한국산학기술학회논문지
Vol. 11, No. 8 pp. 2801-2808, 2010

와이브로 시스템의 정보보호 요구분석

김민선[1*]
[1]협성대학교 유통경영학과

A Study on Applying Information Security Requirement for WiBro System

Min Sun Kim[1*]
[1]**Department of Distribution Management, Hyupsung University**

요 약 유선과 무선으로 경계를 나누어 진화해 온 통신기술은 서비스 간 영역을 넘어 유무선 융합과 모바일 브로드밴드를 전개하면서 향후 제 4 세대(4G) 멀티미디어 시대를 선점하기 위해 총력을 기울이고 있다. 이러한 통신의 발전을 주도하는 중심에 우리나라가 세계 최초로 선보인 와이브로가 자리하고 있다. 와이브로는 차세대 무선통신기술이 결집된 산출물이다. 와이브로 기술은 초고속 인터넷과 이동전화기반 무선인터넷의 장점을 결합하면서, 저렴한 비용으로 모바일 브로드밴드와 컨버전스의 편익과 효용을 제공하는 서비스이기 때문이다. 와이브로는 연관된 산업생태계를 바탕으로 지속적인 발전을 거듭해 왔으며, 이러한 발전은 네트워크 진화를 위한 원동력이 되고 있다. 본 연구에서는 와이브로 시스템의 보안 취약성 및 대책에 대해 제시하였다. 이를 위해 와이브로 서비스에 적합한 보안체계 구축 현황을 기반으로, 안전한 와이브로 서비스 제공을 위해 갖추어야 할 정보보호요구사항을 단말, 기지국, 제어국으로 나누어 분석하였다.

Abstract The technology of WiBro, combining advantages of high speed internet and wireless internet provides the effectiveness and convenience provided by broadband and convergence. WiBro has developed due to supports of the related industries. The advancement of WiBro have created driving force for network advancement. WiBro is a niche market among high speed Internet, wireless LAN, Mobile phone, wireless internet. Through building relationship between market share and the existed telecommunication service, WiBro could improve the convenience of users. The security controls have to be built considering vulnerabilities of WiBro. Based on the study, the architecture of WiBro was suggested through reviewing the vulnerabilities and security controls in the wireless network and wire network. The appropriate security measures to be applied in the environment of WiBro. The outcomes of the study could improve the usage of WiBro.

Key Words : Information security requirement, WiBro, WiBro service

1. 서론

와이브로의 등장은 차세대 무선통신기술이 결집된 산출물이다. 2000년대 이후 차세대 무선통신은 서비스 전 개영역에 따라 혁신적인 진화를 거듭해 왔다. 대표적인 기술로 블루투스, 지그비(ZigBee), 차세대 와이파이(Wi-Fi), 무선 매시네트워크, 고정형 와이맥스, 와이브로(모바일 와이맥스), HSDPA, UWB(울트라 와이드밴드) 등을 들 수 있다. 이러한 차세대 무선통신기술은 전송속도, 이동성, 개인화, 경제성, 망간 융합성, 단말기 통합성을 지향하고 있으며, 이러한 기술 속성은 와이브로를 통해 최적으로 실현되고 있다. 와이브로 기술은 초고속 인터넷과 이동전화기반 무선인터넷의 장점을 결합하면서, 저렴한 비용으로 모바일 브로드밴드와 컨버전스의 편익과 효용을 제공하는 서비스이기 때문이다. 와이브로는 연관된 산업생태계를 바탕으로 지속적인 발전을 거듭해 왔

*교신저자 : 김민선(sunnyminkim@hanmail.net)
접수일 10년 06월 19일 수정일 10년 08월 02일 게재확정일 10년 08월 10일

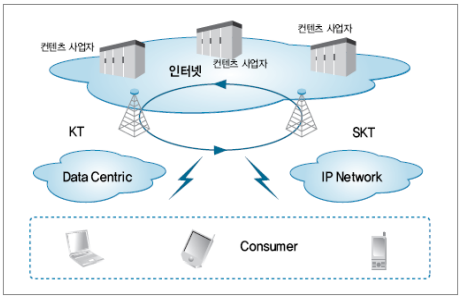
으며, 이러한 발전은 네트워크 진화를 위한 원동력이 되고 있다.

와이브로는 사용자 측면에서 고속의 멀티미디어 서비스, 저렴한 요금, 이동성을 지원할 수 있는 무선인터넷 서비스를 지향하며 등장하였으며, 통신사업자 측면에서는 초고속인터넷 시장포화, 이동통신 시장포화, 신규사업 모델발굴을 위하여 등장하였다. 또한 정부정책적 측면에서는 IT 산업육성, 새로운 수출모델, 정보통신 강국건설을 목표로 등장하였다고 할 수 있다. 그러나 와이브로 서비스의 본격적인 활성화를 위해서는 향후 차세대 네트워크망 및 커버리지 확대가 시급한 실정이다.

2. 관련 연구

2.1 와이브로 개요

와이브로(WiBro)는 Wireless Broadband의 줄임말로, 무선 광대역 인터넷, 무선 인터넷 등의 의미를 내포하고 있으며, 휴대인터넷 기술을 대변하는 용어이다. 와이브로 서비스는 사용자가 이동하는 상황에서 2.3GHz 대역의 주파수를 이용하여 휴대단말기를 통해 초고속 인터넷을 사용할 수 있다는 특징을 가진다[9].



[그림 1] 와이브로 서비스 구조

와이브로는 이동전화단말기처럼 정지하거나 이동 중일 때 언제 어디서나 인터넷을 사용할 수 있다는 것이 무선 랜이나 초고속인터넷, 모바일 인터넷 서비스와 다른 점이다. 무선 랜은 일반적으로 최대 11Mbps의 전송속도를 제공할 수 있는 서비스지만 전송거리가 짧고 한 지역의 서비스 지역에서 다른 서비스 지역으로 이동할 때 접속을 끊고 다시 연결해야 하는 이동성의 제약을 가지고 있다. 이동통신에서의 인터넷 서비스는 넓은 서비스 지역과 이동성의 제약이 없다는 장점이 있지만, 무선 랜보다 낮은 전송속도이면서 이용요금은 비싸다는 문제점을 가지고 있다. 그러나 와이브로는 무선 랜과 같이 이동성의 제약은 물론 모바일 인터넷 서비스처럼 낮은 전송속도 및 비싼 이용요금의 단점을 보완한 것이라 할 수 있다.

와이브로는 한국정보통신기술협회(TTA), 한국전자통신연구원(ETRI), 삼성전자가 주축이 되어 기술 표준이 확정되고, 관련 장비 개발이 추진되었으며, 현재 국내 사업자로 KT와 SK텔레콤이 선정되어 2006년 6월부터 일부 지역에서 세계 최초로 상용화 서비스가 시작되었다.

[표 1] 와이브로와 유사서비스 비교*

구 분	와이브로	초고속 인터넷	무선랜	무선 인터넷 (모바일)
이용 지역	옥내외 (Hot Zone)	옥내	옥내 (Hot Spot)	옥내외 (전국망)
전송 속도	고속	초고속	초고속	중저속
이동성	평상 이동성	없 음	정지 또는 준정지	고속 이동
콘텐츠	유무선 콘텐츠	유선 콘텐츠	유무선 콘텐츠	무선 콘텐츠
요금	상대적 저렴	상대적 저렴	저렴	높음
단말 형태	PDA, 노트북, 핸드폰	데스크탑, 노트북	PDA, 노트북	핸드폰, PDA
셀반경	약 1km	없음	약 100m	1km ~ 8km

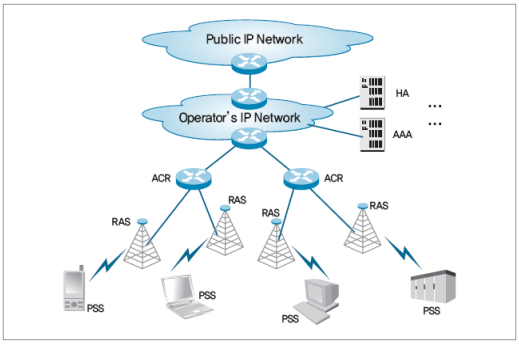
*[2]재인용

[표 2] 와이브로 기술의 특징

구분	특징
기반기술 및 전개방향	-유선 백본망과 무선 가입자망의 결합 -고속데이터 전송에 효율적인 IP기반 전송 기술채택 -무선접속 구간에 OFDM, MIMO, 스마트 안테나 채용을 통한 효율성 제고
대역폭	10MHz
전송속도	하향 최대: 50Mbps
이동속도	120km/h 내외
QoS	보장 어려움
서비스	데이터 중심의 서비스
음성제공	VoIP, 뷰얼모드 단말기를 통해 제공
데이터 서비스	-중품질 대용량 멀티미디어 -인터넷 접속, MMS, M-Commerce -주문형 서비스, 게임
단말기 유형	-핸드폰/스마트폰, PDA, PMP -핸드헬드PC, 노트북
상용화 시기	2006년 6월

2.2 와이브로 기술

와이브로는 음성 통신서비스를 제공하는 이동통신망과 달리 데이터 서비스 제공에 맞게 설계되어 있어, 인터넷 서비스 제공에 적합한 All IP 망구조를 택하고 있다. 와이브로 망구성은 크게 4가지 요소로 구분되는데, 서비스를 이용하는 사용자 단말기(PSS : Portable Subscriber Station), 무선으로 정보를 전달하는 기지국(RAS : Radio Access Station), 이동성/과금/세션 등을 관리하는 제어국(ACR : Access Control Router) 및 각종 부가서비스를 제공하는 서버들로 구성된다. 또한 와이브로 표준기술은 단말, 기지국간 물리계층, 매체접근제어계층을 정의하고 있으며, 매체접근제어계층에는 보안규격이 포함되어 있다.



[그림 2] 와이브로망 구성도

3. 와이브로 정보보호 요구사항

와이브로 서비스의 적용 필요성 분석에 따라 기존의 와이브로 서비스 보안관리체계를 발전시켜 안정성 및 신뢰성을 확보할 수 있는 환경이 요구된다. 본 연구에서는 정보보호관리 절차와 과정을 체계적으로 관리, 운영하기 위한 적용방안을 수립하고, 와이브로 서비스에 적합한 보안체계 구축현황을 기반으로 안전한 와이브로 서비스 제공을 위해 갖추어야 할 정보보호요구사항을 단말, 기지국, 제어국으로 나누어 고찰하였다.

가. 단말에서의 정보보호 요구사항

(1) 사용자가 단말을 분실할 경우를 대비하여 이를 신고할 수 있는 신고센터와 분실된 단말을 이용할 수 없도록 하는 시스템이 필요하다.

(2) EAP 인증시스템(EAP-AKA) 또는 공개키 기반 인증(무선 PKI) 등과 같이 단말과 기지국간 상호인증기술이 적용되어야 한다.

(3) 단말과 기지국에서 무선 주파수를 이용하여 전송되는 데이터가 노출될 수 있다. 데이터 암호화방식으로 128bit AES 기반 암호방식 등 강력한 방식을 적용하여야 한다.

(4) 단말과 기지국에서 전송되는 데이터의 무결성 보장을 위해 CRC와 CheckSum 등과 데이터 오류 검사 기능과 데이터에 대한 해쉬값을 암호화하여 전송하는 등과 같은 위변조방지 기법이 필요하다.

(5) 단말과 기지국과의 통신을 위해 사용하는 무선 주파수 대역을 지속적으로 감시하고, 변동사항을 주시할 수 있는 기술 기법을 기지국에 탑재하여 이에 대한 위협을 조기에 탐지하거나 단말 및 관제센터에 통보할 수 있는 시스템의 구축이 필요하다.

(6) 기지국 및 단말에서 지속적으로 연결을 요청하는 단말 및 기지국을 식별할 수 있는 기술이 필요하다. 또한 기지국 및 단말에서 지속적인 연결 메시지를 거부하거나 차단할 수 있는 기술이 있어야 한다.

(7) 단말이 기지국에 연결을 요청하는 과정에서 전송되는 메시지의 위변조 및 메시지를 전송한 주체에 대한 검증과정이 필요하다.

(8) 단말이 기지국과 인증을 수행하는 과정에서 인증결과를 보내는 메시지에 대해 위변조 및 전송주체에 대한 검증과정이 필요하다.

(9) 단말(기지국)이 기지국(단말)에 연결을 종료하기 위해 전송하는 메시지에 대한 위변조 및 메시지 전송 주체에 대한 검증과정이 필요하다.

(10) 단말이 기지국에 재인증을 요청하는 메시지에 대한 위변조 및 메시지 전송 주체에 대한 검증과정이 필요하다.

나. 기지국에서의 정보보호 요구사항

(1) 기지국에 접근하여 사용하는 내부자에 대한 관리 감독이 필요하다. 기지국을 사용하는 경우 id/password와 같은 인증과정을 거친 후 사용하도록 한다.

(2) 외부에서 네트워크를 통해 접근하여 기지국을 이용할 수 없도록 하거나, 기지국에 접근할 수 있는 IP 주소 및 사용자를 제한하여야 한다.

(3) 기지국에 접속하려는 단말은 단말 인증뿐 아니라 EAP 인증시스템(EAP-AKA) 또는 공개키 기반 인증(무선 PKI) 등과 같은 인증과정이 필요하다.

(4) 기지국에 설정된 기본적인 id/password를 삭제하거나, 기본적인 id/password를 통해 기지국의 중요 정보에 접근하지 못하도록 접근제한을 둔다. 또한 각 사용자별로 접근할 수 있는 데이터 항목을 구분하

여 설정할 수 있도록 하는 기술을 적용한다.

(5) 기지국과 장치 및 서버간 전송되는 데이터를 생성한 주체를 검증하는 과정이 필요하다. 또한 전송된 데이터가 변조되었는지를 판단할 수 있는 검증과정이 있어야 한다.

(6) 기지국과 장치 및 서버와 전송되는 데이터에 대해 암호화 기능을 적용하여, 데이터가 유출되지 않도록 하여야 한다.

(7) 기지국(사용자 단말)에서 사용자 단말(기지국)과의 접속을 종료하는 경우, 접속 종료를 요청하는 메시지 및 메시지를 보낸 주체에 대한 검증과정이 필요하다.

(8) 기지국은 일정시간이 지나면 재인증을 요청한다. 일정시간이 지나지 않은 상황에서 공격자가 정상적인 사용자 단말로 위장하여 재인증 메시지를 전송할 때, 전송되는 메시지를 보낸 주체 및 메시지 변조여부를 검증해야 한다.

(9) 사용자 단말이 다른 지역으로 이동하는 경우, 기존 기지국과의 연결을 종료하기 위해 존 통화회선을 끊고 새로운 기지국으로 연결하는 handoff 메시지를 전송한다. 기지국에 전송되는 메시지를 보낸 주체 및 메시지 변조 여부를 검증해야 한다.

다. 제어국에서의 정보보호 요구사항

(1) 제어국에 접근하여 사용하는 내부자에 대한 관리 감독이 필요하다. 제어국을 사용하는 경우 id/password와 같은 인증과정이 필요하다.

(2) 외부에서 네트워크를 통해 제어국을 이용할 수 없도록 하거나, 제어국에 접근할 수 있는 IP주소 및 사용자를 제한해야 한다.

(3) 제어국의 서비스를 이용하려는 서버 및 장치는 항상 공개키 기반 인증(유선 PKI) 등과 같은 인증과정을 거치도록 한다.

(4) 제어국으로 장치 및 서버간 데이터를 전송하는 경우 데이터를 생성한 주체에 대한 인증 및 데이터 위변조 여부를 검증할 수 있어야한다.

(5) 기지국과 장치 및 서버와 전송되는 데이터에 대해 암호화 기능을 적용하여 중요 정보가 유출되지 않도록 해야 한다.

(6) 제어국에 속한 기지국 및 사용자 단말에 대용량의 데이터를 전송하는 경우 제어국에 미리 전송할 데이터의 양을 통보하는 메커니즘을 도입하여 제어국의 용량에 맞게 처리할 수 있도록 해야 한다.

4. 와이브로의 보안체계 구축현황 및 보안대책

4.1 유·무선 환경에서 와이브로의 보안위협 및 보안대책

본 연구에서는 u-IT 전략에 따른 와이브로 서비스의 활성화와 와이브로 서비스 제공에 대한 위협요소들과 이를 체계적으로 관리할 수 있는 정보보호 관리체계 및 보안대책을 분석하고자 유·무선 환경에서 와이브로의 보안위협 및 보안대책을 분석하였다.

[표 3] 와이브로 무선구간에서의 보안위협 및 보안대책

구 분	보안 이슈	보안 대책
전 파 간 섭	-전파교란, 불법주파수 임의사용	-중앙전파관리연구소에 전파간섭 사실 신고 및 대응
불 법 복 제단말	-와이브로 단말 불법복제에 의한 망 접속 및 서비스 사용	-복제불가능한 스마트 카드를 활용한 인증방식 도입
망접근 통제	-허가받지 않은 사용자에 의한 와이브로망 불법접근 및 서비스 사용	-단말/기지국간 양방향 인증 기능을 제공하는 PKMv2기반 EAP-AKA 인증기능 사용
통 신 내 용도청	-사용자 통신내용 도청에 의한 계정, 패스워드 및 금융정보 유출 -802.16e 안정성 여부	-단말/기지국간 통신내용에 대해 암호화기능 및 인증, 안전키 교환 사용(EAP-AK에서 상호인증 메커니즘 제공)
통 신 내 용 위변조	-정상 사용자 통신내용 위/변조에 의한 피해발생	-단말/기지국간 통시내용에 대하 무결성 검사 기능 사용
서비스 거부 공격	-IP 자원의 고갈유도를 통한 서비스 거부공격발생 -RES-CMD 메시지 등에 의한 서비스 거부공격 발생	-트래픽 및 IP 사용현황에 대한 모니터링 및 대응 -MAC 스케줄러를 통한 과다한 트래픽 제어 -개인별 트래픽 모니터링 및 Rate Limit에 의한 트래픽 차단

[표 4] 와이브로 유선구간에서의 보안위협 및 보안대책

구 분	보안 이슈	보안 대책
시스템 접속제한	-망구성 주요장비인 RAS, ACR등에 대해 비인가자의 시스템 접속에 우발적, 의도적 피해발생	-주요장비인 ACR, RAS 등에 대해 사전승인부서의 특정 IP, 사용자에 대해서만 허용 -EMS 등을 도입하여 시스템 접근에 대한 체계적인 관리

주요 시스템에 대한 보안위협	-운영체제 및 데이터베이스 등에 대한 보안취약성을 이용한 공격발생	-운영체제 및 데이터베이스 등에 대한 보안패치 및 최신버전으로 업그레이드 -임베디드운영체제 사용
주요 시스템에 대한 불필요한 요소제거	-사용하지 않는 telnet, ftp등의 서비스와 포트 등을 이용한 불법접속 및 해킹발생	-시스템에 불필요한 telnet, ftp등의 서비스 제거 -사용하지 않는 포트차단 및 사용자 계정 삭제
비정상 트래픽 모니터링 및 차단	- 비정상트래픽 Flooding 공격	-ESM의 보안관제 시스템 등을 사용하여 사고발생 및 즉각대응

5. 사업자를 위한 보안점검사항

5.1 운영서버 및 네트워크 장비에 대한 보안 점검사항

서버관리자는 운영 중인 서버가 해킹, 웜·바이러스 공격 등의 피해를 입지 않도록 주의해야 한다. 표 5 및 표 6에서는 운영서버의 공통 보안점검사항을 제시하였다.

[표 5] 운영서버에 대한 보안점검사항

구분	주요 내용
공통	서버설정 화일변경, 네트워크 주소변경 등 주요 변화에 따른 불필요한 서비스 추가여부
	사용자 계정에 대한 필요이상의 권한부여 여부
	신규 웜/바이러스에 대한 정보 파악여부
	발표된 웜/바이러스등의 정보와 관련된 운영서버 확인 및 패치적용여부
	서버운영에 불필요한 계정의 존재여부
	불필요한 네트워크 서비스 사용여부
	서버 S/W에 대한 보안패치 적용여부
	시스템 로그 점검 및 불법접근 가능성에 대한 점검여부
	시스템에 대한 로그기능 사용여부
	백업된 데이터에 대한 적절한 관리여부
	주기적으로 중요시스템 및 데이터베이스 백업여부

[표 6] 네트워크 장비에 대한 보안점검사항

구분	주요 내용
공통	네트워크 취약점 스캐너등 사용여부
	필요에 따라 이중화 및 백업체계 마련여부
	네트워크 장비(라우터, 스위치등)에 대한 로그기능 설정 및 모니터링 여부
	네트워크 장비에 대한 보안패치 적용여부
	기본으로 제공하는 서비스 중 사용하지 않는 서비스 중지 여부(예: 웹을 이용한 원격관리 서비스)
	네트워크 장비에 대한 사용계정 관리여부
라우터	네트워크 장비의 OS 최신버전 설치여부
	네트워크 장비로의 접근 통제콘솔/AUX/VTY 포트 패스워드 설정여부 enable 패스워드 설정여부 및 접속가능한 사용자/시스템에 대한 ACL 설정여부
	불필요한 프로토콜/서비스 제거여부 ICMP관련 서비스, Source Routing, Small Services
	IP 주소 위조 방지 수단 사용여부 사설 IP 주소 차단 uRPF 사용
	라우팅 프로토콜 인증 설정 여부
	ACL로 차단된 트래픽에 대한 로깅관리 여부
	ACL등 접근 통제정책 적용여부
스위치	가상 LAN(VLAN) 구성하여 운영여부
	네트워크 장비의 OS 최신버전 설치여부
	Port Security 기능 설정여부
	ARP Inspection 기능 설정여부

5.2 보안시스템 점검사항

정보보호담당자는 와이브로 시스템 보호를 위해 설치한 보안 장비가 정확하게 설정되어 있는지 주기적으로 확인하여 침해사고를 예방하여야 한다. 표 7은 보안시스템에 대한 점검사항을 나타낸다.

[표 7] 보안시스템에 대한 보안점검사항

구 분	주요 내용
보안시스템	침입차단/탐지시스템의 로그를 주기적으로 모니터링 여부
	침입탐지시스템 탐지규칙을 최신으로 업데이트 여부
	관리시스템으로부터 들어오는 트래픽의 허용 설정여부
	관리시스템외의 시스템에서 들어오는 트래픽은 거부로 설정여부

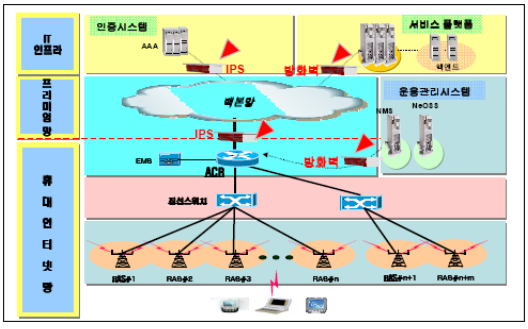
	내부 DNS서버로 들어오는 모든 외부 트래픽은 거부로 설정여부
	외부 DNS로 나가는 트래픽은 DNS(port 53 TCP/UDP)만 허용여부
	각 서비스 포트는 반드시 필요한 경우만 허용 설정여부
	바이러스 월의 필터링규칙을 최신버전으로 업데이트 여부
	내외부에서 보안도구를 사용하여 침입차단시스템 설정여부

5.3 보안시스템 구성

와이브로 서비스의 네트워크 서버군 및 액세스망을 위한 전체적인 보안시스템 구성을 종합하면 그림 5와 같다.

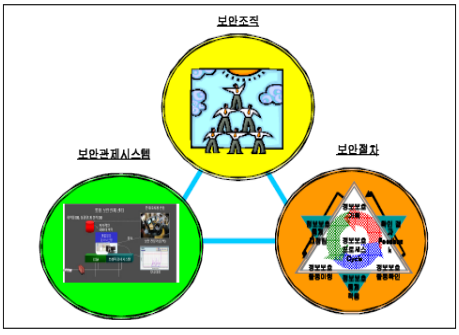
5.4 관리체계 구성

보안요구사항은 와이브로 서비스의 안정성 및 정보의 신뢰성을 확보하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 관리하고 운영하기 위한 종합적인 체계라고 할 수 있다.



[그림 5] 네트워크 서비스 및 액세스망 보안시스템 구축

기존 와이브로 서비스의 보안관리체계는 보안조직, 보안절차, 보안관제시스템으로, 그 구성은 그림 3과 같다.



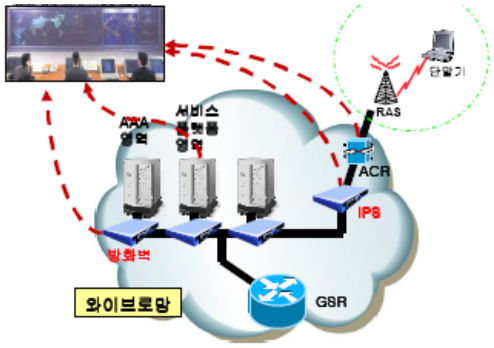
[그림 3] 기존의 와이브로 보안관리체계

와이브로 서비스 보안관제시스템은 보안 이벤트 발생 및 트래픽 소통상황, 시스템 자원 사용 탐지 및 모니터링 하여 종합적으로 분석, 대응할 수 있는 통합보안 관리리스템의 도입이 필요하다. 와이브로 서비스의 보안관제 대상과 관련 수집정보는 표 8과 같다.

[표 8] 보안관제 대상 및 수집정보

관제 대상	수집 정보
방화벽	보안 이벤트 및 리소스 정보
IPS	보안 이벤트 및 리소스 정보
서버	EMA, AAA, 서비스플랫폼 등 주요서버의 보안로그
네트워크장비	네트워크 트래픽 정보
기타	감염 및 리소스 정보 패치 작업 및 리소스 정보

그림 4는 와이브로 서비스의 통합보안관리체계이다.



[그림 4] 와이브로 통합 보안관리체계

5.5 보안체계 관련 법/제도

와이브로 서비스의 관련 법/제도적 이슈 사항들을 '사용자 이용약관'에 반영하여 종합적인 보안체계를 구축하여야 한다. 보안체계 구축을 위한 법/제도적 이슈 사항들은 표 9와 같다.

[표 9] 보안체계 구축을 위한 법/제도적 이슈

구 분	적용 방안	내 용
개인정보보호	개인정보보호 정책수립	와이브로서비스 개인정보보호 정책 수립 개인정보보호 책임자 및 담당자 지정
	이용약관 반영	개인정보 수집 동의, 이용, 보존 등 관련사항 이용약관 반영

시 스 템 침해	이용약관 반영	장애초래, 다량정보전송, 바이러스 등 악성코드 유포, 불법광고, 스팸메일, 시스템 침투 등 불법 사용시 서비스 제한, 계약해지, 손해 배상 등 사항 약관 반영
위 치 정 보보호		타인의 불법위치 정보수집, 수집정보 누설시 서비스 제한 또는 계약해지 사항의 이용약관 반영
도청		타인의 통신내역 도청, 도청 내역 유출시 서비스 제한 또는 계약해지 사항의 약관 반영
기타		와이브로 서비스 관련 S/W 또는 H/W의 변조, 복제 등으로 서비스에 지장을 주거나, 타인에 피해를 입힌 경우 서비스 제한 또는 계약해지 등 약관 반영

6. 결론

본 연구는 와이브로 프로토콜의 적용기술 연구를 위해 와이브로의 개요, 와이브로 표준화 및 기술동향을 분석하고 와이브로 시스템 구성과 와이브로의 적용 방안을 제시하였다.

와이브로(WiBro)는 무선 광대역 인터넷, 무선 인터넷 등의 의미를 내포하고 있으며, 휴대인터넷 기술을 대변하는 용어이다. 와이브로 서비스는 사용자가 이동하는 상황에서 2.3GHz 대역의 주파수를 이용하여 휴대단말기를 통해 초고속 인터넷을 사용할 수 있다는 특징을 가진다. 와이브로는 시속 120km의 이동성을 가지며, 실내외에서 끊김없이 초고속 무선 인터넷 서비스를 제공할 수 있도록 설계되어 있다. 와이브로 서비스는 이동전화가 제공하는 고품질 음성 서비스의 데이터 통신 영역을 보완하는 고속의 대용량 데이터 서비스이다. 기술상으로는 VoIP 기술을 단말기에 탑재하여 이동전화를 대체할 수도 있다.

와이브로는 국내에서는 TTA PG302에서 표준화 작업을 진행하고 있다. 와이브로는 특히 OFDMA, MIMO, 스마트 안테나 기술을 통해 제 4세대 멀티미디어 통신의 핵심기술로 다른 서비스에 비해 빠르게 구현하고 있어, 시장선점과 주도권싸움에서 가장 유리한 지위를 확보하고 있다고 평가된다. 특히 와이브로 단말의 상호운용성을 확보하기 위해 무선 접속 실무반 산하에 IOT/CT(Inter-Operability Test/Conformance Test) Task Force팀을 구성하여 표준화를 추진하였다.

국외에서는 IEEE 802.16에서 표준화 작업을 진행중인데, 과거 IEEE 802.11 규격 완성으로 무선 네트워크인 Wi-Fi가 대량 보급된 것처럼 IEEE 802.16e의 국제표준확정이 와이브로 및 와이맥스 보급에 긍정적인 역할을 할 것으로 전망되며, 향후 와이브로의 세계시장 규모를 고려하면 국내 IT 산업발전에 기여할 수 있을 것으로 예상된다.

와이브로는 음성통신 서비스를 제공하는 이동통신망과 달리 데이터 서비스 제공에 맞게 설계되어 있어, 인터넷 서비스 제공에 적합한 All IP 망 구조를 택하고 있다. 특히 와이브로의 보안기술은 단말, 기지국간 물리계층, 매체접근제어계층을 정의하고 있으며, 매체접근제어계층에는 보안규격이 포함되어 있다.

본 연구에서는 u-IT 서비스의 주요한 서비스 중 하나인 와이브로에 대한 적용방안을 개발하고 와이브로 서비스의 안정성 확보를 위한 방안을 수립하였다. 정보보호관리 절차와 과정을 체계적으로 관리, 운영하기 위한 적용방안을 수립하고 와이브로 서비스에 적합한 보안체계 구축 현황을 기반으로, 안전한 와이브로 서비스 제공을 위해 갖추어야 할 정보보호 요구사항을 단말, 기지국, 제어국으로 나누어 기술하였다. 본 연구에서 제시한 와이브로 시스템의 보안위협과 보안대책에 관련한 분석은 실제 와이브로 활용에 있어 정보보호와 관련한 이슈에 도움이 되리라 본다.

참고문헌

[1] 김종기, 김기윤, 이경석, 김정덕, "정보시스템 재해에 대비한 업무 지속성 관리,“ 정보보호학회지, Vol. 11, No. 1, pp. 9-19, 2001.

[2] 알엔디비즈 편집부, “와이브로 시장동향 리포트,” (주) 알엔디비즈, p. 13,, 2006.

[3] Anderson R., “Why Information Security is Hard - An Economic Perspective," *17th Annual Computer Security Applications Conference,* Dec. 2001.

[4] Brink, D., *A Guide to Determining Return on Investment for e-security,* RSA Security Inc. 2001.

[5] Cavusoglu, H., Mishra, B. and Raghunathan, S., “A Model for Evaluating IT Security Investments”, *Communications of the ACM,* Vol. 47, No. 7, pp. 87-92, July 2004.

[6] Eloff, M. and Solms, S.H., “Information. Security Management, An Hierachical Framework for Various Approaches," *Computers and Security,* Vol. 19, No. 3, pp. 243-256, 2000.

[7] Fung, A.R.W., Farn K.J., and Lin, A.C., "A Study on the Certification of the Information Security Management Systems," *Computer Standards and Interfaces,* Vol. 25, No. 5, pp. 447-461, 2003.
[8] Gentile, F., Giuri, L., Guida, F., Montolivo, E., and Volpe, M., "Security Evaluation in Information Technology Standards," *Computers and Security,* Vol. 13, No. 8, pp. 647-650, 1994.
[9] Lee, S., Park, S., Cho, C., Lee, H. and Ryu, S., "The Wireless Broadband(WiBro) System for Broadband Wireless Internet Services," *IEEE Communications Magazine,* Vol. 44, No. 7, pp. 106-112, 2006.

김 민 선(Min Sun Kim) **[정회원]**

- 1990년 2월 : 이화여자대학교 대학원 경영학과 (경영학석사)
- 2006년 2월 : 이화여자대학교 대학원 경영학과 (경영학박사)
- 1995년 9월 ~ 2006년 2월 : 이화여자대학교 지식정보화전략연구센터 책임연구원
- 2009년 9월 ~ 현재 : 협성대학교 유통경영학과 교수

<관심분야>
E-business, IT 서비스관리, IT 거버넌스, EA/ITA, 유비쿼터스(Ubiquitous), 정보보호 등