는 IEEE에서 제정한 무선랜 표준을 만족하는 장치에 표준 적합 인증마크를 부여하고 있다. 대부분의 무선랜 관련

* 한국인터넷진흥원 (jhbaek@kisa.or.kr, cptpark@kisa.or.kr)

〔표 1〕 무선랜 기술표준 및 특징

무선랜 표준	제정 시기	주파수 대역	속도 (최대)
802.11	1997	2.4GHz	2 Mbps
802.11a	1999	5GHz	54 Mbps
802.11b	1999	2.4GHz	11 Mbps
802.11g	2003	2.4GHz	54 Mbps
802.11n	2009	2.4 / 5GHz	540 Mbps

장치에는 와이파이 인증마크가 부착되는데 이러한 이유로 흔히 무선랜과 와이파이라는 표현은 혼용되어 사용되고 있다[5].

무선랜 보안기술은 무선 AP에서 설정하도록 하는 기술로 인증과 암호화 방식에 따라 WEP (Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), WPA2(Wi-Fi Protected Access2)로 나뉜다.

각 보안 기술에서 사용자 인증 방법은 사전 공유한 패스워드 입력을 통해 이용자를 인증하는 방법(PSK : Pre-Shared Key)과 별도의 인증 서버를 통해 인증하는 방법이 있다. 암호화 방법은 유선상의 보안성 제공을 목적으로 하는 WEP 방식과 Key 동적 변경, 인증 서버 연동 등 WEP의 취약성을 개선한 WPA와 강력한 블록 암호화 방법인 AES(Advanced Encryption Standard)를 적용한 WPA2 방식이 있다.

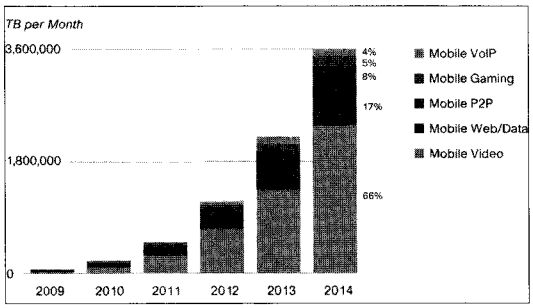
2.2 무선랜 현황

스마트 폰은 단순한 음성 통화기능 외에 인터넷전화, 모바일 게임, 모바일 Web, 모바일 비디오 등 데이터 통신을 이용하는 다양한 기능을 제공하고 있어 스마트폰 출시를 계기로 모바일 트래픽 사용량은 증가하였다. 태블릿 PC, Wi-Fi 제공 피처 폰(feature phone) 등 다양한 형태의 모바일 단말기가 출시되고 다양한 모바일 서비스가 활성화됨에 따라 향후에도 모바일 데이터 트래픽은 지속적으로 증가할 것으로 예상되고 있다[6].

〔표 2〕 무선랜 보안기술

구분	WEP	WPA	WPA2
인증	PSK	PSK or 인증서버	PSK or 인증서버
암호화	RC4	RC4-TKIP	AES-CCMP

※ TKIP : Temporal Key Integrity Protocol
CCMP : Counter Mode with Cipher Block Chaining Message Authentication Code Protocol



〔그림 1〕 모바일 트래픽 전망

이동통신사에서는 이동통신 네트워크만으로는 급증하는 모바일 트래픽을 수용하기 어려워짐에 따라 분산처리를 위한 대체 망 확보가 시급하게 되었고 이에 따라 무선랜이 주목받게 되었다.

무선랜은 공공 주파수 대역을 사용하므로 전파 사용료 지불 및 송출 허가가 불필요 하고 무선 AP의 가격이 저렴하여 단기간에 구축하기 적합하다. 또한 사용자 입장에서도 기존 이동통신 네트워크보다 빠른 속도와 저렴한 이용료로 이용할 수 있는 장점이 있다.

이러한 무선랜의 장점으로 2010년 상반기부터 경쟁적으로 이동통신사의 무선랜 구축이 이루어 졌으며, 그 결과 국내에서는 2010년 11월 현재 약 7만 곳 이상의 와이파이존이 구축되어 운용되고 있다. [표 3] 에서는 국내 이동통신 사업자가 구축한 와이파이존 현황을 보여주고 있다.

한편 국내에서는 무선 공유기를 함께 제공하는 인터넷 전화 보급 확대와 저렴한 무선 공유기 판매로 일반 가정에서도 무선랜을 구축하는 사례가 증가하고 있다. 또한 은행, 호텔, 레스토랑, 공항 등 공공시설에서도 고객 편의제공을 위한 무선랜 접속시설을 확대하는 등 전국적으로 무선랜을 이용할 수 있는 환경이 조성되고 있다.

〔표 3〕 국내 이동통신 3사 와이파이존 구축 현황

이동통신사	'09년 말	'10.7월	'10.12월
KT	약12,000	27,000	42,000
SKT	-	5,000	17,000
LGU+	-	-	16,000
계	약12,000	32,000	75,000

출처 : 각 사업자 발표, 언론보도

〔표 4〕 국내 인터넷전화 보급현황

단위 : 만명

구분	2006	2007	2008	2009	2010.10
가입자 (누적)	32	61	248	666	878

Ⅲ. 국내 무선랜 환경

국내 무선랜 이용환경은 구축 주체, 관리 주체, 이용 주체 등에 따라 5가지로 구분될 수 있다.

3.1 상용 무선랜 환경

이동통신사가 자사 고객 서비스용으로 구축·운영하는 무선랜 환경으로 일반적으로 와이파이존을 의미하며 이동통신사 이용 정책에 따라 개방형과 폐쇄형으로 나뉠수 있다. 상용 무선랜 환경 중 개방형 환경은 자사 고객 뿐 아니라 타사 고객까지 이용을 허가하는 환경을 의미하며 자사 고객의 경우 USIM(universal subscriber identity module), MAC(Media Access Control), ID/Password 등을 통해 이용하고, 타사 고객의 경우 실명인증 등의 방법을 통해 이용하는 방식이다. 폐쇄형 환경은 자사 고객에 대해서만 접속을 허용한다.

특히, 최근 무선랜 구축이 마케팅의 방법으로 대두되면서 경기장, 해수욕장, G20 정상 회담과 같은 각종 행사 장소 등지에 한시적인 무료 와이파이존을 구축하기도 하였다.

3.2 공중 무선랜 환경

고객들이 무료로 이용할 수 있도록 공공기관, 호텔, 카페 등에서 자체적으로 구축한 무선랜 환경을 의미하며, 이동통신사가 구축한 무선랜 환경이 주로 자사 가입자 중심인데 반해 공중 무선랜 환경의 이용자는 해당 사업자를 방문하는 고객이 대상이다. 공중 무선랜 환경은 소규모 환경으로서 별도의 보안 관리자를 두고 있지 않아 상대적으로 보안이 취약한 편이다.

3.3 사설 무선랜 환경

일반인들이 전자상가 등지에서 구매한 무선공유기를 임의로 설치하여 운영하는 환경으로 자신 또는 주변인만 이용 가능 하도록 구축한 환경이다. 무선공유기는 보안 기능은 탑재되어 있으나, 초기에 보안이 설정되어 있지 않고 이용자가 보안설정 지식 및 인식부족, 편의성을 이유로 보안을 설정하지 않고 이용하는 사례가 많다.

3.4 인터넷전화용 무선랜 환경

인터넷전화 설치 시에 제공되는 무선랜 환경으로서 인터넷전화용 무선공유기는 인터넷전화용과 데이터 통신용의 두 가지 무선랜을 동시에 제공한다. 인터넷전화용 무선랜의 경우 보안이 설정되어 있고 무선랜 정보가 숨겨져 있기 때문에 비교적 안전하지만 데이터 통신용 무선랜의 경우 외부에 알려진 초기 패스워드 사용으로 무단접속, 정보유출 등의 보안위협이 존재할 수 있다.

최근 이러한 문제를 개선하기위해 인터넷전화 사업자들은 초기 패스워드를 기기마다 다르게 설정하여 출시하고 있다. 가정에서 기존에 보급된 인터넷전화용 무선랜을 사용하는 경우 초기 설정된 패스워드를 변경하여 사용하는 것이 보다 안전한 무선랜을 이용하는 방법이다.

3.5 기업 무선랜 환경

기업이 내부 업무용으로 구축한 무선랜 환경을 의미하며 최근 스마트폰을 이용한 스마트 오피스, 스마트 워크 도입이 확산됨에 따라 점차 구축사례가 증가하고 있다. 기업 유선 네트워크로 접근할 경우 Firewall, IDS(Intrusion Detection System) 등 다양한 보안 시스템들로 내부망을 보호할 수 있으나 무선 네트워크의 경우 유선상의 보안 장치들을 우회 접근할 수 있어 별도의 보안 시스템 적용하는 것이 필요하다.

일반적으로 기업 무선랜 환경에서는 무선 AP 자체의 보안 설정, 인증서버 구축을 통한 인증 및 접근제어, WIPS(Wireless Intrusion Prevention System)등 다양한 보안 시스템을 적용할 수 있다.

3.6 이용 환경에 따른 무선랜 환경 구분

이용 주체 및 환경에 따라 무선랜 환경을 구분하면 [표 5]와 같이 크게 공중 및 개인 무선랜으로 구분 될수 있다. 공중 무선랜은 불특정다수를 대상으로 제공되는 무선랜을 의미하며 개인 무선랜은 가정내에서 개인이

〔표 5〕 이용 환경에 따른 구분

구분		제공 및 이용자	사례
공중	상용	통신사 제공, 다수 이용	QOOKnSHOW, T-WiFi zone, U+Zone
	사설	개인·기업 등 제공, 다수 이용	호텔, 커피숍 등에서 제공하는 Wi-Fi
개인	상용	통신사 제공, 개인 이용	인터넷전화, QOOKHub 등
	사설	개인 제공, 개인 이용	가정에서 개별 설치한 AP 등

이용하는 무선랜을 의미한다. 또한, 이통사 등에서 구축·관리하는 무선랜을 상용, 개인이 직접 구축·관리하는 무선랜을 사설로 구분할 수 있다.

Ⅳ. 무선랜 보안위협 및 대응방안

무선랜은 전파를 이용하여 통신하는 특성 때문에 물리적인 접근 없이 제공되는 서비스를 이용할 수 있고 전파 수집 및 교란을 통한 다양한 보안 위협을 야기할 수 있다.

이 글에서는 무선랜에서의 보안위협을 기술적인 측면과 함께 관리적, 물리적 측면으로 나누어 무선랜 보안위협과 대응방안을 설명한다[7][8].

4.1 기술적 보안 위협

무선랜의 기술적 보안위협은 전파수집, 불법접속, 중간자 공격(Man in the Middle Attack) 등을 통한 사용자 주요정보 유출과 전파 교란(Jamming), 다량의 패킷 전송을 이용한 서비스거부 공격이 있으며 WEP 등 취약한 보안설정을 해킹하여 불법접속 및 내부 망으로 침투하는 등 다양한 공격유형이 있다.

무선랜의 기술적 보안위협은 WPA2등 무선 AP에서 제공하는 보안을 설정함으로써 대부분 차단가능하다. 하지만 기업환경 등 중요정보를 취급하는 장소에서 무선랜 이용은 WIPS 등 전문 무선 보안 시스템 도입이 필요하다.

4.2 관리적 보안 위협

무선랜에 강력한 보안기술을 적용하여도 적절한 관리가 이루어지지 않는다면 이를 쉽게 우회할 수 있다. 관리적 보안위협으로는 무선랜 장비 및 단말 관리 미흡, 사용자 보안의식 결여로 인한 침입허용, 전파관리 미흡에 따른 외부자의 내부 AP접속 및 내부자의 외부 AP 접속 허용 등이 있다.

무선랜 관리적 보안위협의 대응 방안으로는 AP와 같은 접속장치 및 단말에 대한 관리방안을 수립·실시하고, 이용자들에 대한 주기적인 인식제고 및 교육, 내·외부 불법 접속에 대한 점검 등을 실시하여야 한다.

4.3 물리적 보안 위협

유선인터넷 환경의 네트워크 장비들이 대부분 일반 사용자가 접근하기 어려운 곳에 설치·관리 되는 것에 비해, 무선 AP는 전파송출의 필요성 등으로 외부에 노출되어 설치되는 경우가 많다. 이러한 경우 무선 AP는 도난/파손, 전원차단, 랜선 분리 등의 위험이 있으며, 서비스에 장애 상태가 발생할 수 있다. 또한, 무선단말기가 분실되어 저장된 무선랜 접속정보 및 보안설정 정보가 유출될 경우 비인가자의 무선랜 접속을 허용할 수 있다.

이와 같은 위협에 대비하기 위해서는 무선 AP가 외부에 노출되지 않도록 하고 설정정보를 주기적으로 변경하며 동시에 무선랜을 이용하는 단말 관리 및 분실대비 방안을 강구해야 한다.

4.4 기타 보안 위협

최근 인터넷전화 보급 및 공중무선랜 구축이 증가하게 되면서 새로운 보안위협이 등장하고 있다. 먼저 인터넷전화의 경우 초기패스워드가 외부로 알려져 있으나 인터넷전화 사용자들이 보안지식 및 인식부족으로 이를 변경하고 이용하지 않아 이를 통한 다양한 보안사고 발생 위협이 있다. 따라서 사업자 및 정부차원에서 무선랜의 보안위협을 충분히 인지시키고 이용자들이 스스로 또는 사업자들이 서비스 제공시 보안설정 및 암호 변경을 하도록 유도해야 한다.

공중 무선랜의 경우 누구나 이용할 수 있도록 구축되어져 있어 일반인 뿐 아니라 해커가 접속할 수도 있다. 이러한 경우 악성코드 유포 및 스팸발송의 근원지가 될 수 있으며 공중 무선랜에서 침해사고 발생 시 무선 AP까지만 추적이 가능하여 대응에 어려움을 야기할 수 있

다. 따라서 공중 무선랜 구축 시에는 이용자 접속관리 시스템 등 침해사고 추적을 위한 장치가 필요하다.

V. 정부 정책 방향

본 장에서는 최근 무선랜 이용이 급증함에 따라 무선랜 이용자를 보호하고 안전한 무선랜 이용환경 조성을 위한 정부의 정책방향에 대해 설명한다.

5.1 대국민 인식제고

최근 방통위에서 발표한 스마트 모바일 시큐리티 종합대책에 따르면 사설 무선랜 AP의 48%가 보안설정이 없는 것으로 파악되었다[10]. 이는 무선랜에 대한 보안 기술이 부재하다기 보다는 이용자들의 보안설정에 대한 지식 부족 및 보안인식 부족에 따른 것으로 판단된다. 이에 따라, 정부에서는 무선랜 보안 강화를 위한 대국민 인식제고를 추진하고 있으며 KISA에서는 국민친화적인 대중매체를 통한 홍보를 실시하고 있다.

무선랜을 안전하게 이용하기 위해서는 무선랜 설치 시 초기 패스워드 변경 등 보안설정을 반드시 수행하여야 하며, 무선랜을 사용하지 않을 경우 전원을 끄고, 제공자가 불명확한 무선랜 사용 않기 등 이용 수칙을 지켜야한다. 이를 위해 KISA에서는 해당 수칙을 홍보하기 위한 리플릿을 제작하여 전국 지자체에 배포하였으며, 버스 및 지하철 등 대중교통 수단을 이용한 홍보, 무선랜 보안 관련 TV 및 라디오 방송 송출 등의 인식제고 사업을 추진하였다. 또한, Weekly 공감과 같은 정책홍보지, TTA 저널 등에 무선랜 보안 관련 기고를 추진하였으며, 보호나라에 무선랜 보안 전용 페이지를 개설하여 국민들이 무선랜 보안에 대한 관련 정보를 쉽게 접할 수 있도록 하였다.

이와 같이 정부에서는 국민들이 보다 쉽게 무선랜 보안 관련 정보를 획득하고 안전한 무선랜 이용 환경을 조성하기 위해 대국민 인식제고 사업을 지속적으로 확대해 나갈 예정이다.

5.2 무선랜 구축 시 보안 기능 강화

무선랜 이용자를 대상으로 추진하는 보안 인식제고 이외에 이통사와의 협력을 통해 무선랜 구축·운영 시 보안 기능을 강화하는 방안이 추가적으로 필요하다.

현재 이통사의 경우 스마트폰 보급 등으로 무선랜 이용의 급격한 증가에 맞춰 '10년 하반기부터 자체적인 보안을 강화하고 있다. KT의 경우 USIM을 이용한 인증, 단말-AP 구간에 WPA2 적용, I-WLAN 도입 등을 통하여 스마트폰 이용자 및 가정내 고객에게 안전한 무선랜 서비스를 제공하고 있다. LGU+의 경우 802.1x 기반 인증, WPA2 암호화, 사용자 유형별 개인별 트래픽 분리 등 TTA 인증 3중 보안체계 적용을 통해 안전한 무선랜 서비스를 제공하고 있다. SKT의 경우 단말과 AP를 연결하는 Access 구간, AP와 라우터를 연결하는 전송 구간, 관제 및 인증을 담당하는 Infra 구간으로 분리하여 관리 및 PDG 기술을 도입하여 안전한 서비스를 제공하고 있다.

또한, 이통사는 방통위, KISA와 협력하여 고객 상담센터 운영, A/S 기사 등 기술 지원조직을 활용한 무선랜 보안 설정 서비스 제공, 신규 단말 설치 시 설치기사를 통한 안내, 제품 사용설명서 개정, 서비스 홈페이지를 통한 안내, 요금 고지서를 통한 안내, 안내 메일 발송, 무선 공유기에 보안 문구 표기 부착 등을 통해 보안을 강화하고 있다.

5.3 법제도 개선 검토

무선랜 보안을 위한 대응방안의 하나로 법제도 개선 방안을 마련할 수 있다. 하지만, 대부분 국민이 주로 이용하는 무선랜에 대해 강제적인 법제도를 마련하는 것은 부작용이 발생할 수 있기 때문에 신중한 접근이 필요하다. 현재 국외 무선랜 보안 관련 법제도 현황은 무선랜 운영자에 대한 보안 사고 책임 부과, 사용자 권한 없는 접근 금지 및 처벌, 요금회피 목적 타인 서비스 이용 금지, 허가제도 등의 규제를 일부 국가에서 추진하고 있다[11]. 우리나라의 경우 현재 무선랜 보안 관련한 직접적인 규제는 없는 상황이며 추후 필요성 검토를 통해 우선적으로 기업이 구축·운영하는 무선랜 환경에 대한 보안 강화 제도 방안을 마련할 수 있을것으로 판단된다.

예를 들어, 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따른 정보보호관리체계(ISMS) 인증 기준에 무선랜 사용자 인증, 통신 암호화 여부, 무선 AP에 대한 운영·관리를 위한 정책 수립·시행 등 무선랜 보안 관련된 부분을 포함하는 방안을 검토할 수 있다. 또

한, ISP 및 VoIP 등 관련 사업자의 이용 약관에 무선 AP 보안설정 사항을 반영하는 방안도 고려할 수 있다. 약관의 경우 사업자가 이용자에게 무선AP의 보안 위험성에 대한 고지, 이용자가 보안설정을 하지 않아 발생하는 정보유출 등 문제에 대한 ISP의 면책규정을 추가 방안 등이 가능할 것으로 보인다.

Ⅵ. 결 론

2009년 하반기부터 시작된 스마트폰 열풍으로 무선랜 이용은 급격히 증가하였다. 무선랜 기술이 갑자기 등장한 것은 아니지만 이동통신사업자의 적극적 무선랜 인프라 활용, 유무선 융합 서비스 출시, 다양한 형태의 사설 무선 AP 보급 등으로 다양한 환경에서 무선랜을 사용하게 됨에 따라 무선랜은 점차 필수적인 서비스가 되고 있다.

무선랜의 경우 제조 시부터 보안 설정이 가능하도록 출시가 되고 있지만 대부분 이용자들의 인식부족이나 사용 불편으로 보안 설정을 하지않고 사용하는 경우가 많이 존재한다. 이에 따라, 최근 무선랜을 통한 개인정보 유출 등에 대한 이슈가 발생하고 있다. 지난해부터 정부를 중심으로 무선랜 보안 인식제고를 위한 다양한 방식의 홍보가 추진되고 있어 무선랜 보안에 대한 대국민 인식이 개선되고 있는 실정이긴 하지만 여전히 보안 강화를 위한 노력이 다방면으로 확대·추진될 필요가 있다.

특히, 공중 무선랜 뿐아니라 보안설정이 상대적으로 낮은 사설 무선랜에 대한 보안 강화 노력이 필요하다. 이를 위해, 호텔, 학교, 커피숍 등에서 별도로 설치 운영하고 있는 무선랜에 대한 특화된 보안 대책이 필요하다. 또한, 이동통신사와 정부간 협력을 통해 와이파이존과 같은 상용 무선랜에서도 보안사고 방지를 위한 대응체계 수립이 필요하며, 동시에 인터넷 전화 등 가정용 무선랜 상품에 대한 보안 대책도 추진해야 한다.

안전한 무선랜 이용을 위해서는 정부, 이동통신사, 제조사 등의 보안 강화 노력이 중요한 요소이긴 하지만, 무선랜 특성상 무엇보다도 국민 개개인이 보안의식을 고취하고 스스로 무선랜 보안을 책임진다는 생각으로 무선랜 보안 설정에 앞장서야 한다. 무선랜 보안 설정이 기술적으로 관리적으로 어려운 내용이 아니기 때문에 내 개인정보는 내가 지킨다는 생각으로 개개인이 속해 있는 가정이나 직장 등의 무선랜 보안 설정을 실천하는 것이 무엇보다 중요하다. 무선랜 보안 설정 관련 정보는 정부에서 제공하는 홍보물이나 웹사이트 등을 통해 손쉽게 획득할 수 있다[7][9].

참고문헌

[1] 백종현, "Wireless LAN Status and Security Issues in Korea" CJK SWIS 2010, Nov 2010.

[2] 백종현, "국내 Wi-Fi 보안 현황 및 안전한 무선랜 이용 가이드", TTA Journal No,132, pp. 67-72, Nov 2010.

[3] 박순태, 원용근, 백종현, "무선랜 이용 환경별 보안 위협 및 대응방안", 제34회 한국정보처리학회 추계 학술발표대회 논문집 제17권 제2호, pp. 1350-1353, 2010년 11월.

[4] http://standards.ieee.org/getieee802/ 802.11.html

[5] http://www.wi-fi.org/brand.php

[6] CISCO, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2009-2014", Feb 2010.

[7] 방송통신위원회, 한국인터넷진흥원, "알기쉬운 무선랜 보안 안내서", 2010년 10월.

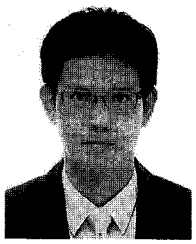
[8] 한국인터넷진흥원, "무선랜 보안 안내서", 2008년 11월.

[9] http://www.boho.or.kr/hacking/hack_06.jsp

[10] 방송통신위원회, "스마트 모바일 시큐리티 종합대책", 2010년 1월

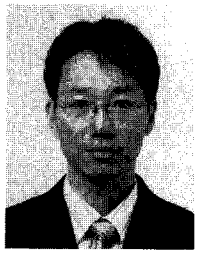
[11] 오병철 외, "해외 무선랜 보안 법제도 연구", 한국인터넷진흥원, 2010년 7월

〈著者紹介〉



백 종 현 (Jonghyun Baek)

1996년 2월 : 순천향대학교 전자공학과 졸업
1998년 2월 : 순천향대학교 전자공학과 석사
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2001년 4월 ~ 현재 : KISA 무선인터넷 팀장('10년 1월 ~ 현재), KISA 전자인증팀장 역임('08~'09)
2009년 2월 ~ 현재 : ITU-T SG17 Q6 의장
<관심분야> PKI, 무선랜보안, 무선인터넷 등



박 순 태 (SoonTai Park)

정회원

1992년 2월 : 단국대학교 전자계산학과 학사
1998년 8월 : 국민대학교 정보과학대학원 정보통신학과 석사
2010년 8월 : 전남대학교 대학원 정보보호협동과정 박사
1994년 7월~1999년 9월 : 육군 전산장교
2000년 4월~현재 : 한국인터넷진흥원 무선인터넷팀
<관심분야> 정보보호, 정보보증, IT 보안성 평가, 정보보호 인력 양성, 정보통신 기반 보호, 무선랜 보안