|  |  |
| --- | --- |
| **KSKSKSKS****KSKSKSK****KSKSKS****KSKSK****KSKS****KSK****KS** | KS X 3100 |
|  | **공공 무선 랜 서비스** KS X 3100 : 2011 (2017 확인) |
| **방 송 통 신 표 준 심 의 회****2011년 6월 27일 제정** |

**심 의 : 전파통신 기술심의회(X)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 성명 |  | 근 무 처 |  | 직위 |  |
| (회 장)  |  | 윤영중 |  | 연세대학교 |  | 교수 |  |
| (위 원) |  | 김동일 |  | 동의대학교 |  | 교수 |  |
|  |  | 김창주 |  | 한국전자통신연구원 |  | 책임연구원 |  |
|  |  | 박준구 |  | 경북대학교 |  | 교수 |  |
|  |  | 최상호 |  | 한국전파진흥협회 전자파기술원 |  | 원장 |  |
|  |  | 최조천 |  | 목포해양대학교 |  | 교수 |  |
| (간 사) |  | 권병욱 |  | 국립전파연구원 |  | 과장 |  |

표준열람 : 국립전파연구원(<http://www.rra.go.kr>)

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

제 정 자：방송통신표준심의회 위원장 담당부처：과학기술정보통신부 국립전파연구원

제 정：2011년 6월 27일

심 의：방송통신표준심의회 전파통신 기술심의회(X)

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

이 표준에 대한 의견 또는 질문은 국립전파연구원 웹사이트를 이용하여 주십시오.

이 표준은 방송통신표준화지침 제18조의 규정에 따라 매 5년마다 방송통신표준심의회에서 심의되어 확인, 개정 또는 폐지됩니다.

목 차

[머 리 말 4](#_Toc434321810)

[1 적용범위 및 목적 5](#_Toc434321811)

[2 인용규격 5](#_Toc434321812)

[3 정의 5](#_Toc434321813)

[3.1 공공 무선 랜 5](#_Toc434321814)

[3.2 서비스 세트 식별자(SSID: Service Set Identifier) 5](#_Toc434321815)

[3.3 IEEE 802.1x 5](#_Toc434321816)

[3.4 IEEE 802.11i 5](#_Toc434321817)

[3.5 AES-CCMP 5](#_Toc434321818)

[3.6 사용자 인증서(User certificate) 6](#_Toc434321819)

[3.7 와이파이(Wi-Fi, Wireless Fidelity) 6](#_Toc434321820)

[4 공공 무선 랜 서비스 제공 현황 및 문제점 7](#_Toc434321821)

[5 공공 무선 랜 서비스 제공 방식 7](#_Toc434321822)

[5.1 참조 모델 7](#_Toc434321823)

[5.2 참조 사례 10](#_Toc434321824)

[6 요구 사항 12](#_Toc434321825)

[6.1 네트워크 12](#_Toc434321826)

[6.2 보안 14](#_Toc434321827)

[6.3 일반 사항 16](#_Toc434321828)

[7 상호 운용성 17](#_Toc434321829)

[8 공공 무선 랜 서비스 제공 점검 리스트 18](#_Toc434321830)

머 리 말

본 표준에서는 무선 네트워크 일반 설정, 사용자 인증 방식, 암호화 방식 등 공공 목 적의 무선 랜 인프라 구축에 참조 가능한 서비스 제공 모델을 제공한다. 개방형과 데이 터 암호화를 동시에 지원하도록 하여 보안 적용 여부를 선택할 수 있도록 하고 무선 네트워크 식별자인 서비스 세트 식별자(SSID:Service Set ID)를 코드 표기 방식으로 체계 화 한다. 데이터 보안을 위한 암호화 방식으로는, IEEE 802.11i에서 정의하고 있는 고급 암호 표준(AES: Advanced Encryption Standard)을 이용한 무선 공유기(AP)(CCMP: Counter mode with CBC-MAC Protocol) 알고리즘을 적용할 것을 권고한다. 그리고, 사용자 인증 방식으로 유무선 이더넷용 802.1x 기반의 상호 인증 방식을 채택하도록 한다. 또한, 서비스 품질 관리를 위해서 무선 공유기(AP) 접속 인원 제한, 대역폭 제한, 이용 시간 제한 등의 일반 요구 사항도 제시한다.

스마트폰 확산에 따라 무선 랜 접속을 통한 무선 인터넷 이용이 급증하는 가운데, 지자체 및 공공기관 등에서 본 표준에서 권고하고 있는 기술 사항들을 참조한다면 보다 안전하고 안정적인 무선 랜 인프라 확산 및 이용 활성화에 기여할 수 있을 것이다.

**방송통신표준**

**KS X 3100 : 2011**

|  |
| --- |
| **공공 무선 랜 서비스**  |

WLAN Service for Public Sectors

# 적용범위 및 목적

본 표준은 공공시설(관공서, 공원, 도서관 등)에서 일반 이용자의 인터넷 접속을 위한 공공 무선 랜 서비스 제공 시, 보다 안전하고 편리한 무선 랜 이용 환경 조성을 위해 공 공 무선 랜 서비스 제공 참조 모델과 해당 기술 요구 사항들을 제시한다.

# 인용규격

- IEEE, "Local and metropolitan area networks-Specific requirements - Part11:Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specifications", IEEE Std 802.11TM-2007, June 2007

- WPA for 802.11 Specification - Version 2.0, April 29, 2003

- TTA, TTAS.KO-12.0031, "안전한 무선 랜 사용을 위한 가이드", 2005.12.

- 방송통신위원회, "무선 랜 보안 운영 권고안", 2003.7.

- 국가정보원 국가사이버안전센터,"무선LAN'의 안전한 사용을 위한 보안 대책", 2005.9.

# 정의

이 표준의 목적을 위해 다음의 용어 정의가 적용된다.

## 공공 무선 랜

지자체 및 공공 기관에서 대민 서비스 차원에서 인터넷 접속을 사용자에게 제공하는 공공 분야 무선 랜

## 서비스 세트 식별자(SSID: Service Set Identifier)

SSID는 무선 랜을 통해 전송되 는 패킷들의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로서 서비스 받 고 있는 무선 랜을 식별하거나 확인하기 위해 사용)

## IEEE 802.1x

802.1x는 유선 이더넷 네트워크 및 무선 802.11 네트워크에 대한 인증된 네트워크 액세스를 제공하는 IEEE 표준으로, 중앙 사용자 ID, 인증, 동적 키 관리 및 계정을 지원

## IEEE 802.11i

IEEE 802.11i 표준은 무선 랜 사용자 보호를 위해서 사용자 인증 방식, 키 교환 방식 및 향상된 무선 구간 암호 알고리즘을 정의한 표준

## AES-CCMP

CCMP(Counter mode with CBC-MAC Protocol)는 CCM 모드를 사용하는 고급 암호 표준 (AES: Advanced Encryption Standard) 암호 알고리즘 사용

## 사용자 인증서(User certificate)

인증 기관의 개인 키로 암호화되어 위조할 수 없게 만들어진 사용자의 공개 키 및 기타 정보

## 와이파이(Wi-Fi, Wireless Fidelity)

근거리 무선 랜이라고 함. 무선 공유기(AP)의 일정 거리 안에 있으면 전파나 적외선을 이용해 스마트폰·노트북 등 휴대기기로 인터넷을 쓸 수 있는 근거리 무선망

# 공공 무선 랜 서비스 제공 현황 및 문제점

- 애플 앱 스토어, 안드로이드 마켓과 같은 모바일 시장의 등장과 함께 아이폰 등 스마트폰 보급이 급속히 확산되면서 무선데이터 이용량도 급증하는 추세.

- 공중 무선 랜 서비스 지역은 약 16,500개소(‘10년 4월 기준)가 구축되어 있으며, 2010년 말에는 총 66,000개소 구축이 계획되어 있음. 그러나 핫스팟은 유동 인구가 많고 홍보 효과가 높은 장소에 편중되어 있음.

- KT, AT&T 등 통신사들은 초기 가입자 기반 유료 서비스를 제공하였으나, 현재는 결합 상품, 스폰서 기업 제휴를 통한 무료 무선 랜 서비스를 확대하고 있다. 구글, 야후, 네이버 등 인터넷 기업은 검색과 광고 시장 확대를 위해 무료 무선 랜 서비스를 제공 중 .

- 일부 지자체에서 도시 내 일부 지역에 무선 공유기(AP)를 구축하고 시민에게 무료 개방.

- 공공 기관에서 제공 중인 대국민 무선 랜 서비스의 경우, 관리 기관에 따라 구축 방식과 서비스 제공 방식이 다르며, 개별적 운영되고 있음.

- 무인증․무보안으로 서비스를 제공하고 있어 무선 랜 서비스를 이용하고자 하는 사용 자를 대상으로 서비스 제공 지역 등에 대한 신뢰성 있는 정보 제공에는 미흡

- 안정적인 무선 랜 서비스 제공을 위해서는 네트워크 식별, 무선 랜 접속, 인증, 보안 관리를 위한 통합 권고 지침 마련 필요

# 공공 무선 랜 서비스 제공 방식

공공장소에서 보편적 인터넷 접속 제공을 목적으로 제공되는 무선 랜 서비스의 경우, 모두 공공 무선 랜 서비스의 범주에 해당하며 정부 기관, 산하 기관, 공기업, 지자체 단독 또는 통신 사업자와의 협력 등을 통해 공공 무선 랜 인프라의 구축, 운영 및 관리가 가능하다. 이처럼 다양한 주체에 의해 제공될 수 있는 공공 무선 랜은 본 장에서 제시하는 참조 모델에 따라 구축하고 서비스를 제공함으로써 이용의 편의성과 보안성 향상을 도모할 수 있다.

## 참조 모델

공공 무선 랜 서비스는 무선 보안 적용 수준에 따라 크게 개방형, 사용자 인증, 데이터 암호화 등의 3가지 방식으로 구분 할 수 있으며, 서비스 제공 주체는 이들 제공 방식의 조합을 통해 최종적인 공공 무선 랜 서비스 제공 형태를 결정할 수 있다.

### 개방

단말과 무선 공유기(AP) 간 무선 연결이 완료되면 인터넷 프로토콜(IP)주소를 할당하여 즉시 인터넷 접속이 가능하도록 하는 방식으로, 별도의 사용자 인증과 데이터 암호화 과정이 필요 없고 사용자는 무선 네트워크 식별자인 서비스 세트 식별자(SSID)로 연결 시도만 하면 즉시 인터넷에 접속할 수 있다. 일반적인 웹 서핑과 정보 검색 등 서비스 내용의 속성상 개인 정보 유출의 위험성이 없는 경우에는 보안상 큰 우려가 없지만, 메일, 메신 저 등 개인정보 노출이 우려되는 웹 서비스의 경우 보안 소켓 계층 (SSL: Secure Sockets Layer)이나 가상 사설 통신망(VPN: Virtual Private Network)등 별도의 데이터 암호화 방식을 적용하는 것이 좋다. 또한 웹사이트 로그인 시 아이디와 비밀번호 정보를 해당 사이트에서 자체적으로 보호하지 않는 경우도 많으므로 이 점에 주의해야 한다.

### 사용자 인증

사용자 인증을 통해 무선 네트워크 접속을 제한적으로 허용하는 방식으로 인증서, 아이디/비밀번호, 단말 매체 접근 제어(MAC: Media Access Control) 주소 등 다양한 방식으로 구현 가능하다. 무선 랜의 경우, IEEE 802.1x 확장 가능 인증 프로토콜(EAP: Extensible Authentication Protocol) 기반의 사용자 인증이 표준기술로 사용되고 있으며 전송 계층 보안(TLS: Transport Layer Security), 터널 전송 계층 보안(TTLS: Tunneled Transport Layer Security), MD5, PEAP-MSCHAPv2 등 지원하는 확장 인증 프로토콜 (EAP) 타입에 따라 여러 가지 방식의 인증이 가능하다.

### 데이터 암호화

무선 데이터 암호화를 위해서 유선급 보안 암호화 방식(WEP: Wired Equivalent Privacy)이나 임시 키 무결성 프로토콜(TKIP:Temporal Key Integrity Protocol)과 같이 무선 공유기(AP)와 단말에서 고정형 암호키를 동일하게 설정하는 방식이 주로 이용되어 왔으며 현재는 AES-CCMP와 같은 보다 강력한 암호화 알고리즘이 표준으로 채택되어 사용되고 있다. 공공 무선 랜 서비스는 불특정 다수를 대상으로 하는 서비스이기 때문에, 고정형 암호화 키를 설정하는 방식은 적용 불가능하므로 IEEE 802.1x 확장 가능 인증 프로토콜(EAP) 방식의 동적 암호화 키 생성 및 공유 프로토콜을 사용해야 한다.

일반 인터넷 이용자를 대상으로 하는 공공 무선 랜 서비스는 공공 서비스 제공 관점에서 사용자 편의성과 보안을 적절히 조화해가는 것이 필요하며, 특히 개인 정보 유출 등의 보안 사고가 발생하지 않도록 무선 데이터 암호화와 같은 보안 체계를 도입하는 것이 바람직하다. <표 5-1>은 대표적인 공공 무선 랜 서비스 제공 형태를 보안 관점에서 차별적으로 분류한 것이다. 가장 높은 수준의 보안을 제공하는 ‘S등급’은 사용자 인증과 데이터 암호화를 모두 지원하는 경우이다. ‘1등급’ 서비스는 데이터 보안 방식을, ‘2등급’ 서비스는 사용자 인증 방식을 제공하는 경우에 해당된다. 위에서 언급한 3가지 등급 모두 개방형 방식을 동시에 제공하여 보안 접속이 어려운 사용자의 선택적 접속을 허용할 수 있으며, 이 경우 보안 네트워크의 보안성을 저해하지 않도록 주의해야 한다.

<표 5-1> 보안 관점에서 분류한 공공 무선 랜 서비스 등급

|  |  |  |  |
| --- | --- | --- | --- |
|  | 개방형(\*) | 사용자 인증 | 데이터 암호화 |
| S등급 | ○ | ○ | ○ |
| 1등급 | ○ |  | ○ |
| 2등급 | ○ | ○ |  |
| 3등급 | ○ |  |  |

 (\*) S등급, 1등급 및 2등급 서비스의 경우, 개방형을 함께 지원하지 않는 경우에도 등급 분류는 동일하게 처리함

안전하고 편리한 공공 무선 랜 서비스 제공이라는 원칙에 근거하여 본 표준에서는 보안 1등급 이상에 해당하면서 개방형을 동시에 제공하는 경우에 한해 ‘공공 무선 랜 제공 참조 모델’로 정의하고 있으며, 각 공공 무선 랜 서비스 운영 주체는 이 참조 모델에 부합

하도록 공공 무선 랜 인프라를 새로 구축하거나 기존 인프라를 변경하는 것이 바람직하다.



(그림 5-1) 공공 무선 랜 서비스 참조 모델

데이터 암호화 방식과 개방형을 동시에 제공하도록 한 기본 참조 모델에서 사용자 인증은 선택적으로 적용할 수 있다. 데이터 암호화 방식만으로 공공 무선 랜 서비스를 제공할 때, 단말의 데이터 암호화 미지원으로 인해 접속이 불가능한 경우가 발생할 수 있으며 이런 점을 고려하여 개방형 방식을 데이터 암호화 방식과 동시에 제공하도록 한다. 즉, 이용자가 데이터 보안 방식과 미보안 상태의 개방형 방식 중 임의의 방식을 선택할 수 있도록 하고, 개방형 방식 선택 시에는 사용자에게 반드시 관련 보안 유의사항을 알려주어야 한다.

이미 개방형 방식으로만 공공 무선 랜 서비스를 제공하고 있는 경우에는 점진적으로 데이터 암호화를 추가하는 것이 필요한데, 데이터 암호화 지원을 위한 단계적 보안 개선 방안을 마련하고 이에 대한 구체적인 실행 계획을 세워 향후에 무선 데이터 암호화를 적용하면 된다. 이러한 점진적 보안 강화 방식은 네트워크 구축 및 서비스 제공 관점의 전략적인 방법의 일환이다.

## 참조 사례

본 절에서는 가상적인 무선 랜 인프라 구축 및 서비스 제공 사례를 통해 앞서 5.1절에서 제시한 공공 무선 랜 서비스 제공 참조 모델의 이해를 돕고자 한다. 참조 사례는 데이터 암호화와 개방형을 동시에 제공하는 공공 무선 랜 핫스팟 구축에 관한 것이다.

### 인프라 구축

관공서, 공원, 도서관 등 공공시설을 대상으로 한 공공 무선 랜 서비스를 제공하기 위한 인프라 구축 방안의 한 예는 아래와 같다.

가. 공공 무선 랜 접속 네트워크와 공공 기관의 내부망을 물리적 또는 논리적으로 분리

나. IEEE 802.11 표준 규격을 준수하는 무선 랜 시스템 도입

다. 캡티브 포털(Captive Portal) 서비스 제공, 래디우스(RADIUS) 서버, 무선 공유기 (AP) 관리 등 소규모 무선 랜 핫스팟 구축에 적합한 무선 랜 컨트롤러 도입

라. 전원 공급을 손쉽게 하기 위하여 이더넷 전원b장치(PoE: Power Of Ethernet) 스위치 도입

마. 무선 랜 컨트롤러의 인증 서버 외에 손쉬운 사용자 관리와 전체 사용자 수를 감안하여 외부 인증 서버 사용여부 검토

바. 다중 서비스 세트 식별자(SSID) 또는 복수의 무선 공유기(AP)를 사용하여 무선 랜 접속 환경을 보안 네트워크와 비보안 개방형 네트워크로 분리

사. 무선 랜 단말의 인터넷프로토콜(IP)은 사설 인터넷프로토콜(IP) 또는 공인 인터넷 프로토콜(IP) 할당할 수 있음

아. 일정 수준 이상의 데이터 속도와 범위를 확보할 수 있도록 무선 공유기(AP) 포설



(그림 5-2) 공공 무선 랜 인프라 구축 예

### 서비스 제공

공공 무선 랜 서비스는 사용자가 좀 더 안전하고 편리하게 공공 무선 랜을 이용할 수 있도록 쉽고 직관적인 무선 랜 접속 서비스를 제공해야 하며, 무인증․ 무보안의 개방형 서비스 제공하는 것뿐만 아니라 사용자 인증 및 데이터 보안 방식도 함께 제공해야 한다. 다음은 공공 무선 랜 서비스의 일반 접속 절차 사례를 소개하고 있다.

가. 무선 네트워크 검색

나. 검색된 서비스 세트 식별자(SSID) 중에서 접속하고자 하는 공공 무선 랜 서비스 세트 식별자(SSID)를 선택

다. 캡티브 포탈 서비스를 제공하는 경우, 웹브라우저 연결 시 초기 안내 메시지 뜸.

- 무선 랜 컨트롤러에서 제공하는 캡티브 포털 서비스를 통하여 접속 안내 페이지로 연결됨.

- 비보안 접속 또는 보안 접속 연결 중 하나를 선택.

라. 비보안 접속인 경우, 무선 보안 취약성에 관한 안내문을 읽은 후 즉시 인터넷 접속 허용.

마. 보안 접속인 경우, 웹 브라우저 초기 안내 페이지의 무선 랜 보안 설정 안내 또는 무선 랜 보안 설정 가이드에 따라 사용자가 직접 설정하거나 자동 접속 툴을 제공.

- 보안 네트워크 접속 파라미터 설정 예는 다음과 같음.

* 네트워크 모드: "Infrastructure"

◇ 802.1x 인증: "enabled"

◇ 보안 타입․ 모드: WPA2-Enterprise (“AES" 데이터 암호), WPA-Enterprise ("TKIP" 데이터 암호)

◇ EAP 타입에 대한 보안 설정: "EAP-PEAP"

* 인증 방법: "EAP-MSCHAPv2"

바. 사용자 등록을 통하여 등록된 아이디, 패스워드를 입력. 별도의 사용자 등록 없이 하나의 공통 아이디 및 패스워드를 사용자에게 제공하여 사용할 수도 있음.

사. 웹브라우저를 오픈하면 '사용자 이용 약관 및 주의 사항'을 인지했음에 동의하여야 무선 인터넷이 연결됨.



(그림 5-3) 공공 무선 랜 서비스 제공 예

# 요구 사항

## 네트워크

### 공공 무선 랜과 내부망 분리

보편적 인터넷 접속을 위해 구축되는 공공 무선 랜은 서비스를 제공하는 공공 기관 또는 지자체의 내부망과 물리적 또는 논리적으로 분리되어 있어야 한다. 예를 들면, 비대칭 디지털 가입자 회선(ADSL)/초고속 디지털 가입자 회선(VDSL), 이더넷, 케이블 등 별도의 가입자 인터넷 회선에 무선 공유기(AP)를 연결하여 제공하는 경우, 물리적으로 내부망과 완전히 분리된 상태라고 볼 수 있다. 만일 물리적으로 분리가 어려울 경우에는 단말 가상화, 네트워크 가상화, 운영 관제 가상화 등을 통한 논리적 망 분리가 필요하며 가상 랜(VLAN), 방화벽(Firewall) 등으로 무선 랜과 내부망의 데이터 트래픽을 관리하는 경우에도 논리적으로 분리되어 있다고 볼 수 있다.

### 보안 및 개방형 무선 랜으로 복합 구성

다중 서비스 세트 식별자(SSID) 또는 다수의 무선 공유기(AP)를 사용하여 보안 네트워크와 비보안 개방형 네트워크로 분리함으로써 사용자가 네트워크 접속 시, 보안 적용 유무를 선택할 수 있도록 한다. 이때, 보안 또는 개방형 네트워크는 각각의 속성이 적용 되는 서비스 세트 식별자(SSID)에 의해 구별되는데, 개방형 무선 랜 접속 시에는 보안 및 개인 정보 유출 위험성 등을 사전에 충분히 고지하고 이에 동의해야만 인터넷 서비스가 가능하도록 한다.

 

(a) 다중 서비스 세트 식별자(SSID) 설정 (b) 2대의 무선 공유기(AP)에 각각 다른 서비스

세트 식별자(SSID) 설정

(그림 6-1) 보안 네트워크와 비보안 네트워크 분리

### 서비스 세트 식별자(SSID) 공개

서비스 세트 식별자(SSID)는 공개로 설정하여 무선 네트워크 검색이 가능하도록 해야 한다. 공공 무선 랜 핫스팟 커버리지 범위 내에 있는 이용자가 공공 무선 랜 서비스 지역임을 인지하고 접속할 수 있도록 반드시 하나 이상의 서비스 세트 식별자(SSID)를 공개해야 한다. 그러나 보안과 개방형 무선 랜에 해당하는 각각의 서비스 세트 식별자 (SSID)를 모두 공개하거나 초기 안내페이지로 연결되는 대표 서비스 세트 식별자(SSID) 만 공개할 수도 있다.

### 서비스 세트 식별자(SSID) 표기 방법 체계화

서비스 세트 식별자 (SSID)는 0~32 바이트 길이이며 아스키 코드로 표기하도록 정해져 있다. (그림 5-1)의 공공 무선 랜 서비스 제공 참조 모델에서 비보안 개방형 무선 네트워크를 지칭하는 서비스 세트 식별자(SSID)를 ‘PublicWiFi’라고 정하고, 서비스 세트 식별자(SSID)를 ‘PublicWiFiSecure'라고 정의한다. 이때, 공공 서비스 세트 식별자(SSID) 역할을 하는 ’PublicWiFi'는 브랜드명 정책에 따라 새로운 이름으로 변경 가능하다. 이러한 단일 서비스 세트 식별자(SSID)표기 방법을 바탕으로 아래와 같이 보다 확장된 서비스 세트 식별자(SSID) 표기가 가능하다.

- 단일 표기 방식 : ‘브랜드명‘ = PublicWiFi 및 PublicWiFiSecure

- 기본 표기 방식 : <SSID>="PublicWiFi"+"@"+<제공 주체>

- 확장 표기 방식 : <SSID>="PublicWiFi"+"@"+<시설명>+"."+<제공 주체>

"PublicWiFi": 공공 무선 랜 서비스임을 표시하는 브랜드명

<제공 주체>: 지자체 및 공공 기관 등의 명칭을 기입함

공공 무선 랜 서비스 제공 주체는 위에서 정의한 단일, 기본 또는 확장 표기 방식 중

적합한 서비스 세트 식별자(SSID) 표기 방식을 선택적으로 적용하면 된다. 예를 들어, <표 6-1>에서처럼 서울시에서 제공하는 공공 무선 랜 서비스의 무선 네트워크 식별자 (SSID)는 'PublicWiFi'나 'PublicWiFi@Seoul'로 서비스 제공 지역에 상관없이 공통적으로 설정할 수 있으며, 도서관, 광장, 학교, 공원, 박물관 등 시설 및 장소에 따라 각각 고유의 서비스 세트 식별자(SSID)를 설정하는 것도 가능하다.

<표 6-1> 서비스 세트 식별자(SSID) 표기 방법 예시

|  |  |  |
| --- | --- | --- |
| 단일 표기 | 기본 표기 | 확장 표기 |
| PublicWiFi PublicWiFiSecure | PublicWiFi@Seoul PublicWiFi@TTA PublicWiFi@Korail PublicWiFi@Subway | PublicWiFi@Library.Seoul PublicWiFi@Square.Seoul PublicWiFi@School.Seoul PublicWiFi@Park.Seoul PublicWiFi@Museum.Seoul |

## 보안

### 무선 데이터 암호화

공공 무선 랜 서비스는 단말과 무선 공유기(AP) 간 무선 구간의 데이터 보안을 위해 IEEE 802.11i 표준 암호화 방식인 AES-CCMP 암호화 알고리즘을 사용하도록 한다. AES-CCMP 알고리즘의 동적 암호화 키 할당을 위해서는 IEEE 802.1x 확장 인증 프로토콜(EAP) 기반 상호 인증 방식을 이용해야 하며 예를 들어 PEAP-MSCHAPv2 방식을 통해 키 생성 및 할당이 가능하다.

AES-CCMP 적용 이전 단계인 무선 랜 서비스 초기에서는 64/128비트 유선급 보안 암호화 방식(WEP) 암호화 알고리즘을 주로 사용해 왔으나, 보안 취약성으로 인하여 더이상 안전한 방식으로 인정받지 못하고 있다. 그러므로 공공 무선 랜 서비스의 데이터 암호화 알고리즘으로 이를 사용하는 것은 적절하지 못하다. 유선급 보안 암호화 방식(WEP) 의 취약점을 일부 보완한 임시 키 무결성 프로토콜(TKIP) 알고리즘도 AES-CCMP 이전 단계에 많이 사용되어 왔으며 기존 하드웨어의 수정 없이 소프트웨어적으로 구현이 가능하여 유선급 보안 암호화 방식(WEP)에서 임시 키 무결성 프로토콜(TKIP) 방식으로 많은 전환이 이루어졌다. 임시 키 무결성 프로토콜(TKIP)은 유선급 보안 암호화 방식(WEP)을 이용한 암호화 이전에 별도의 키 생성 과정을 거치게 하여, 유선급 보안 암호화 방식 (WEP)에 적용되는 키가 각 데이터 프레임마다 변경되도록 하였고 메시지 무결성 코드인(MIC:Message Integrity Code)을 프레임에 포함시켰다. 와이파이 얼라이언스(WiFi Alliance)에서 정의한 WPA(Wifi Protected Access)-Enterprise의 표준 암호화 방식 중 하나가 임시 키 무결성 프로토콜(TKIP)이다.

AES-CCMP는 키 관리와 메시지 무결성이 고급 암호 표준(AES)에 의해 만들어진 컴포넌트에 의해 다루어지기 때문에 임시 키 무결성 프로토콜(TKIP)보다 더 강력한 암호화 방법을 제공하므로 현재 가장 안전한 무선 랜 암호화 방식으로 인정받고 있다. 와이파이 얼라이언스(WiFi Alliance)에서 정의하는 WPA2-Enterprise의 암호화 방식이 AES-CCMP 이며, IEEE 802.11의 보안 네트워크 (RSN: Robust Secure Network)을 구성하는 핵심 기술이 바로 AES-CCMP이다.

이처럼 공공 무선 랜 서비스의 무선 데이터는 AES-CCMP 암호화에 의해 보호되는 것이 가장 바람직하지만, 모바일 단말의 종류에 따라 유선급 보안 암호화 방식(WEP) 또는 임시 키 무결성 프로토콜(TKIP)과 같은 예전 암호화 알고리즘만 지원하는 경우가 발생할 수 있다. 이런 점을 고려하여 공공 무선 랜 서비스에서는 개방형 접속 방식을 제공하고 있으므로 무선 데이터 암호화 측면에서는 모두 AES-CCMP 방식으로 전환하는 것이 바람직하다. 암호화 알고리즘의 경우, AES-CCMP 이외에 IEEE 802.11에서 향후 표준으로 채택하는 알고리즘을 적용할 수 있다.

### 사용자 인증

공공 무선 랜 서비스에서 사용자 관리를 위한 등록 및 인증은 필수 요구 사항이 아니다. 그러나, 사용자 인증을 하기로 결정한 경우에는 상호 운용성 측면에서 적절한 기술적 제반 여건을 갖추어야만 유연한 서비스를 제공할 수 있다. 따라서, 본 절에서는 사용자 인증 제공 시 선택 가능한 몇 가지 중요 사항에 대해서 정리하고자 한다.

무선 랜 접속 제어를 위한 표준 사용자 인증 방식은 IEEE 802.1x 확장 가능 인증 프로 토콜(EAP) 기반의 인증 프로토콜이며 공공 무선 랜 서비스의 경우에는 IEEE 802.1x 방 식 중 윈도즈 운영체제 및 각종 스마트폰에서 대부분 지원하고 있는 PEAP-MSCHAPv2 타입을 우선적으로 제공해야 한다. 이 방식은 사용자 인증과 더불어 동적 암호화 키 분 배를 통해 무선 데이터 암호화가 자동으로 지원하는 장점이 있다. IEEE 802.1x 확장 인 증 프로토콜(EAP)은 PEAP-MSCHAPv2뿐만 아니라 MD5, 전송 계층 보안 (TLS:Transport Layer Security), 터널 전송 계층 보안 (TTLS:Tunneled Transport Layer Security), 가입자 식별 모듈(SIM:Subscriber Identity Module), 지네틱 토큰 카드 (GTC:Generic Token Card), 일회용 패스워드 (OTP:One Time Password) 등 인증서 및 아이디 기반 인증과 키 관리를 위한 프레임워크를 제공하고 있어 다양한 방식으로 인증이 가능하지만 가장 보편적으로 사용할 수 있는 사용자 아이디와 비밀번호 방식인PEAP-MSCHAPv2 타입을 기본 인증 방식으로 사용하도록 한 것이다.

사용자가 아이디와 비밀번호를 입력하여 PEAP-MSCHAPv2 방식의 인증을 요청하고 요청이 무선 공유기(AP)에 전달되면 이후에는 무선 공유기(AP)와 인증 서버 간 래디우스 (RADIUS) 통신을 통해 인증 요청이 처리되고 인증 처리 결과가 사용자 단말로 전달된다. 이때, 무선 공유기(AP)는 래디우스(RADIUS) 인증 요청자 역할을 하게 되고 인증 서버는 래디우스(RADIUS) 서버가 되는데 일반적으로 소규모 무선 랜 환경에서는 무선 랜 컨트롤러 스위치가 래디우스(RADIUS) 인증 서버 역할을 하기도 하고, 무선 공유기(AP)와 래 디우스(RADIUS) 서버가 하나의 장비 형태로 구성되기도 한다. 그리고 대규모 사용자 등록을 처리하기 위해서는 별도 래디우스(RADIUS) 서버를 구성하는 것이 바람직하다.

공공 무선 랜 서비스는 IEEE 802.1x PEAP-MSCHAPv2 방식 표준 무선 랜 인증을 기본적으로 제공하면서 웹 기반의 로그인 인증을 함께 제공할 수 있다. 웹을 통한 사용자 인증은 모바일 기기 종류에 제한을 받지 않고 웹브라우저를 통해 인증 요청을 할 수 있으므로 사용자 접근 편의성 측면에서 고려할 수 있는 방법이다. 또한, 모바일 기기의 매체 접근 제어(MAC) 주소를 이용하여 인증할 수도 있다. 이러한 웹 인증 또는 매체 접근 제어(MAC) 인증 등과 같이 IEEE 802.1x 확장 가능 인증 프로토콜(EAP) 기반의 상호 인증 방식이 아닌 경우에는 무선 데이터 암호화를 위한 동적 암호화 키 분배가 불가능하므로 무선 보안을 위해서는 별도 암호화 설정이 필요함에 유의해야 한다.

## 일반 사항

### 채널 설정

무선 공유기(AP)의 사용 주파수 선택은 ‘자동 선택 모드’과 ‘수동 선택 모드’을 모두 지원해야 한다. 이때, 자동 선택 모드는 전파 간섭을 최소화 할 수 있는 채널을 무선 공유기(AP)가 자동으로 선택하는 것을 의미하며 최초 장비 부팅 시 자동 선택함은 물론 운용 도중에도 데이터 에러 발생률 등을 고려하여 자동으로 채널을 변경할 수 있어야 한다.

### 접속자 수 제한

전송 속도 및 응답 속도 등 일정 수준 이상의 무선 인터넷 품질을 제공하기 위해 하나의 무선 공유기(AP)에 접속할 수 있는 사용자의 수를 제한할 수 있다

### 이더넷 전원장치(PoE) 지원

IEEE 802.3af 이더넷 전원 장치(PoE) 또는 IEEE 802.3at 이더넷 전원 장치(PoE)+ 표준을 지원하는 무선 공유기(AP)의 경우 전원 설치가 어려운 장소에 별도의 전원 연결이 필요 없어 설치가 용이하다. 이때, 무선 공유기(AP)에 전원을 공급해 주는 이더넷 전원 장치(PoE) 스위치가 해당 무선 공유기(AP)에 충분한 전력 공급을 할 수 있는지 반드시 확인해야 한다.

### 사용 시간 제한

사용자 또는 접속별 이용 시간을 제한할 수 있다. 예를 들어, 모든 사용자의 이용 시간을 하루 2시간으로 제한하거나, 한 번의 접속으로 이용할 수 있는 시간을 1시간 등으로 제한할 수 있다.

### 대역폭 제어

효율적으로 무선 랜을 활용하기 위해 대역폭 관리를 할 수 있다. 개인별 고정된 최대 대역폭을 제공하거나, 사용자별 균등 분할 방식으로 동적으로 제어할 수도 있다.

### 접속 가능한 지역 정보 제공

공공 무선 랜 서비스 제공 지역에 대한 정보를 웹사이트 등을 통해서 공개해야 한다.

### 무선 랜 서비스 지역 표식 설치

공공 무선 랜 서비스가 제공되는 장소에 알맞은 표식을 설치하여 서비스 제공 여부가 쉽게 인지될 수 있도록 해야 한다.

### 무선 네트워크 설정 가이드라인

공공 무선 랜 접속을 위해 인증 및 데이터 암호화 등 사용자의 단말에서 직접 설정해야 하는 네트워크 구성에 관해 상세한 절차 설명서를 제공해야 한다. 특히, 이용률이 높은 운영체제(OS) 플랫폼 별 사용자 무선 네트워크 설정 매뉴얼을 별도로 제공하는 것이 좋다. 예를 들어, 윈도즈 XP/비스타(Vista)/7, 맥OS X, 아이폰, 안드로이드, 윈도즈 모바일, 심비안 등 컴퓨터 및 스마트폰에 사용되는 운영체제에 따라 상세한 무선 랜 보안설정 방 법을 공공 무선 랜 서비스 운영 주체에서 제공할 수 있다.

# 상호 운용성

무선 네트워크 식별, 무선 랜 접속, 사용자 인증, 데이터 암호화 적용 및 인터넷 연결 허용 등 일련의 공공 무선 랜 서비스가 원활하게 제공되려면 무선 랜 단말과 무선 공유 기(AP) 및 인증 서버간의 상호 운용성이 보장되어야 한다. 이러한 상호 운용성을 확보하려면 반드시 준수해야 할 프로토콜 적합성, 기능 및 성능에 대한 범위와 내용을 사전에 정의하고 이를 검증할 수 있는 시험 방법론도 함께 마련하여야 한다.

공공 무선 랜 서비스의 경우, IEEE 802.11g 또는 IEEE 802.11n의 물리계층(PHY)/매체 접근 제어(MAC) 무선 규격을 준수하고 IEEE 802.1x 확장 가능 인증 프로토콜(EAP) 기 반의 상호 인증 프로토콜 지원 및 AES-CCMP 암호화 지원을 필수 범위로 정하고 각 세 부 기술 요소 사항 및 상호 연동 시나리오별 시험 절차를 정의할 수 있다.

특히, 다양한 일반 기기의 인터넷 접속을 허용해야 하는 공공 무선 랜 시스템의 특성을 감안할 때 네트워크 구성 시 여러 가지 상황의 접속 요구를 유연하게 처리할 수 있도록 상호 운용성 부분을 면밀하게 검토해야 한다.

# 공공 무선 랜 서비스 제공 점검 리스트

<표 8-1> 은 안전하고 편리한 공공 무선 랜 서비스 제공에 필요한 점검 항목이다. 필수항목은 무선 랜의 안전한 운용을 위하여 반드시 필요한 항목이며, 선택 항목은 현실적으로 불가능하거나 고차원의 보안 서비스를 제공하지 않을 경우 불필요한 항목이다.

<표 8-1> 공공 무선 랜 서비스 제공 점검표

|  |  |  |  |
| --- | --- | --- | --- |
| 점검 항목 | 관련항목 | 필수항목 | 선택항목 |
| 공공 무선 랜 망과 지자체․ 공공 기관의 내부망이 분리되어 있는가? | 6.1.1 | V |  |
| 보안 및 개방형 무선 랜을 복합 구성함으로써 이용자가 보안 사용 여부를 선택할 수 있도록 하고 있는가? | 6.1.2 | V |  |
| 개방형 무선 랜 접속 시, 보안 및 개인 정보 유출 위험 사항 등을 알리고 동의를 구하고 있는가? | 6.1.2 | V |  |
| 서비스 세트 식별자(SSID)는 공개로 설정하여 공공 무선 랜 서비스임을 알려주고 있는가? | 6.1.3 | V |  |
| 공공 무선 랜의 서비스 세트 식별자(SSID) 표기 방식 체계를 따르고 있는가? | 6.1.4 | V |  |
| IEEE 802.11i 표준 암호화 알고리즘(예. AES-CCMP)을 지원하는가? | 6.2.1 |  | V |
| IEEE 802.1x 기반 PEAP-MSCHAPv2 인증을 지원하는가? | 6.2.2 | V(\*) |  |
| 매체 접근 제어(MAC)인증을 지원하는가? | 6.2.2 |  | V |
| 웹 인증을 지원하는가? | 6.2.2 |  | V |
| 무선 랜 채널 자동 및 수동 선택 모드를 지원하는가? | 6.3.1 | V |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 점검 항목 | 관련항목 | 필수항목 | 선택항목 |
| 하나의 무선 공유기(AP)에 접속할 수 있는 사용자의 수를 제한할 수 있는가? | 6.3.2 |  | V |
| 무선 공유기(AP)가 이더넷 전원장치(PoE) 또는 PoE+를 지원하는가? | 6.3.3 |  | V |
| 무선 공유기(AP)의 전력 소모량에 적합한 이더넷 전원장치(PoE) 스 위치를 설치하였는가? | 6.3.3 |  | V |
| 사용자의 무선 랜 서비스 사용 시간을 제한할 수 있는가? | 6.3.4 |  | V |
| 무선 랜 사용자들에게 제공되는 대역폭을 제어할 수 있는가? | 6.3.4 |  | V |
| 무선 랜 사용자에게 접속 가능한 지역 정보를 제공하고 있는가? | 6.3.6 |  | V |
| 장소에 공공 무선 랜 서비스 지역임을 알리는 표식을 설치하였는가? | 6.3.7 | V |  |
| 사용자를 위한 네트워크 설정 매뉴얼을 제공하고 있는가? | 6.3.8 | V |  |

(\*) 사용자 인증을 지원하는 경우에는 필수 사항임

**KS X 3100 : 2011**

|  |
| --- |
| **KSKSKS****SKSKS****KSKS****SKS****KS****SKS****KSKS****SKSKS****KSKSKS** |

|  |
| --- |
| **WLAN Service for Public Sectors** |
|  |