최종연구보고서	KISA-WP-2011-0036

인터넷전화(VoIP) 사업자 정보보호 모델 연구

수탁기관: 한국정보보호학회

2011. 12.

KISA 한국인터넷진흥원
Korea Internet & Security Agency

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “인터넷전화(VoIP) 사업자 정보보호 모델 연구”의 최종 연구보고서로 제출합니다.

2011년 12월 15일

수탁기관 : 한국정보보호학회 회장 염 흥 열 (인)
연구책임자 : 충 남 대 학 교 교수 류 재 철 (인)
참여연구원 : 연 구 원 민 승 욱 (충남대학교 컴퓨터공학과)
연 구 원 이 희 경 (충남대학교 컴퓨터공학과)
연 구 원 유 성 민 (충남대학교 컴퓨터공학과)
연 구 원 조 형 진 (충남대학교 컴퓨터공학과)
연 구 원 오 진 석 (충남대학교 컴퓨터공학과)

“이 페이지는 공백임”

요 약 문

1. 제목

인터넷전화(VoIP) 사업자 정보보호 모델 연구

2. 연구개발의 목적 및 중요성

인터넷전화(VoIP, Voice over Internet Protocol) 기술은 음성정보를 비롯한 데이터, 비디오 정보 등 다양한 정보를 패킷 형태로 변환하여 전송하는 기술을 말한다.

VoIP는 이동성 정도에 따라 크게 유선 VoIP와 모바일(무선) VoIP로 분류할 수 있는데, 이 중에서도 mVoIP는 스마트폰의 확산과 함께 무선 인터넷망을 이용해 사용자들에게 어디서나 저렴한 통신 서비스를 제공할 수 있는 장점으로 빠르게 확산되고 있다.

하지만 VoIP의 경우 인터넷을 이용하기 때문에 인터넷에서 발생 가능한 여러 보안위협들이 그대로 적용되며, 실제로도 이를 이용한 몇몇 보안사건이 발생하였다. mVoIP 역시 통화와 관련된 기반 기술은 기존 유선 VoIP 기술을 사용하기 때문에 이러한 보안위협들에 노출되어 있다. 뿐만 아니라 mVoIP 어플리케이션이 탑재되는 스마트폰은 이동성이 높은 반면 분실 위험이 크기 때문에 mVoIP를 이용하기 위해 스마트폰에 저장되는 ID, 패스워드, 통화기록 등 중요정보의 분실위협 또한 커진다. mVoIP의 또 하나의 장점은 무선랜(Wi-Fi) 기술을 이용하여 거의 무료로 통화가 가

능하다는 점이지만, 이 역시 무선랜의 보안 취약성을 이용한 공격이 용이함을 의미하기도 한다. 무선랜 보안 취약성은 이미 여러 차례 지적된 바 있으며, 특히 도청 등에 이용되어 사용자에게 피해를 입히는 여러 사례가 보고된 바 있다.

이와 같이 mVoIP에 대한 보안위협이 심각함에도 불구하고 mVoIP 보안 대응은 매우 미흡한 실정이다. 국내 유선 VoIP의 경우, 한국인터넷진흥원을 통해 이미 VoIP 보안권고해설서, VoIP 침해사고대응해설서 등이 배포되어 VoIP 사업자 및 사용자의 보안인식을 확고히 하고 보안사고를 줄이는데 기여하고 있다. 외국의 경우에도 NIST에서는 “Security Consideration for Voice over IP Systems"와 같은 보고서를 통해서 VoIP 정보보호에 대한 대책을 제시하고 있다. 하지만 mVoIP에 대해서는 국내외적으로 이와 같은 보안 대책이 전무하다시피 한 실정이다. 특히 중소규모의 개발사나 개인 개발자가 공급하는 경우가 많은 mVoIP에서 보안위협에 대한 서비스의 안전성을 검증하는데 현실적으로 많은 어려움이 존재하기도 한다. 따라서 mVoIP 서비스 이용자를 보호하고 신뢰할 수 있는 mVoIP 서비스 이용 환경을 조성하기 위한 연구가 필요하다.

3. 연구의 내용 및 범위

본 연구의 목표는 이미 보고되거나 발생 가능한 mVoIP 보안위협으로부터 서비스 이용자를 보호하고 안전하고 신뢰할 수 있는 mVoIP 서비스 이용 환경을 조성하기 위해서 필요한 기술적・관리적 사항을 설명하는데 있다.

이를 위해 우선적으로 1) mVoIP의 기술적 개요와 기술 및 시장동향을 분석하고, 2) mVoIP의 보안위협 및 정보보호를 위한 요구사항을 식별한다. 3) 그리고 mVoIP의 보안위협에 대응하기 위한 정보보호 대응방안을 연구하고, 4) VoIP 사업자를 위한 보안모델을 제시한다.

추가적으로 정보보호체계와 관련한 표준화 동향을 살펴보고, 기존 VoIP 정보보호 점검항목을 수록하여 mVoIP와의 비교를 돕는다.

4. 연구결과

○ mVoIP 기술 및 시장동향 분석

- mVoIP를 정의하고 mVoIP 서비스인 skype, Truphone, Fring, Jajah, i2 Telecom, 마이피플, 올리브폰 등에 대해 분석하였다.

○ mVoIP 보안위협 및 정보보호요구사항 식별

- 음성 및 메시지 도청, 서비스 거부 공격, 중요정보유출 및 재사용 등 다양한 보안위협을 식별하고, 이와 같은 보안위협을 최소화하기 위한 mVoIP 정보보호 요구사항을 도출하였다.

○ mVoIP 정보보호 대응방안 제시

- mVoIP 정보보호 요구사항을 근거로 mVoIP 소프트웨어 개발사가 실행할 수 있는 정보보호대책 및 정보보호 점검항목을 제시하였다.

○ VoIP 사업자 보안모델 제시

- 보안위협에 대한 사업자별 보호대책을 제시하고 기업 규모 및 망 구성에 따른 VoIP 서비스 보안모델을 제시하였다.

5. 활용에 대한 건의

본 연구에서는 mVoIP 이용자를 보호하고 특히 국내 mVoIP의 안전성을 향상시키기 위해서 필요한 mVoIP 정보보호 대책을 제시하였다. 본 연구에서 제시한 mVoIP 정보보호 대책은 이용 주체에 따라 각각 다음과 같이 활용될 수 있다.

○ 이용자

- 안전한 mVoIP 어플리케이션을 선택하는데 참고할 수 있다.
- mVoIP 어플리케이션을 안전하게 이용하기 위해서 필요한 소프트웨어 설정, 무선 네트워크(Wi-Fi) 설정, 스마트폰 설정 등에 활용할 수 있다.

○ mVoIP 어플리케이션 개발 업체

- 안전한 mVoIP 어플리케이션을 개발하는데 활용할 수 있다.
- 안전한 mVoIP 어플리케이션 개발을 통해 사용자의 신뢰를 얻을 수 있다.
- 국산 mVoIP 솔루션의 경쟁력을 강화하는데 활용할 수 있다.

○ 정부

- mVoIP 운영정책을 수립하는데 활용할 수 있다.
- 전체 스마트폰 이용환경의 보안정책을 수립하는데 활용할 수 있다.

6. 기대효과

스마트 환경 시대의 도래와 함께 mVoIP의 이용은 더욱 확대될 것으로 기대되고 있다. mVoIP의 활성화를 위해서는 서비스 초기 단계인 지금부터 안전성 확보를 위한 노력을 기울여야 한다. 이를 위해 본 연구에서 제시한 mVoIP 정보보호 대책을 기반으로 한 다양한 mVoIP 정보보호 연구 및 개발 활동이 이루어질 것으로 기대하며, 이를 통해서 국내 mVoIP 산업의 국제 경쟁력 확보를 이뤄낼 수 있을 것으로 본다.

목 차

그 림 목 차

표 목 차

“이 페이지는 공백임”

제 1 장 서 론

○ 스마트폰의 보급 확대와 함께 킬러 앱 가운데 하나인 모바일 인터넷전화(mVoIP) 서비스에 대해서 도청을 비롯한 보안문제 해결을 위해 mVoIP 정보보호 대책 수립의 필요성이 매우 높음

○ 본 보고서의 목표는 안전한 mVoIP 환경 구축을 위해서 mVoIP 보안 위협을 분석 및 이를 기반으로 한 mVoIP 정보보호 대책 제시임

○ *키워드: mVoIP(모바일 인터넷전화), 스마트폰, 정보보호*

제 1 절 배경 및 필요성

인터넷전화(VoIP, Voice over Internet Protocol) 기술은 기존 전화가 회선 교환기술을 이용하여 음성 정보를 전달하던 것과는 다르게 음성 정보를 패킷 형태로 변환하여 IP(Internet Protocol) 방식으로 전송하는 기술을 말한다. 그러나 최근의 VoIP는 단순히 음성 정보를 패킷으로 변환하여 전송하는 기술 자체로 간주하기 보다는 IP 기반의 인터넷 환경에서 음성, 데이터, 그리고 비디오 정보 등 다양한 정보의 통합 전송을 가능하게 하는 기술을 포괄적으로 의미하고 있다.

VoIP는 이동성 정도에 따라 크게 유선 VoIP와 모바일(무선) VoIP로 분류할 수 있다. 기존의 유선전화와 같이 고정된 장소에서 초고속 인터넷망을 이용하여 음성통화를 하는 서비스의 형태가 유선 VoIP라면, 차세대 모바일 인터넷망을 사용하여 이동전화와 비슷한 전화 서비스를 제공하는 것이 모바일 VoIP, 곧 mVoIP(mobile Voice over Internet Protocol)이다.

국내의 경우, 기존 유선전화에 비해 저렴한 통신요금을 무기로 하는 VoIP의 이용자 수가 급속하게 증가하고 있다. 또한, mVoIP도 스마트폰의 확산과 함께 무선 인터넷망(3G, WiBro, 무선랜(Wi-Fi) 등)을 이용한 높은

이동성을 제공하여 사용자들이 어디서나 사용할 수 있어 빠른 속도로 활성화되는 추세이다.

하지만 VoIP의 경우 인터넷을 이용하기 때문에 인터넷에서 가능한 여러 가지 보안위협들이 그대로 적용되는 위험이 존재한다. 그 사례로 2008년 1월 미국 유타주에서 청각 장애인들에게 무료로 화상전화를 제공하는 회사인 유타(Utah)에 대한 해커의 공격을 들 수 있다. 해커는 미국 전역의 가정과 회사에 설치된 3만개 이상의 비디오폰을 감염시킨 후 VoIP 사업자를 대상으로 수만 통의 거짓 전화를 발생시켜(Call Flooding - 과도한 콜 트래픽을 일으켜 시스템을 다운시키는 공격) 서버를 불능상태로 만들었다. 이 때문에 1만명 이상이 서비스를 이용하지 못하는 큰 피해를 입은 바 있다. 또한 지난 2006년 미국 뉴욕에선 한 해커가 2년여 동안 15개 VoIP 서비스 사업자의 서버를 해킹하여 1000만 달러 상당의 회선을 불법으로 사용한 사건이 발생하기도 했다.

이러한 사례에서 알 수 있듯이 연평균 53%씩 빠르게 급성장하며 많은 이용자를 끌어 모으고 있는 VoIP 서비스는 해킹, 스팸 등 보안위협에 심각하게 노출되어 있다. 이러한 이유로 주요기업 및 행정기관에서는 정보 유출과 원활한 의사소통 문제로 인해 경제성과 이동성의 장점에도 불구하고 VoIP의 도입을 지연하고 있기도 하다.

한 편, 최근 스마트폰 사용자가 급증하면서 스마트폰 상에서의 킬러앱의 하나로 mVoIP가 주목 받고 있다. mVoIP 관련 어플리케이션은 2011년 7월 현재 아이폰에서만 150개 이상을 다운로드 받을 수 있다. 중소업체 및 개인 개발자가 공급하는 제품이 많아 정확한 제품 사용통계를 산정하기 어려운 실정이지만, 매우 많은 사용자가 mVoIP 어플리케이션을 다운로드 받아 사용하고 있음은 쉽게 알 수 있다.

그러나 기존의 유선 VoIP와 마찬가지로 보안문제는 mVoIP 어플리케이션을 사용하는데 있어서 반드시 주의해야 할 부분이다. 실제로 2011년 3월 국내 한 일간지에서는 국내 주요 mVoIP 서비스 6개에 대해서 도청 테스트를 수행하였는데, 그 결과 실험대상이 된 모든 mVoIP 서비스에서 도청이 가능하다는 결과를 발표하였다[3].

mVoIP에서 통화와 관련된 기반 기술은 기존 VoIP 기술을 그대로 이용한다. 이는 곧 VoIP의 보안위협을 그대로 상속받게 됨을 의미한다. 또한, mVoIP 어플리케이션이 탑재되는 스마트폰은 이동성이 높은 반면 분실위험이 크다. mVoIP를 이용하기 위해서는 사용되는 ID, 패스워드, 통화기록 등 중요정보들이 스마트폰에 저장되게 된다. 스마트폰의 분실위험이 큰 만큼 이러한 중요정보의 분실위협 또한 함께 커진다는 점은 기존 VoIP에 비해서 심각한 문제이다. mVoIP의 또 하나의 장점은 무선랜(Wi-Fi) 기술을 이용하여 거의 무료로 통화가 가능하다는 점이다. 그러나 이 역시 무선랜의 보안 취약성을 이용한 공격이 용이함을 의미하기도 한다. 무선랜 보안 취약성은 이미 여러 차례 지적된 바 있으며, 특히 도청 등에 이용되어 사용자에게 피해를 입히는 여러 사례가 보고된 바 있다.

이와 같이 mVoIP에 대한 보안위협이 심각함에도 불구하고 mVoIP 보안 대응은 매우 미흡한 실정이다. 국내 유선 VoIP의 경우, 한국인터넷진흥원을 통해 이미 VoIP 보안권고해설서, VoIP 침해사고대응해설서 등이 배포되어 VoIP 사업자 및 사용자의 보안인식을 확고히 하고 보안사고를 줄이는데 기여하고 있다. 외국의 경우에도 NIST에서는 “Security Consideration for Voice over IP Systems"와 같은 보고서를 통해서 VoIP 정보보호에 대한 대책을 제시하고 있다. 하지만 mVoIP에 대해서는 국내외적으로 이와 같은 보안 대책이 전무하다시피 한 실정이다. 특히 앞서 언급한 바와 같이 중소규모의 개발사나 개인 개발자가 공급하는 경우가 많은 mVoIP에서 보안위협에 대한 서비스의 안전성을 검증하는데 현실적으로 많은 어려움이 존재하기도 한다. 따라서 일반 사용자가 안심하고 mVoIP 서비스를 이용하기 위해서는 도청을 비롯한 보안문제가 반드시 선결되어야 한다.

제 2 절 목표 및 내용

본 연구의 목표는 이미 보고되거나 발생 가능한 mVoIP 보안 위협으로부터 서비스 이용자를 보호하고 안전하고 신뢰할 수 있는 mVoIP 서비스 이용 환경을 조성하기 위해서 필요한 기술적·관리적 사항을 설명하는데 있다.

본 보고서의 구성은 다음과 같다. 우선 2장에서는 mVoIP의 기술적 개요와 기술 및 시장 동향에 대해서 기술한다. 3장에서는 mVoIP 보안위협 및 정보보호 요구사항에 대해서 설명하고, 4장에서는 mVoIP 보안위협에 대응하기 위한 mVoIP 정보보호 대응방안에 대해서 기술한다.

추가적으로 부록 A에서는 기존 VoIP 정보보호 점검항목을 수록하여 mVoIP와의 비교를 돕는다. 그리고 부록 B, C, D에서는 정보보호체계와 관련한 표준화 동향을 살펴본다.

제 2 장 mVoIP 동향

○ mVoIP는 모바일 단말(스마트폰)을 기반으로 저렴한 비용으로 이용이 가능한 인터넷 전화를 의미

○ skype, fring(국외), 마이피플, 올리브폰(국내) 등이 가장 대표적인 서비스

○ 전 세계적으로 2015년까지 5억명 이상의 이용자를 확보할 것으로 예상되는 매우 전망이 좋은 서비스임

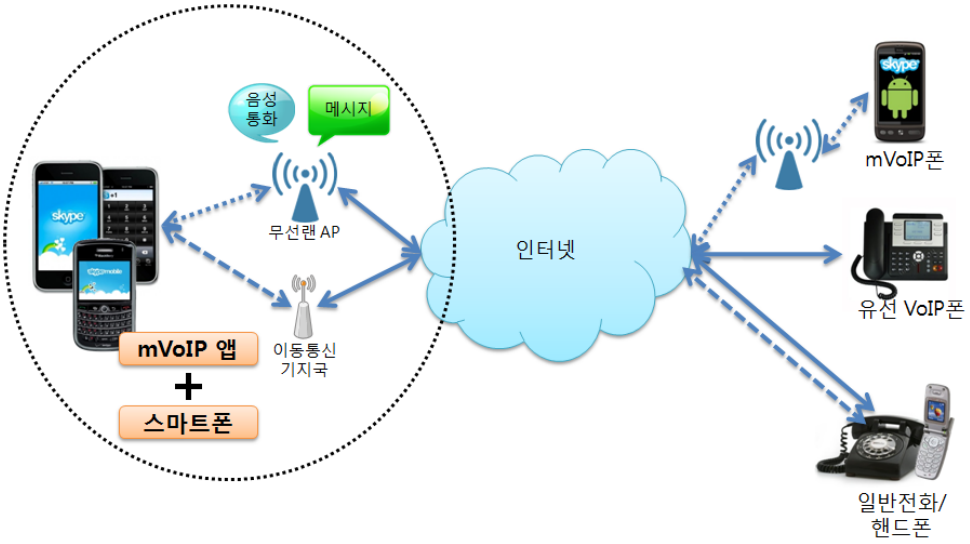
○ *키워드: mVoIP의 정의, mVoIP 시장 전망*

제 1 절 mVoIP 개요

1. mVoIP 정의

mVoIP는 모바일 단말(스마트폰 등)과 무선 네트워크(3G, WiFi 등)를 통해 제공되는 인터넷전화(VoIP)로 정의할 수 있다. 여기서 VoIP는 아날로그 상태인 음성을 디지털로 바꿔 회선교환 방식 대신 인터넷으로 전송하는 기술을 말한다. 음성통화를 발신단에서 패킷으로 나누고, 인터넷을 통해 전송한 후 착신단에서 다시 조합하여 제공함으로써 단대단(end-to-end) 결합을 필요로 하지 않는 점이 기존의 회선교환 방식과 다른 점이다. 이로 인해 사업자 간 상호접속 및 로밍계약이 필요하지 않아 사용자에게 저렴한 요금으로 제공할 수 있으며, 특히 회원 간에는 추가적인 비용이 발생하지 않아 무료전화 서비스를 이용할 수 있다.

최근 스마트폰의 활성화와 함께 mVoIP는 (그림 2-1)과 같이 스마트폰에 mVoIP 앱(어플리케이션)을 설치하여 다른 mVoIP폰, 유선 VoIP 폰, 일반 전화 및 핸드폰 사용자와의 통화를 제공하는 서비스라고 할 수 있다.



(그림 2-1) mVoIP의 개념

이러한 mVoIP는 제공주체에 따라서 설비기반의 mVoIP와 애플리케이션 형태의 mVoIP로 구분할 수 있다. 현재 많이 이용되고 있는 mVoIP는 3rd party mVoIP 사업자의 소프트웨어를 이동단말에 다운로드 및 설치하여 3G 또는 WiFi 망을 통해 사용하는 형태이다.

2. mVoIP 비즈니스 모델

현재의 mVoIP 시장은 통신 사업자보다는 3rd party 애플리케이션 사업자나 인터넷 사업자가 주도하고 있다. 초기의 mVoIP 비즈니스 모델은 '전통적인 VoIP 사업의 모바일화'라고 할 수 있다. 대표적인 사업자로는 Skype 및 Truphone이 있으며, 회원 간의 무료서비스 제공을 통해 이용자를 확대하여 국제전화 매출을 발생시키는 모델이다. 특히, Skype는 기존의 PC 기반 소프트웨어로 출발하여 2009년 4월에 아이폰용, 2010년 10월에는 안드로이드용 애플리케이션을 출시하여 모바일 단말기를 통한 서비스제공 채널을 확장하고 있다[1].

최근에는 인터넷의 양면 시장적 특성을 활용하여 포털 사업자 및 SNS

(Social Network Service) 사업자가 무료 mVoIP를 제공하는 경우가 증가하고 있다. Google이나 다음(Daum)과 같은 포털사업자나 eHarmony 등의 SNS 사업자는 무료 mVoIP의 제공을 통해 가입자를 확대하여 모바일 광고 분야에서의 매출확대를 꾀하고 있다[2]. 또한 전 세계적으로 5억명 이상의 사용자를 확보하고 있는 최대 SNS인 페이스북(Facebook) 역시 최근에 VoIP를 지원하기로 한 바 있다. 이는 향후 스마트 라이프 시대에 mVoIP가 매우 중요한 역할을 할 것임을 예측 가능케 한다.

2개의 비즈니스 모델 모두 회원 간에 무료 통화 제공을 통해 이용자를 확대한다는 공통점이 있다. 하지만 후자의 경우에는 전자와 달리 국제전화와 같은 통신매출의 발생을 주된 목적으로 하지 않는다는 점에서 차별화된다[1]. 해외 주요 mVoIP 사업자의 요금구조를 살펴보면 [표 2-1]과 같다.

[표 2-1] 주요 mVoIP 요금 구조

업체명	내용	공통사항
skype	· 미가입자로 연결시 1분당 2.3센트 · 국가별 월정액 운영	가입자간 통화 무료
Fing	· 미가입자로 연결시 1분당 1센트	
Truephone	· 1달 15달러의 3개월 단위 충전식 카드 · 사용시간과 연결국가에 따라 비용청구	
Nimbuzz	· 자유설정 금액의 충전식 카드 · 사용시간과 연결국가에 따라 비용청구	

이와 같이 mVoIP 기반의 비즈니스 모델이 등장하고 다양한 활용 방안을 모색하고 있는 가운데, [표 2-2]에서 보는 바와 같이 mVoIP 시장은 지속적으로 증가할 것으로 예상되고 있다.

[표 2-2] mVoIP 시장 전망

구분	2010	2011	2012	2013	2014	2015
mVoIP 이용자수 (백만명)	38.5	58.8	107.3	182.3	296.2	453.1
mVoIP 매출 (백만$)	949.4	1,926.9	3,469.4	6,225.3	11,110.8	18,864.4
mVoIP 통화량 (십억분)	15.1	33.7	66.4	132.2	259.3	470.7

(출처: Juniper Research (2010))

3. mVoIP 기술

기술적인 측면에서 mVoIP는 이동성이 가미된 기존 VoIP의 확장이라고 할 수 있다. 바꿔 말하면 휴대용 단말기를 이용해서 VoIP 서비스를 이용하는 형태가 mVoIP라고 할 수 있다. 따라서 mVoIP 클라이언트를 구현하는 가장 대표적인 형태는 표준 SIP 클라이언트를 스마트폰 등 휴대용 단말에 적합하게 구현하는 것이다. 이 때 SIP은 IP 네트워크를 지원하는 모든 네트워크(EVDO, HSDPA, Wi-Fi, WiMax 등) 위에서 동작 가능하다. 따라서 mVoIP의 경우에는 사용하는 네트워크에 따라서 통화품질과 경제성에 차이가 생길 수밖에 없다. 예를 들어 Wi-Fi를 이용한 mVoIP 서비스의 경우, 거의 무료로 이용이 가능하지만, 이용범위가 AP의 서비스 범위로 제한되고 핸드오프 역시 제한적이다. 하지만, 3G/4G 망을 이용한 mVoIP 서비스의 경우에는 이용비용은 높아지지만, 좋은 통화품질과 빠른 핸드오프를 보장할 수 있다.

앞서 언급한 바와 같이 기술적으로 mVoIP는 VoIP의 확장이기 때문에 별도의 표준은 존재하지 않으며, VoIP 기술과 표준기술을 공유한다고 할 수 있다. 현재 대부분의 mVoIP 서비스 역시 IETF(Internet Engineering

Task Force)에서 주도하고 있는 SIP 및 RTP을 기술 표준으로 참조하고 있다. IETIF의 SIP 및 RTP 표준화 현황을 살펴보면 다음과 같다.

[표 2-3] mVoIP 관련 표준 현황

분류	문서번호	문서명	등록일
제어 프로토콜	RFC3261	SIP: Session Initiation Protocol	2002. 6
미디어 프로토콜	RFC3550	RTP: A Transport Protocol for Real-Time Applications	2003. 7
보안 프로토콜	RFC4556	SDP: Session Description Protocol	2006. 7
	RFC3711	Ther Secure REal0Time Transport Protocol	2004. 3
	RFC3830	MIKEY: Multimedia Internet KEYing	2004. 8

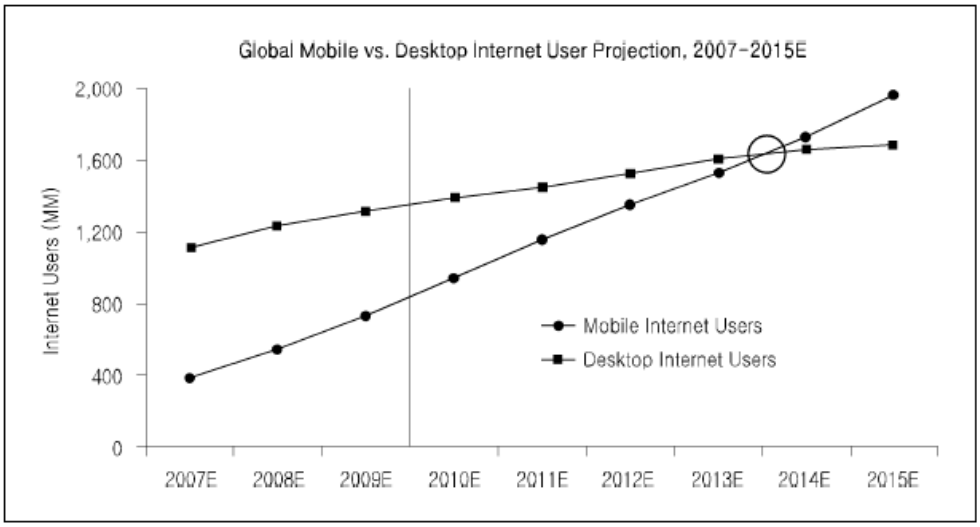
4. mVoIP 시장 전망

가. 해외 시장 전망

지난 2009년과 2010년은 세계의 주요 이동통신사들이 어플리케이션 기반의 VoIP 서비스에 대한 기존의 태도를 바꾼 역사적 전환의 시기라고 볼 수 있다. 2007년 스마트폰이 출시되었을 당시만 해도 대부분의 이동통신사들은 VoIP 서비스 이용에 뚜렷한 제한을 두고 있었다. 그러나 인터넷 기반의 VoIP 사업자들이 다양한 스마트폰 OS 및 단말기에 자신들의 클라이언트를 개발하는 플랫폼 전략을 추진한 결과 mVoIP를 사용하는 이용자가 급격하게 증가하였다. 다양한 어플리케이션을 탑재한 스마트폰이 대중의 호응을 얻으면서 mVoIP 서비스 활성화에 대한 시작의 기대도 함께 커졌으며, [표 2-2]에서 이미 살펴본 바와 같이 2015년까지 mVoIP의 통화량이 지금보다 30배가 넘는 수준으로 성장할 것이라는 예측이 나오

기도 하였다[9].

mVoIP 서비스 확산의 가장 큰 원동력 가운데 하나로 모바일 기반의 인터넷 사용자의 급속한 증가를 꼽을 수 있다. 2010년 4월 모건 스탠리(Morgan Stanley)는 전세계 모바일 인터넷 이용자의 규모가 늦어도 5년 이내에 PC 기반의 인터넷 이용자 규모를 앞지를 것이라는 내용의 보고서를 발표하였다[10]. (그림 2-2)에서 보듯이 2010년에는 전세계 데스크탑 인터넷 이용자 수가 모바일 인터넷 이용자 수보다 많지만, 2014년에는 동일한 수준에 이르고 그 이후에는 앞지를 것으로 전망했다.



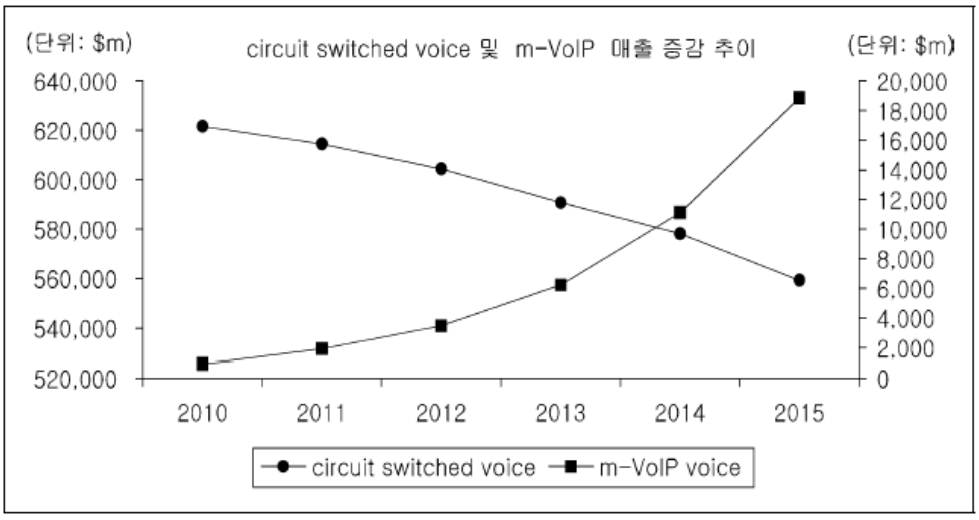
자료: Morgan Stanley(2010. 4)

(그림 2-2) 전세계 모바일 및 데스크탑 인터넷 이용자 추이 전망

모건 스탠리에 의하면 현재의 모바일 인터넷 이용의 확산은 10년 전 AOL/Netscape 기반의 유선 인터넷 확산보다 빠르게 진행되고 있다[10]. 특히 지난 3년 동안의 스마트폰의 확산은 이러한 모바일 인터넷 인구 급증에 직접적인 요인으로 작용하고 있다[9].

mVoIP 서비스 확산의 또 다른 배경요인으로 모바일 인터넷 전화 어플리케이션의 확산을 들 수 있다. skype, Nimbuzz, Fring, Truphone 등으로

대표되는 mVoIP 사업자들은 P2P 방식을 기반으로 다양한 모바일 OS 플랫폼과의 호환을 통해 자신들의 가입자 규모를 늘려왔다. 이들 mVoIP 사업자들의 목표는 자신들의 소프트웨어가 다양한 모바일 OS 및 단말기에서 운용되는 것이며, 이를 위해서 서로 연동이 되도록 협정을 맺고 저렴한 서비스를 제공하고 있다[9]. 선두 사업자인 skype는 iPhone용 버전을 출시한 이후 뒤 이어 안드로이드용 버전을 출시하였으며, Nimbuzz, Fring, Truphone도 iPhone, 안드로이드, 심비안, 윈도우 모바일, 리눅스 등의 플랫폼을 지원하고 있다.

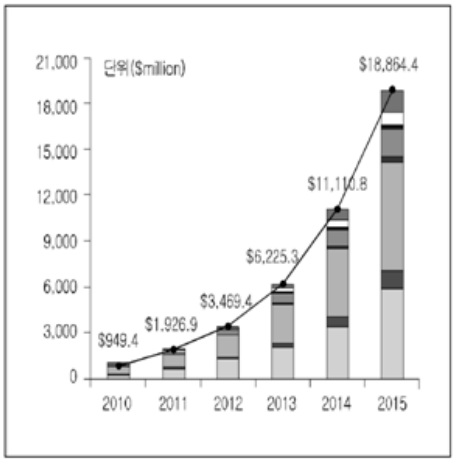


(그림 2-3) 서킷 방식의 음성 매출 및 mVoIP 음성 매출의 증감 추이 비교

모바일 브로드밴드 인터넷 이용자가 급증하고 mVoIP 어플리케이션이 확산되고 있는 가운데, 향후 mVoIP 사용자의 증가가 가파른 상승곡선을 보일 것이라는 예상이 일반적이다. 시장조사업체인 가트너(Gartner)는 mVoIP 사용자가 2013년에 전세계적으로 3억명에 이를 것으로 예측하였고, 주니퍼 리서치(Juniper Research) 역시 mVoIP 사용자가 2년 내에 1억명에 이를 것이라고 전망하였다((그림 2-3) 참조).

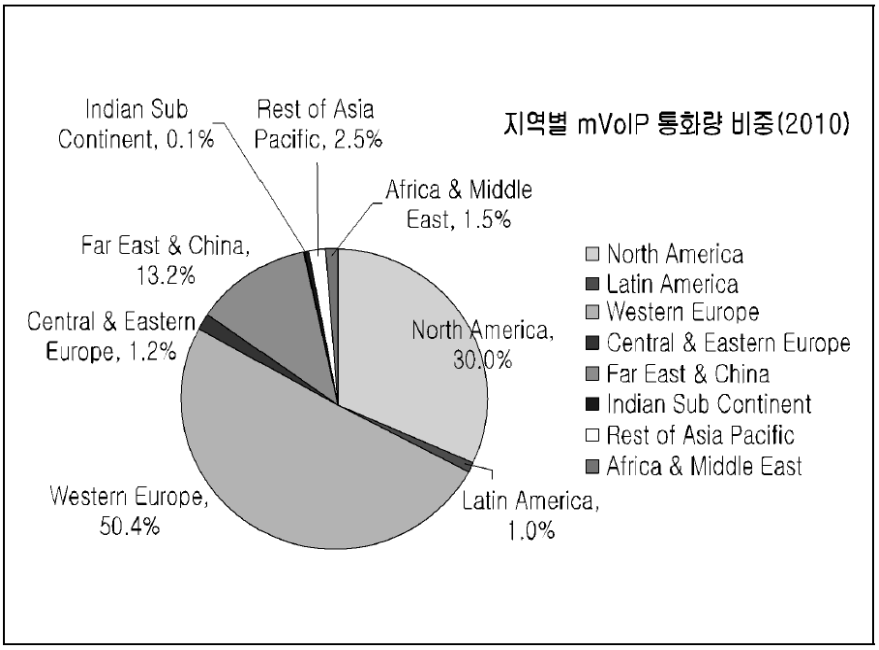
물론 서킷교환방식의 음성통화의 경우, 2010년에는 6,216억 달러로 절대

적인 수치로 비교하였을 때, mVoIP 시장은 서킷교환방식 시장의 0.15%에 불과한 작은 시장이다. 그러나 증감 추이를 비교해본 결과, 2015년에 서킷교환방식의 음성 매출은 5,594억 달러로 감소하는 반면 mVoIP는 189억 달러로 급증하여 서킷교환방식의 3.4%까지 이를 것으로 예상된다.



(그림 2-4) 지역별 mVoIP 통화량 비중의 연도별 추이

이러한 전세계의 mVoIP 시장에 대한 전망은 지역마다 큰 차이를 보이는데, 지역별로 가장 큰 mVoIP 시장은 서유럽으로 2015년 기준 70억 달러, 전체시장의 37%를 차지할 것으로 예측된다. 두 번째로는 북미가 59억 달러로 전체 시장의 31%를, 다음으로는 극동 아시아 및 중국이 18억 달러로 10%를 차지할 것으로 예상된다. 반면에 중·동부 유럽, 인도 및 나머지 아시아 지역, 아프리카 및 남미 지역의 mVoIP 통화량은 각각 7%를 넘지 못할 것으로 예상된다. 2010년 말 mVoIP 통화량 기준으로도 서유럽은 50.4%, 북미는 30%, 극동 아시아 및 중국은 13.2%로 mVoIP 통화량의 대부분(93.2%)를 차지하고 있는 반면 나머지 지역의 통화량은 각각 3%를 넘지 못하고 있다((그림 2-4), (그림 2-5) 참조)[9].



(그림 2-5) 지역별 mVoIP 통화량 비중

앞서 살펴보았듯이 글로벌 mVoIP 사업자인 skype, Fring, Nimbuzz, Truphone 등은 모두 주로 서유럽을 기반으로 성장하고 있으며, 이는 모바일 생태계가 지역적인 편차를 두고 성장하고 있음을 보여주는 단면이라고 할 수 있다. 지역적인 편차가 발생하는 원인을 몇 가지로 추측해볼 수 있는데, 그 중 가장 큰 원인은 모바일 브로드밴드의 발전단계가 국가 및 지역별로 다르기 때문인 것으로 판단된다[9].

한 편, mVoIP 서비스 확산이 일어날 수 있는 가장 유력한 시장 가운데 하나가 국제전화시장이다. 미국의 한 설문조사에 의하면 국제전화를 이용하는 사람들 가운데 유선전화로 국제전화를 이용하는 사람들은 51%, 휴대폰을 이용하는 국제전화 사용자는 44%이다. 휴대폰을 통화 국제전화 이용자 가운데 9% 정도가 mVoIP 어플리케이션을 사용하는 것으로 나타났다[9]. 사용자에게 mVoIP는 일반 시내전화보다는 국제전화의 용도로 더욱 매력적이라고 할 수 있는데, 이는 최근의 스마트폰 요금제에서 이용자에게 250분 이상의 충분한 음성 통화 시간이 주어지기 때문이다.

[표 2-4] 국제전화 요금 비교

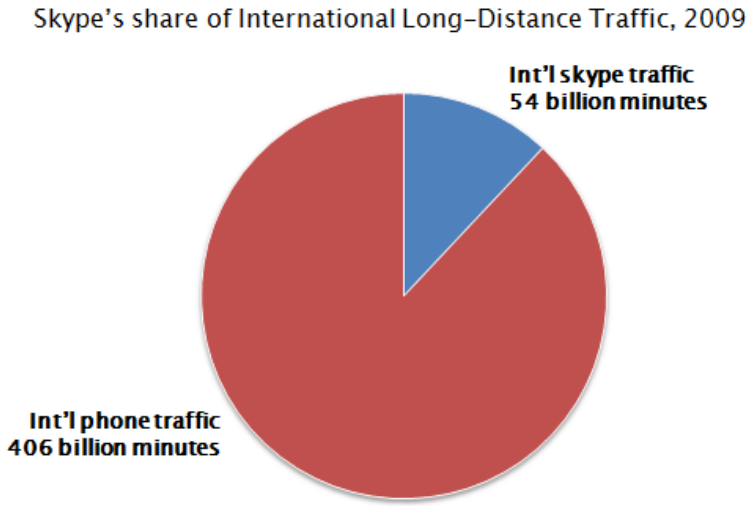
(단위: 펜스, 2010년 11월 현재)

	Orange	Vodafone	BT	skype	Truphone
휴대폰 수신(영국 발신 기준)					
호주	20.0	15.0	26.9	11.8	1.3
인도	20.0	15.0	8.9	4.7	2.5
중국	7.0	5.0	26.9	1.4	1.3
폴란드	20.0	15.0	26.9	14.5	1.3
러시아	40.0	15.0	26.9	4.9	2.5
미국	7.0	5.0	2.5	1.4	1.3
한국	15.0	20.0	26.9	4.2	4
일본	18.0	15.0	26.9	9.9	1.4
유선전화 수신(영국 발신 기준)					
호주	6.0	5.0	2.5	1.4	1.3
인도	12.0	5.0	5.3	4.7	2.5
중국	6.0	5.0	2.5	1.4	1.3
폴란드	12.0	5.0	2.5	1.4	1.3
러시아	20.0	5.0	5.3	1.4	2.5
미국	7.0	5.0	2.5	1.4	1.3
한국	7.0	10.0	5.3	1.4	1.3
일본	10.0	5.0	2.5	1.6	1.4

실제로 국제전화 시장에서 Truphone은 다른 이동통신사 및 경쟁업체보다 경쟁력 있는 요금 서비스를 제공하고 있다. Truphone은 전세계적으로 약 38개국이 넘는 국가에서 모바일-유선으로의 국제전화 요금을 분당 약 5센트에서 2.1센트 정도로 저렴하게 제공하고 있으며, 무제한 모바일 국제전화 서비스의 경우, 월 12.95달러로 제공하고 있다. [표 2-4]에서 보듯이 Orange, Vodafone, BT의 국제전화요금은 수신지역에 따라 적게는 2배에

서 많게는 16배 정도나 높은 가격수준을 형성하고 있다[11].

한편, skype 역시 국제전화시장에서 괄목할 만한 성장을 이어가고 있다. 2009년에는 전세계 국제전화 통화량 4,060억분에서 skype가 차지하는 비중은 12%에 해당하는 540억분에 이르렀다. 이는 2008년보다 51% 증가한 수치이다. 통신사업자들이 제공하는 국제전화 통화량의 증가속도는 줄어드는 추세이나, skype의 국제전화 통화량의 증가속도는 급격하게 늘어나 국제음성전화 시장에서 skype의 시장 점유율이 상승하고 있다((그림 2-6) 참조)[12]. skype는 지금까지의 어떤 통신사업자보다 큰 규모의 국제전화 통화량을 기록하고 있으며, 이를 통해 기존 통신 사업자에게 위협적인 존재가 되고 있다.



(그림 2-6) skype의 국제전화 트래픽 비율

나. 국내시장 전망

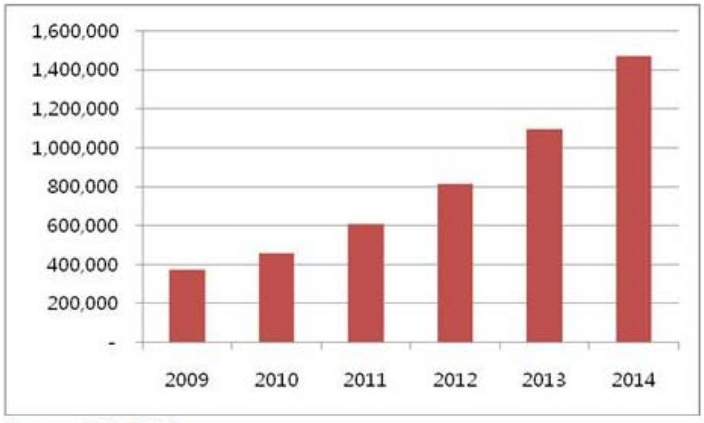
국내 VoIP 시장은 2009년 약 602억원에서 2010년에 약 608억원 규모로 소폭 성장하였다. 시장 초기에서 성숙기로 이동하면서 다소 더딘 성장세를 보이는 것으로 판단된다. VoIP는 초기에 기업시장을 중심으로 성장하였

으나, 기존 PSTN 서비스 사업자들이 VoIP 서비스에 적극적으로 대응함에 따라 가정용 시장으로 확산되고 있다. 이와 같은 가정용 시장의 성장에 힘입어 향후 5년간 연평균 33%로 성장하여 2014년에는 약 2,508억원대 규모가 될 것으로 전망하고 있다.

VoIP 서비스 시장은 KT를 포함한 주요 사업자들의 적극적인 가정용 서비스 시장 확대 노력에 힘입어 크게 성장하고 있다. 사업자들의 이러한 시장 확대는 지속될 것으로 보이며 이로 인한 일반 가정 전화 시장의 축소가 가속화될 것으로 예상 된다. 가정용 VoIP 서비스는 주로 초고속 인터넷과 방송이 결합된 TPS(Triple Play Service) 형태로 제공되고 있으며, 통신 사업자간 경쟁적인 마케팅 추진으로 가입자는 빠르게 증가되고 있다.

한편, 2008년 번호이동성제도의 시행은 지금까지 '070'번호로의 전환 문제로 인해 도입을 꺼리던 기업시장에 활력소가 되고 있다. 이제까지 통화료 절감을 위한 목적으로 사용되어 왔던 VoIP 서비스가 통합 커뮤니케이션(UC, Unified Communications) 형태의 각종 부가서비스와 결합하여 시장 활성화의 한 요소가 될 것으로 예상 된다.

또한 최근 Wibro, LTE 기반의 4G 도입이 이루어지고 있는데, 이를 기반으로 한 mVoIP의 활성화가 기대되고 있다.



Source: IDC, 2011

(그림 2-7) 국내 VoIP 서비스 시장 전망, 2009

(단위: 백만 원)

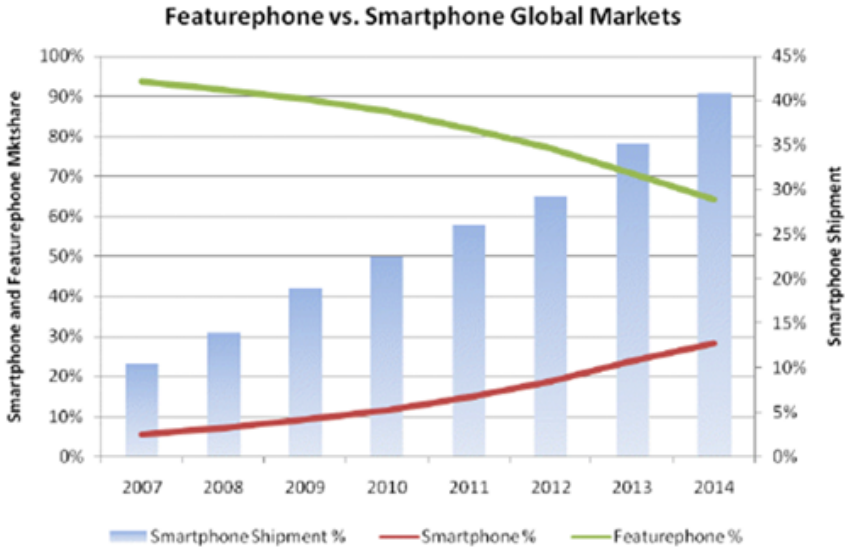
국내 VoIP 시장 전망에서 대해서 살펴보면, 2011년 국내 VoIP 서비스 시장은 전년 대비 32.4% 성장하며 6,070억 원대 시장을 형성할 것으로 전망되고 있다. 나아가 이 시장은 향후 5년간 연평균 31.4%의 성장세를 보이며 2014년에는 약 1조 4,688억원 규모에 이를 것으로 전망된다 ((그림 2-7) 참조).

(그림 2-8) 국내 스마트폰 판매 추이

(그림 2-8)은 국내 스마트폰 판매 추이이다. 이를 통해 스마트폰 시장의 잠재력과 규모를 알 수 있다. 특히, 2009년 아이폰 도입 이후, 스마트폰이 사회적 이슈가 되어 스마트폰 사용자들이 2009년에서 2010년 대폭 증가한 것을 알 수 있다. 아직까지는 전체 휴대폰 시장에서 스마트폰이 차지하는 비율이 미비한 실정이지만 일반 휴대폰의 점유율이 점차 낮아지고 스마트폰의 점유율은 성장하고 있어, 전문가들은 이러한 추세라면 머지않아 스마트폰이 일반 휴대폰을 대체할 것이라는 의견까지 내놓고 있다.

(그림 2-9)에서 휴대폰 시장의 일반 휴대폰과 스마트폰의 점유율을 확인할 수 있다. 향후 꾸준한 스마트폰 판매량의 증가를 예측할 수 있다. 전체 휴대폰 시장에서 스마트폰의 점유율이 높아지는 반면에 기존의 일반

휴대폰의 경우 점유율이 점차 낮아질 것으로 예상된다. 특히 2014년에 이르러서는 일반 휴대폰의 점유율은 70%대로 떨어지고 스마트폰의 점유율은 30%까지 상승할 것으로 예측된다.



(그림 2-9) 휴대폰 시장의 일반 휴대폰과 스마트폰 점유율

다. mVoIP 정책

앞서 설명한 바와 같이 스마트폰의 증가와 함께 VoIP 사용자도 꾸준히 증가하고 있어, mVoIP 시장이 대폭 확대될 것으로 예상하고 있다. mVoIP는 스마트폰의 이동성과 무선 인터넷 망(Wi-Fi 또는 3G/4G망)을 통한 통화료 부담을 해소할 수 있어, 많은 스마트폰 사용자들이 이용할 것으로 예상된다. 또한, 해외의 사례에 따르면, 2010년 10월 7일, 북미통신사업자협회주체 'CTIA(Cellular Telecommunications Internet Association) IT & 엔터테인먼트'에서 제나코스키 FCC(Federal Communications Commission) 의장이 참석하여 망 중립성을 공식적으로 무선망에 적용할 것이라고 발언하여 통신업체가 VoIP 데이터를 제한하지 못 하도록 하는 방안이 마

련되었다. 즉, 통신업체가 VoIP에 관한 데이터를 망 중립성에 의해서 고의지연 및 차단을 할 수가 없게 된다. 이에 따라 사용자는 VoIP를 통한 저렴한 음성서비스를 수준 높게 사용할 수 있게 된다. 한편, 국내에서는 2017년까지 4세대 통신망을 전국적으로 구축할 예정이다. 4세대 통신망은 ALL-IP 기반으로 방송, 통신, 인터넷을 통합하여 사용하기 때문에 mVoIP는 앞으로 더욱 발전할 것으로 예상된다.

현재까지, mVoIP 사업과 관련한 국내외 사업자 동향과 정책을 보면, KT는 Qook & Show 상품을 출시하여 서비스하고 있다. KT의 경우 자사의 서비스 이외의 VoIP 서비스에 대해서 사용 불가를 선언하였지만, 아직까지 크게 제한을 두고 있지는 않다. SKT의 경우는 정액제 가입자 대상에 한해서 mVoIP 서비스를 허용하고 있다. LG U+의 경우는 Wi-Fi에서만 사용 가능하도록 서비스를 제공하고 있다. 그러나 이와 같은 국내 이동통신업체의 정책에 최근 변화가 일고 있는데, 이에 대해서는 뒤에서 좀 더 자세하게 설명하기로 한다.

국외의 경우 AT&T가 자사의 이동통신망인 2G/3G 망에서도 VoIP 서비스를 이용하도록 허용하고 있으며, 유럽 및 영국에서는 VoIP 사업자인 Truphone와 Fring.com이 가상이동망사업자(MVNO)로 등록하여 가입자 번호를 확보하고 있다.

제 2 절 mVoIP 서비스 제공 현황

1. 해외 현황

mVoIP 서비스 제공에 관심을 가지는 사업자들은 크게 4가지로 구분할 수 있다. 첫째, VoIP 서비스 제공 사업자와 이동전화 사업자의 제휴 사업자로 skype와 Hutchison 등이 있으며, 둘째 모바일 소프트 폰 서비스 형태로 Fring, Nimbuzz, Truphone, Jajah 등이다. 세 번째로 MVNO (Mobile Virtual Network Operator) 사업자인 Japan Communications Inc.의 NTT Docomo의 3G 망 이용 사례가 있다. 마지막으로 Google 등 포털 서비스 제공 사업자 등으로 구분된다[2].

유선 VoIP에서도 선두 위치를 점하고 있는 skype는 모바일 서비스도 적극적으로 제공하고 있으며, 네덜란드에서 설립된 Nimbuzz는 2010년 9월 기준으로 220개가 넘는 국가에서 서비스를 제공하고 있는데, 3,000만명의 가입자를 확보하고 하루에 5만 5천명의 새로운 사용자가 서비스에 가입하고 있다. 또한 이스라엘의 Fing 역시 2010년 12월 기준으로 200개가 넘는 국가에서 서비스 되고 있다. Fing이 2008년 10월 발표한 자료에 따르면, Fring이 앱스토어에 등록된지 24시간 만에 9만 여건이 다운로드 되었다[9]. 본 항에서는 해외의 mVoIP 사업자 현황에 대해서 살펴보고자 한다.

가. skype

VoIP 서비스 제공 사업자 가운데 가장 큰 규모를 가진 사업자로 2011년 현재 전 세계적으로 6억명이 넘는 가입자를 확보하고 있다. 2010년 음성/영상 통화시간이 2천억분을 넘어섰다. skype는 2005년 9월 온라인 옥션 업체인 eBay에 인수되었으며, 이후 올해 5월 마이크로소프트사에 85억 달러에 인수되었다.

2006년 2월, skype는 영국의 후발 이동전화 사업자인 Hutchison 3, 단말기 제조 사업자인 Nokia와 협력 체계를 구축하여 세계 최초로 mVoIP 서비스를 상용화하는데 성공하였다. 이 비즈니스 모델에서 skype는 mVoIP 서비스 제공 및 과금을 담당하고 있으며, Nokia가 skype의 인터넷 전화 기능을 단말기에 장착하여 Hutchison 3에 제공하고 Hutchison 3은 자사의 3G망에서 skype 폰을 통해 mVoIP 서비스를 제공한다. 2007년 10월에는 Hutchison 3의 서비스제공 지역 가운데 영국, 이탈리아, 홍콩, 오스트리아에 skype 서비스제공이 시작되었으며 서비스지역은 계속 확대되어 가고 있다[2].

(그림 2-10) iPhone에서 skype 이용 화면

아이폰, 안드로이드 등 스마트폰이 활성화 되면서 skype는 아이폰용 앱((그림 2-10) 참조)과 안드로이드용 앱((그림 2-11) 참조)을 모두 제공하고 있다.

(그림 2-11) 안드로이드폰에서 skype 이용 화면

한 편, skype에서 제공하는 기능을 살펴보면 다음과 같다.

○ 무료 통화: skype 사용자와 skype 사용자 간에 무료통화가 가능하다.
○ 일반전화 및 휴대전화: skype를 통해서 일반전화 및 휴대전화로 전화가 가능하다(유료 서비스).
○ 컨퍼런스 통화: 다자간 통화 기능을 제공한다. 모든 참여자가 skype를 이용한다면 무료로 이용 가능하다. 그룹 영상 통화 기능도 함께 제공한다.
○ 보이스 메일: 통화를 할 수 없을 때 skype를 통해서 메시지 전달이 가능하다.
○ 파일 전송: skype를 통해서 문서, 비디오 클립, 사진 등을 전송할 수 있다.
○ 착신 통화 전화: 인터넷을 이용하지 않고 있을 때 skype 통화를 사용자가 선택한 전화로 연결이 가능하다.
○ 화면 공유: skype 통화를 하면서 프레젠테이션, 사진 등을 상대방과 공유할 수 있다.
○ SMS: skype를 통해서 저렴한 요금으로 상대방의 휴대전화로 문자

메시지를 전송할 수 있다.

○ 인스턴트 메시지: 일반적인 메신저에서 제공하는 인스턴트 메시지 기능을 제공한다.

나. Truphone

2007년 8월 영국의 솔루션 사업자인 Truphone은 휴대폰, PC 등 전자제품의 글로벌 소매업체인 eXpansys와 제휴를 체결하고 Nokia N 및 Nokia E 시리즈 듀얼폰 사용자를 대상으로 mVoIP 서비스를 제공하기 시작했다. 사용자는 자신이 가입한 이동전화 사업자가 제공하는 무선 데이터 접속, 3G 정액요금제 이용 및 Wi-Fi 접속 서비스 등을 통해 mVoIP 서비스를 이용할 수 있다.

2008년 5월부터 셀룰러망을 대상으로 한 VoIP 서비스 'Truphone Anywhere'를 시작하였으며, 사용자들은 Wi-Fi 핫스팟을 벗어난 경우 셀룰러 망을 이용하여 mVoIP 서비스를 이용할 수 있다. 아이폰용 어플리케이션은 2008년 7월 공개하였다.

(그림 2-12) iPhone에서 Truphone 이용 화면

2009년 2월에는 전세계 어디에서나 사용할 수 있는 USIM 기반의 mVoIP 서비스 'Truphone Local Anywhere'를 출시하였다. USIM 카드가 발행한 전화번호를 무제한 기억할 수 있게 함으로써 국가별 고유번호를 기억시켜 휴대폰만 있으면 해외에서도 해당 국가의 번호로 통화나 데이터 통신, SMS 등을 이용할 수 있는 서비스를 제공하고 있다[2].

현재 Truphone은 안드로이드, iPhone((그림 2-12) 참조), iPod, iPad, 심비안(노키아), 블랙베리 등 거의 모든 스마트폰 플랫폼에서 이용이 가능하다.

라. Fring

이스라엘에서 서비스를 시작하여 미국 시애틀까지 진출한 Fring은 3G 또는 Wi-Fi 네트워크에서 모바일 소프트폰 서비스와 구글 Talk와 같은 음성채팅 서비스를 2007년 2월부터 제공해오고 있다. Fring은 단말기 내에서 소프트폰 프로그램을 통해 음성 신호를 데이터로 변환하여 이동전화 사업자의 3G 망이나 Wi-Fi 망을 이용하여 송수신하는 방식으로 서비스를 제공하고 있다.

(그림 2-13) Fring 이용 화면

서비스 이용자들은 데이터변환이 가능한 스마트폰 또는 포켓 PC로 Fring 뿐만 아니라 구글 Talk, MSN 메신저 간 음성 채팅 서비스를 이용할 수 있다. 데이터접속요금은 별도이나, Wi-Fi Hotspot 지역에서는 mVoIP 서비스에 자동으로 로그인 되어 무료로 서비스를 이용할 수 있다.

2008년 2월에는 파일공유 등 데이터 응용서비스를 추가하였으며, 2008년 4월, iPhone용 앱을 발표하였다. 2008년 10월 오스트리아의 Mobikom이 Fring의 'VoIP3G' 솔루션을 채택하였다[2].

Fring의 제공기능은 무료음성통화, 영상통화, 그룹영상통화, 인스턴트 메시지 등 다른 mVoIP 서비스와 유사하다((그림 2-13) 참조).

마. Jajah

Jajah는 자사의 웹 사이트에서 발신자 전화번호로 전화를 걸 수 있도록 하여 기존의 사용자들의 이동 및 유선전화 단말에 음성서비스를 제공하는 방식이다. 서비스를 개시한지 1년 만에 200만 명의 가입자를 확보하였다.

Jajah는 2007년 10월 일본의 3G 신규 사업자인 e-Mobile이 HSDPA 지원 PDA 단말인 'E 모바일 ONE a'에 'Jajah Phone' 소프트웨어를 탑재하여 음성통화 서비스를 제공하면서 첫 서비스를 개시하였다. 2008년 7월부터는 인터넷전화 번호(050)를 부여하여 타망 착발신이 가능해지게 되었다.

2007년 5월 인텔은 Jajah와의 제휴를 선언하고 마케팅, 상품개발을 공동으로 추진하여, Jajah의 VoIP 호 처리 알고리즘을 인텔 칩에 내장할 계획을 발표하였다. 2008년 4월 Jajah는 셀룰러-Wi-Fi 겸용 방식을 채택한 iPhone용 mVoIP 어플리케이션과 iPod Touch용 VoIP 어플리케이션을 발표하기도 하였다.

2008년 5월, Jajah는 야후와 제휴를 체결하여 야후 메신저를 통한 음성서비스의 인프라 부분을 일임하게 되었다[2].

바. i2 Telecom

2008년 7월부터 i2 Telecom은 블랙베리와 스마트폰에서 MyGlobal Talk를 통한 VoIP 서비스를 개시하였다. 여타 mVoIP 서비스들이 대체로 Wi-Fi 망을 이용하거나 3G망을 이용할 경우 음성이나 SMS 채널을 이용한데 반해, MyGlobal Talk는 데이터 채널만을 통해 서비스를 제공한다.

이러한 경우 다른 mVoIP 서비스와 달리 이동통신업체에 의한 차단이 어려워 이들로부터의 간섭이 적을 것으로 예상된다. MyGlobal Talk는 i2 소프트웨어를 단말기에 다운로드 받아 설치하고 나면 별도의 소프트웨어 구동작업 없이 통화버튼만으로 통화가 가능하여 이용편의성을 상당히 높은 것으로 알려져 있다[2].

2. 국내 현황

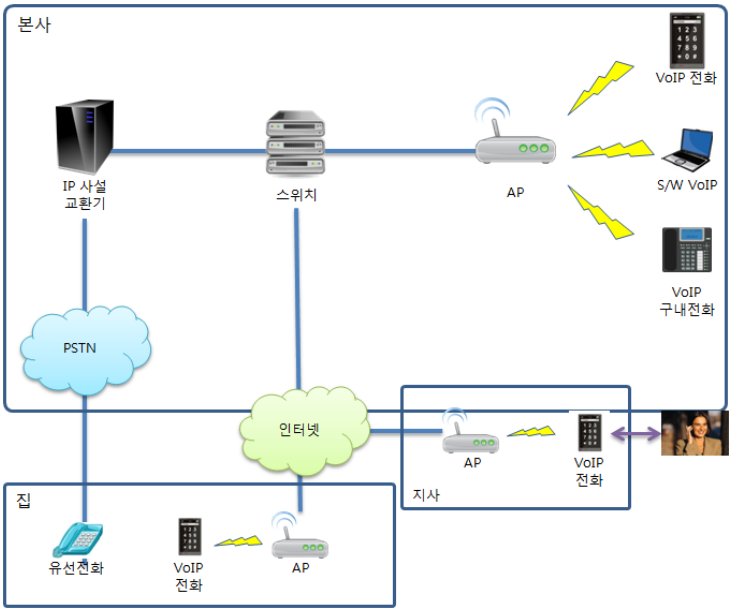
가. 개요

국내의 경우, mVoIP는 유무선 융합기술인 FMC(Fixed Mobile Convergence) 기술을 촉진시키는 역할을 하리라는 기대를 낳고 있다. 예를 들어 SK 텔레콤과 KT가 mVoIP의 전면 허용에 최근까지도 부정적인 입장을 가지고 있는 반면, LG U+(유플러스)의 경우에는 FMC를 통해 보다 적극적으로 mVoIP 서비스를 제공하고 있다. LG 유플러스의 FMC 서비스인 '오즈 070'은 휴대폰 하나로 이동사 3G망과 Wi-Fi 모두에서 통화가 가능한 서비스이다. 3G망을 이용하면 초단 1.80원, Wi-Fi를 이용하면 초당 1.17원이 과금되며 망내 통화는 무료이다[13]. LG 유플러스는 자사의 FMC 서비스를 위해서 mVoIP 전용 앱인 'U+070'도 2010년 11월 도입했다. 타사 스마트폰 이용자들도 이 앱을 무료로 다운 받아 가입하면 저렴하게 mVoIP 서비스를 이용할 수 있다. 국제전화를 걸 때 상대방 유선전화에 002 국제전화 식별번호를 이용해 걸면 미국, 중국, 일본 등 주요 20개국 기준 1분당 50원이라는 저렴한 요금으로 이용할 수 있다.

SK텔레콤의 경우에도 TB폰을 통해서 FMC 서비스 이용이 가능하다. (그림 2-14)에서 보는 바와 같이 하나의 단말에서 3G와 Wi-Fi를 모두 지원하기 때문에 Wi-Fi 이용가능지역에서는 저렴한 가격으로 mVoIP 서비스를 제공 받을 수 있으며, Wi-Fi 이용이 불가능한 지역에서는 3G 망을 이용해서 데이터 서비스 및 통화서비스를 이용할 수 있다.

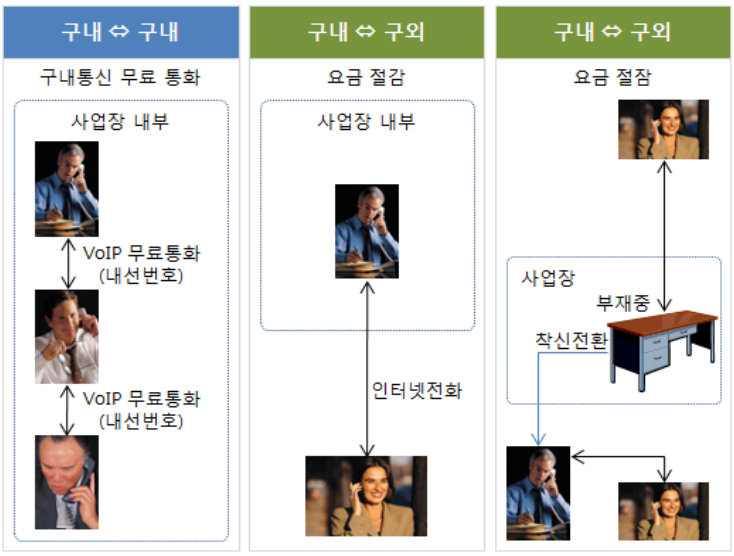
(그림 2-14) SK텔레콤의 FMC 서비스 TB폰

이는 같은 국내 이동통신 사업자들의 FMC 서비스 확대는 세계 유수의 이동통신사들이 skype와 구글 보이스 등을 3G 망에서 이용할 수 있도록 허용하는 추세와 유사하다. 2010년 2월 미국의 버라이존은 3G망에서 skype를 사용할 수 있도록 하겠다고 발표했다. 유럽의 이동통신사 3UK, 보다폰, 텔레포니카 등도 자사 망에서 skype를 허용하고 있으며, O2 역시 자사 가입자들에게 mVoIP 서비스를 제공하기 위해서 VoIP 사업자인 Jajah를 인수한 바 있다.



(그림 2-15) FMC 서비스 구조

mVoIP가 중심이 된 FMC 서비스 구조는 (그림 2-15)와 같으며, (그림 2-16)은 FMC의 적용사례이다.



(그림 2-16) FMC 적용 사례

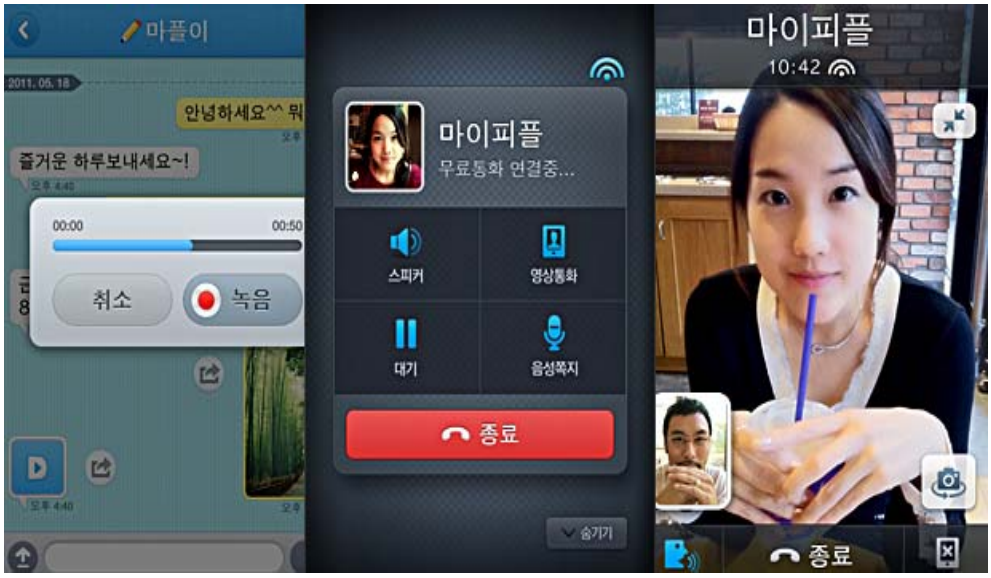
FMC는 얼마 전까지만 해도 (그림 2-16)과 같은 기업용 시장만을 목표로 하고 있었다. 사무실 안에서는 Wi-Fi 기능을 활용하고, 외근 시에는 이동통신망을 활용해 휴대폰을 사용하는 것 정도에 그쳤다. 그러나 최근에는 기업뿐만 아니라 가정에도 FMC가 속속 진출하고 있다. 집안에서는 인터넷 전화를 쓰고 외출을 하면 휴대폰으로 사용하는 것이다. 이와 같은 FMC의 확대에는 스마트폰과 mVoIP이 큰 역할을 하고 있다는 것은 부인할 수 없는 사실이다.

이와 같은 FMC는 이동성의 극대화를 통해 기업 측면에서는 업무 생산성의 대폭적인 증대를 가져올 수 있으며, 개인 사용자는 상승하는 통신비용을 절감할 수 있다.

나. 마이피플

현재 1천100만명의 가입자를 확보하고 있는 마이피플은 스마트폰의 등장과 함께 가장 각광받는 mVoIP 어플리케이션 가운데 하나이다. 마이피플은 아이폰, 안드로이드 등 스마트폰용 소프트웨어뿐만 아니라 윈도우, 맥용 소프트웨어를 함께 제공하고 있으며, 웹을 통해서도 서비스를 이용할 수 있도록 하고 있다. 마이피플의 제공하는 mVoIP 기능을 살펴보면 다음과 같다.

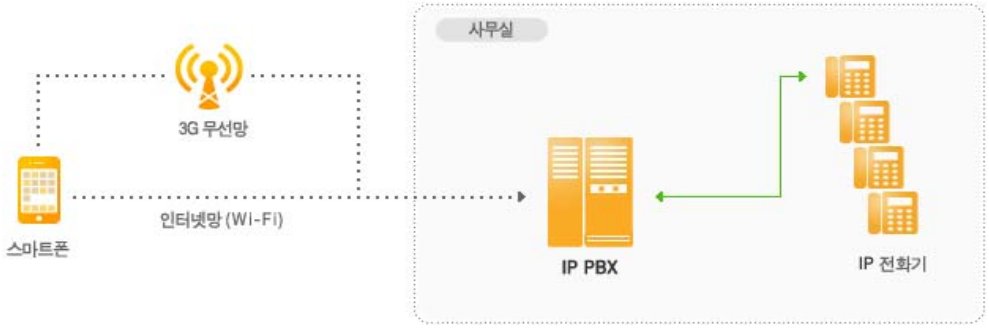
- ○ 무료 음성 및 영상 통화 기능: 3G, Wi-Fi 망을 이용하여 문자, 음성통화, 영상통화 가능(영상 통화의 경우, Wi-Fi 망에서만 가능), 무료 문자 기능 제공 ((그림 2-17) 참조)
- ○ 친구 관리 기능: 스마트폰의 주소록과 연계한 친구 관리 기능
- ○ 메시징 기능: 텍스트, 음성 쪽지, 이미지, 동영상 등을 교환할 수 있는 메시징 서비스 제공



(그림 2-17) 마이피플 - 무료 음성 및 영상 통화 기능

다. 올리브폰

250만 사용자를 확보한 올리브폰은 기업용 mVoIP 솔루션으로 유무선 전화를 통합하는 FMC(Fixed Mobile Convergence) '넷다이얼 SIP폰'과 mVoIP 기반 영상상담 솔루션 등을 출시한 바 있다.



(그림 2-18) 스마트폰용 SIP폰 구성도

올리브폰은 (그림 2-18)과 같이 표준 SIP 프로토콜을 채택하여 다양한

IP-PBX와 호환성을 확보하였다. 외부에서도 자신에게 걸려온 전화를 수신할 수 있기 때문에 외근, 출장이 잦은 경우에 매우 유용한 어플리케이션이라고 할 수 있다. (그림 2-19)는 올리브폰의 사용 화면이며, 주요 기능을 살펴보면 다음과 같다.

○ 음성통화 및 영상통화기능: 고품질의 음성통화 및 영상통화기능 제공
○ 무료통화: Wi-Fi 망에서 이용할 경우, 가입자간 무료통화가능
○ FMC 기능지원: 구내 IP-PBX와 연동하여 내선 전화기의 기능을 대체, 협업통화, 호전환 뿐만 아니라 3자통화기능 제공
○ 070 인터넷전화 지원: 삼성 와이즈, SK 등의 070 인터넷 전화기로 사용 가능
○ 다수계정 지원: 최대 4개의 인터넷 전화계정을 지원하며, 복수 개의 전화를 수신가능
○ 음성압축 기술: 3G 망에서 음성압축 기술제공. 망 이용요금을 절감하는 동시에 음성통화 지연현상을 없앰.

(그림 2-19) 올리브폰 사용화면

“이 페이지는 공백임”

제 3 장 mVoIP 보안위협

○ mVoIP는 기존 유선 VoIP가 갖는 보안위협을 그대로 상속함과 동시에 무선환경 및 단말의 특성에 의해 새로운 보안위협에 노출됨

○ 이에 따라 mVoIP는 음성 및 메시지 도청, 서비스 거부 공격, 중요 정보유출 및 재사용 등 다양한 보안위협에 노출이 불가피함

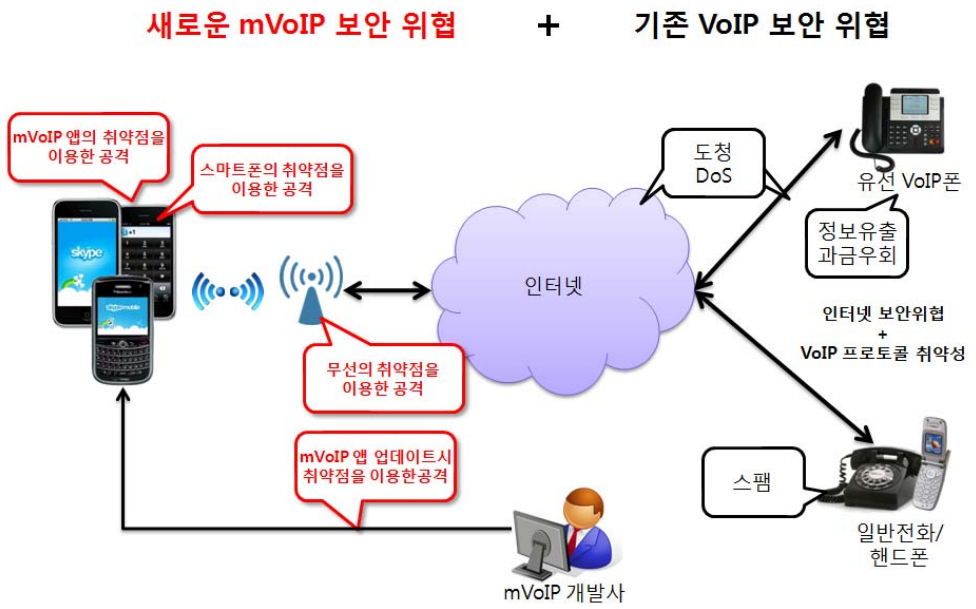
○ 이와 같은 보안위협을 최소화하기 위해서는 음성 및 메시지 암호화, VoIP 관리 메시지보호 등 mVoIP 정보보호 요구사항을 준수해야함

○ *키워드: mVoIP 보안위협, mVoIP 음성 및 메시지 도청, mVoIP 음성 및 메시지 암호화, mVoIP 정보보호 요구사항*

제 1 절 mVoIP 보안위협 개요

mVoIP 기술이 갖는 특성은 IP 망에서 이루어지는 서비스라는 점과 VoIP 기술을 이용한다는 점이다. 이는 곧 기존의 인터넷 망에서 발생 가능한 보안위협에 mVoIP가 그대로 노출될 수 있으며, VoIP 보안취약점 역시 그대로 적용될 수 있음을 의미한다. 기존 유선 VoIP와 비교하여 mVoIP가 갖는 가장 큰 기술적인 특징은 mVoIP 서비스를 제공하는 소프트웨어가 스마트폰으로 대표되는 무선단말에 탑재되어 무선기술을 이용한다는 점이다. 이러한 관점에서 mVoIP 보안위협을 (그림 3-1)과 같이 정리할 수 있다.

기존 VoIP 보안위협은 인터넷 보안위협과 VoIP 프로토콜의 취약성을 이용하게 되는데, 네트워크 상에서 도청 및 서비스 거부 공격, 단말에 설치된 VoIP 어플리케이션에서의 정보 유출 및 과금 우회, 스팸 공격 등을 포함한다. 네트워크 보안위협의 경우, 인터넷과 VoIP 폰 사이의 구간에서도 발생할 수 있지만, VoIP 사업자가 관리하는 네트워크 영역에서도 발생할 수 있다.



(그림 3-1) mVoIP 보안위협 개요

이와 비교하여 mVoIP 보안위협은 다음과 같이 mVoIP만이 갖는 특징을 이용한다.

○ mVoIP 앱의 취약점을 이용한 보안위협: mVoIP 앱 구현물이 갖는 보안 취약점을 이용하는 보안위협이다. 유선 VoIP에서 소프트폰의 취약점을 이용하는 보안위협과 유사하다. 유선 VoIP의 경우, VoIP 서비스가 하드웨어와 일체형으로 제공되는 경우가 많아 이러한 보안위협의 심각성이 낮다고 할 수 있으나, mVoIP의 경우는 누구나 쉽게 앱 개발에 참여할 수 있기 때문에 이와 같은 보안위협의 위험도가 매우 크다. mVoIP 앱의 취약점을 이용한 보안위협의 가장 대표적인 형태는 악성코드를 통해 단말 단에서 통화내용 및 메시지를 도청하는 것이다. 또한 현재 대부분의 mVoIP 앱들은 mVoIP 서비스 이용을 위해 필요한 중요정보를 mVoIP 앱 내부에 저장한다. 이 때 mVoIP 앱들이 이들 중요정보 보호에 취약점을 가지고 있다면 이러한

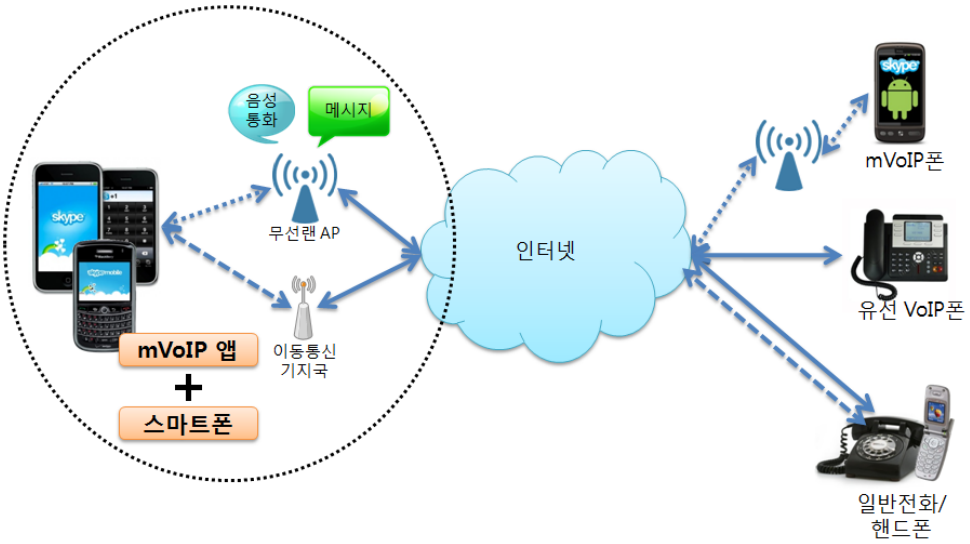
정보의 외부유출이 가능하다. 이러한 중요정보에는 ID/패스워드, 통화기록, 통화내용기록, 송수신 메시지 등이 포함된다. 특히 사용자 인증정보를 재사용하여 불법적으로 정상사용자의 서비스를 이용할 수도 있다. 추가적으로 대부분의 mVoIP 앱이 제공하는 메시징 및 주소록 관리기능을 이용한 스팸 역시 mVoIP 활성화에 큰 위협이 될 수 있다.

○ mVoIP 앱 업데이트시 취약점을 이용한 보안위협: mVoIP 앱 역시 다른 스마트폰 앱들과 마찬가지로 앱 스토어, 안드로이드 마켓 등 플랫폼 제공업체에서 운영하는 앱 배포체계에 의해서 이용자에게 다운로드 된다. 그러나 일단 다운로드가 완료되고 mVoIP 앱을 이용하는 과정에서 공지사항 전달, 환경설정은 앱 제조사와의 직접 통신을 통해 이루어지게 된다. 현재 기존환경과 비교해서 현저하게 보안수준이 떨어지는 앱 제조사의 환경을 고려할 때 mVoIP 앱 제조사와 mVoIP 앱의 통신과정에서 악성코드의 배포가 이루어질 위험이 매우 크다.

○ 스마트폰의 취약점을 이용한 공격: 최근 스마트폰 사용자가 급격히 증가하면서 가장 우려되는 사항 가운데 하나는 스마트폰의 보안 취약점을 이용한 악성코드의 범람이다. 그러나 현재 스마트폰용 안티바이러스 솔루션의 보급은 매우 미비한 상태이다. 따라서 스마트폰의 취약점을 이용한 도청, 인증우회 등 다양한 공격이 가능하다.

○ 무선 취약점을 이용한 공격: mVoIP 서비스는 Wi-Fi를 이용할 때 거의 무료로 통화가 가능하다. 따라서 많은 이용자들이 Wi-Fi 환경에서 mVoIP 서비스를 이용하게 된다. 그러나 Wi-Fi 기술이 3G/4G 등 셀룰러 망이나 인터넷보다도 많은 보안 취약성을 갖는다는 것은 이미 매우 잘 알려진 사실이다. ARP Poisoning, 위장 AP 등을 이용한 무선 구간에서의 도청, 메시지 flooding 등을 통한 서비스 거부

공격, VoIP 메시지 변조를 통한 사용자 위장 등 다양한 네트워크 상의 공격이 가능하다.



(그림 3-2) mVoIP 보안위협 적용 범위

기존 VoIP의 경우에는 VoIP 단말 및 네트워크뿐만 아니라 VoIP 사업자망구간에도 보안위협이 존재했다. 그러나 mVoIP의 경우에는 (그림 3-2)에서 보는 바와 같이 mVoIP 및 스마트폰, 그리고 무선 네트워크 구간에서만 보안위협이 적용된다. 이는 mVoIP의 경우에는 기존 VoIP와 같은 사업자망의 개념이 존재하지 않기 때문이다. mVoIP 보안위협을 정리하면 [표 3-1]과 같다.

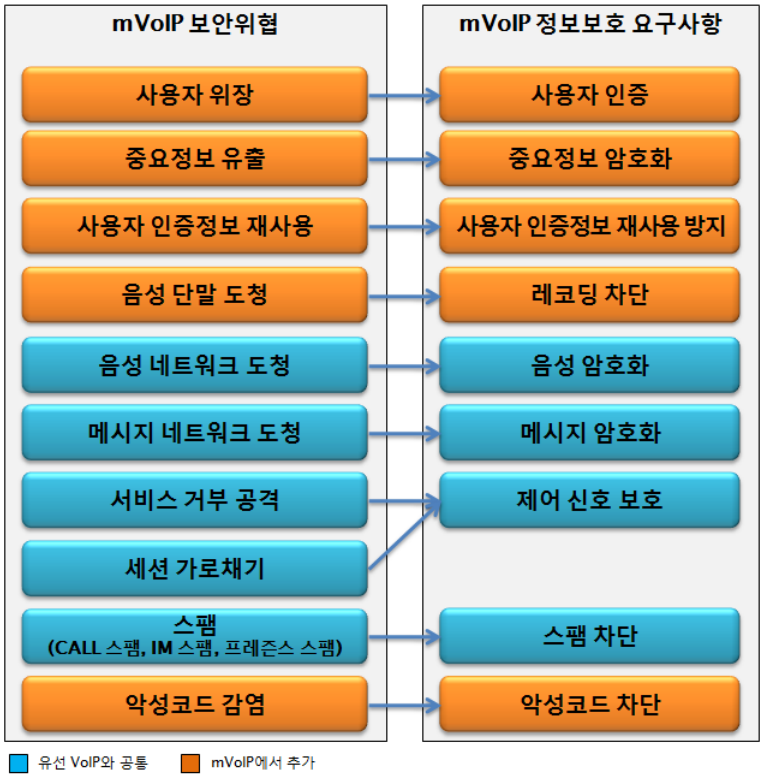
[표 3-1] mVoIP 보안위협

보안위협	설명
사용자 위장	비인가 사용자가 정상 사용자로 위장하여 정상 사용자의 mVoIP 서비스를 불법적으로 이용하는 보안위협이다.
중요정보 유출	ID/패스워드, 통화기록, 통화내용, 송수신 메시지

	등의 중요 정보를 단말로부터 외부로 유출시키는 보안위협이다.
사용자 인증정보 재사용	탈취한 인증정보를 복제하여 다른 단말 또는 PC 등에서 재사용함으로서 정상 이용자의 서비스를 가로채는 보안위협이다.
음성 도청 (네트워크)	단말과 Wi-Fi AP 사이의 구간에서 통화 내용을 도청하는 보안위협이다. ARP Poisoning, 위장 AP (Rougue AP/Fake AP) 등의 공격을 이용해서 도청을 수행하기 된다.
메시지 도청 (네트워크)	단말과 Wi-Fi AP 사이의 구간에서 사용자가 전송한 텍스트 메시지를 도청하는 보안위협이다. 음성 도청과 마찬가지로 ARP Poisoning, 위장 AP (Rougue AP/Fake AP) 등의 공격을 이용해서 도청을 수행하기 된다.
음성 도청 (단말)	스마트폰에 악성코드를 설치하고 이 악성코드를 이용해서 통화 내용을 도청하는 공격이다.
서비스 거부 공격	SIP 메시지 플러딩(flooding) 공격 등을 통해서 정상 mVoIP 서비스를 방해하는 보안위협이다.
세션 가로채기	SIP 관리 메시지를 가로챈뒤 그 내용을 변조하여 정상적으로 제공되고 있는 mVoIP 서비스에 개입하는 보안위협이다. 정상 사용자가 이용하고 있는 서비스를 가로채거나 방해하는 형태로 공격이 가능하다.
스팸	친구 추가 메시지 등을 이용해서 정상 이용자에게 스팸 메시지를 발송하는 보안위협이다.
악성코드	mVoIP 소프트웨어와 제조사의 통신 과정에서 악성코드를 배포하는 보안위협이다.

제 2 절 mVoIP 보안 요구사항

앞서 1절에서 살펴본 바와 같이 mVoIP에는 여러 가지 다양한 보안위협이 존재한다. 이와 같은 보안위협으로부터 mVoIP 서비스 및 이용자를 보호하기 위해서는 암호화 등 보안기술이 사용되어야 한다. mVoIP 보안위협에 대처하기 위한 mVoIP 보안 요구사항에 대해서 살펴보면 (그림 3-3)과 같다.



(그림 3-3) mVoIP 정보보호 요구사항

이와 같은 mVoIP 보안 요구사항은 모두 mVoIP 클라이언트, 즉 mVoIP 앱에 적용되는 사항이다. 악성코드 차단의 경우에는 mVoIP 클라이언트와 mVoIP 클라이언트와 mVoIP 클라이언트 개발사 사이의 네트

워크 구간에도 적용이 된다. [표 3-2]는 mVIP 보안 요구사항을 요약한 내용이며, 각각의 mVoIP 보안 요구사항에 대해서 살펴보면 다음과 같다.

[표 3-2] mVoIP 정보보호 요구사항 요약

	요구사항	내 용
1	사용자 인증	·비인가 사용자의 mVoIP 서비스 이용을 차단해야 한다.
2	중요정보 암호화	·mVoIP 소프트웨어가 저장하는 중요정보를 암호화해야 한다.
3	사용자 인증 정보 재사용 방지	·mVoIP 소프트웨어는 사용자 인증에 사용되는 인증 정보가 재사용되는 것을 방지하는 메커니즘을 적용해야 한다.
4	레코딩 차단	·악성코드의 레코딩 API 접근을 차단해야 한다.
5	음성 암호화	·mVoIP 소프트웨어는 모든 음성 통화 내용을 암호화해야 한다.
6	메시지 암호화	·mVoIP 소프트웨어는 모든 텍스트 메시지를 암호화해야 한다.
7	제어 신호 보호	·SIP 등 mVoIP 소프트웨어에 적용된 VoIP 제어 신호에 대한 기밀성 및 무결성을 보장해야 한다. ·SIP 등 mVoIP 소프트웨어에 적용된 VoIP 기술은 관련 표준 규격을 정확하게 준용해야 한다.
8	스팸 차단	·콜 스팸, 프레즌스 스팸 등 스팸 유포 시도를 차단할 수 있는 기능을 제공해야 하다
9	악성코드 차단	·mVoIP 소프트웨어와 mVoIP 제작업체 간의 네트워크는 악성코드 침투로부터 보호되어야 한다.
10	안전한 암호 기술	·검증된 암호기술을 mVoIP 소프트웨어에 적용해야 한다. ·암호화에 사용되는 암호키를 검증된 키 관리 기법을 통해서 보호되어야 한다.
11	프로토콜 구현의 정확성	·SIP등 VoIP 기술을 적용할 경우, 국제/국내 표준 규격을 정확하게 준용하여 구현해야 한다.

1. 사용자 인증

○ 요구사항: 비인가 사용자의 mVoIP 서비스 이용을 차단해야 한다.
○ 요구사항 설명: 안전한 mVoIP 서비스의 가장 기본적인 요구사항이라고 할 수 있다. 최소한 ID/패스워드 방식의 사용자 인증메커니즘을 적용함으로써 비인가 사용자가 불법적으로 정상사용자의 mVoIP 서비스를 도용하는 공격을 차단해야 한다.

2. 중요정보 암호화

○ 요구사항: mVoIP 소프트웨어는 mVoIP 서비스 제공을 위해서 사용되는 정보를 mVoIP 소프트웨어 내에 저장할 때, 암호화해야 한다.
○ 요구사항 설명: mVoIP 소프트웨어는 mVoIP 서비스 제공을 위해서 이용자 ID/패스워드, 통화 기록(통화 시작 시각, 통화 시간 등), 메시지기록(메시지 송수신 시각 등), 과금정보, 이용자 기본정보(e-mail 주소 등) 등 다양한 정보를 mVoIP 소프트웨어 내에 저장한다. 이와 같은 정보는 앱 DB나 로그 파일 형태로 저장되는 일반적이다. 정상적인 경우, 다른 앱에서 이와 같은 mVoIP 소프트웨어 내에 저장되는 정보에 접근하는 것이 불가능하지만, OS 해킹(아이폰의 경우 탈옥, 안드로이드의 경우 루팅이라 불림)에 의해 정보접근이 가능하며, 이와 같은 OS 해킹은 빈번하게 발생하고 있다. 따라서 OS 해킹을 가정하고 mVoIP 소프트웨어에 저장되는 정보를 보호하기 위해서 암호기술을 적용할 필요가 있다. 여기서 보호되어야 하는 정보는 앞서 기술한 바와 같으며, 저장되는 형태는 앱 DB, 로그파일, 에러 메시지 등 중요정보가 기록될 수 있는 모든 형태이다. 특히 DB 명이나 파일 명 등도 가능하면 암호화하여 중요정보가 누출될 수 있는 가능성을 최소화해야 한다.

3. 사용자 인증 정보 재사용 방지

○ 요구사항: mVoIP 소프트웨어는 사용자 인증에 사용되는 인증 정보가 재사용되는 것을 방지하기 위한 메커니즘을 적용해야 한다.

○ 요구사항 설명: 최근의 mVoIP 소프트웨어는 스마트폰에서만 사용할 수 있을 뿐만 아니라, PC용 소프트웨어나 웹에서 이용할 수 있는 형태의 VoIP 소프트웨어와도 호환이 가능하도록 서비스를 제공하고 있다. 이 경우, 유료 통화를 위한 잔액 등의 정보를 공유해야 하는데, 이를 위해서 mVoIP 서비스 제공 업체 측에서 이와 같은 정보를 저장 및 관리하게 된다. 따라서 이용자는 이용자 인증 성공 후에 이와 같은 정보에 접근할 수 있으며, 이용자 인증 과정에서 인증 정보가 이용되게 된다. 이 때, 단순히 ID/패스워드만을 인증에 이용하게 된다면, 공격자가 ID/패스워드를 알지 못하는 상태에서 ID/패스워드가 암호화된 상태 그대로 유출하여 재사용하는 공격이 가능하다. 이를 방지하기 위해서는 인증에 사용되는 정보에 인증 때마다 달라지는 정보를 삽입하는 방법 등을 사용해야 한다. 따라서 이 요구사항은 mVoIP 서비스에 적용되는 사용자 인증 메커니즘과도 밀접한 관련을 갖는다.

4. 레코딩 차단

○ 요구사항: 악성코드의 레코딩 API 접근을 차단해야 한다.

○ 요구사항 설명: 단말에서의 음성 도청은 악성코드가 레코딩 API에 접근해 사용자가 마이크로 입력한 음성을 녹음하는 방식으로 이루어진다. 따라서 단말에서의 음성 통화도청을 차단하기 위해서는 레코딩 API에 대한 악성코드의 접근을 차단해야 한다.

5. 음성 암호화

○ 요구사항: mVoIP 소프트웨어는 모든 통화내용을 암호화해야 한다.
○ 요구사항 설명: 음성 도청 보안위협으로부터 이용자의 프라이버시를 보호하기 위해서 mVoIP 소프트웨어는 통화내용을 암호화 하는 기능을 제공해야 한다. 이 때, 통화내용이라 함은 모든 음성통화를 의미하며, 영상통화에 암호화 기능의 지원여부는 mVoIP 소프트웨어 개발사의 선택사항이다. 암호화기술은 VoIP 보안기술인 SIP 메시지 암호화, RTP 메시지 암호화기술 등이 적용될 수 있다.

6. 메시지 암호화

○ 요구사항: mVoIP 소프트웨어는 응용·부가 서비스의 하나로 제공되는 메시징 서비스에서 주고받는 모든 메시지를 암호화해야 한다.
○ 요구사항 설명: 메시징 서비스는 거의 모든 mVoIP 소프트웨어가 제공하는 응용·부가 서비스이다. 메시지 도청 보안위협으로부터 이용자의 프라이버시를 보호하기 위해서 mVoIP 소프트웨어는 주고받는 모든 메시지를 암호화하는 기능을 제공해야 한다.

7. 제어 신호 보호

○ 요구사항: mVoIP 소프트웨어가 송수신하는 mVoIP 제어신호의 기밀성 및 무결성을 보장해야 한다.
○ 요구사항 설명: mVoIP 서비스는 VoIP 기술을 이용한다. 따라서 SIP 등 VoIP 서비스에 사용되는 기술이 사용된다. SIP 메시지의 위・변조를 통한 서비스 거부 공격, 세션 가로채기 공격 등은 이미 잘 알려져 있다. 이와 같은 SIP 메시지에 대한 보안위협은 암호화 등을 통해 SIP 메시지에 대한 기밀성 및 무결성을 보장함으로써 대응할 수 있다.

8. 스팸 차단

○ 요구사항: mVoIP 소프트웨어는 콜 스팸, 프레즌스 스팸 등 스팸시도를 차단할 수 있는 기능을 제공해야 한다.
○ 요구사항 설명: VoIP와 마찬가지로 mVoIP 역시 스팸유포의 주요 목표가 될 수 있다. mVoIP 소프트웨어는 스팸을 차단하기 위해서 필터링 등 필요한 기능을 제공해야 한다.

9. 악성코드 차단

○ 요구사항: mVoIP 소프트웨어와 mVoIP 제작업체 사이의 통신 구간에 악성코드가 침투하는 위협에 대해 대응수단을 제공해야 한다.
○ 요구사항 설명: mVoIP 제작업체는 공지사항 전파, 주소록 공유 등의 mVoIP 소프트웨어와 통신할 수 있다. 이 과정에서 공격자가 네트워크 해킹 등의 방법을 통해서 악성코드를 mVoIP 소프트웨어로 침입시킬 수 있다. mVoIP 제작업체는 이와 같은 보안위협을 최소화하기 위한 노력을 강구해야 한다. 이는 서버의 안전한 운영, 네트워크 구간에서 트래픽 암호화 등을 포함한다.

10. 사용자 인증

○ 요구사항: mVoIP 소프트웨어는 정당한 사용자의 mVoIP 서비스 이용을 보장하고, 비인가 사용자의 서비스 이용을 차단해야 한다.
○ 요구사항 설명: 본 보고서에서 수행한 테스트에서는 사용자 인증메커니즘을 우회하여 공격자가 정상적인 사용자로 위장하는 보안위협은 발견되지 않았다. 그러나 사용자 인증은 안전한 서비스 제공을 위한 가장 기본적인 정보보호 요구사항이라고 할 수 있어 포함되었다.

11. 암호 기술

○ 요구사항: mVoIP 소프트웨어는 암호화기술을 사용할 때 검증된 기술을 사용해야 한다.

○ 요구사항 설명: mVoIP 통신 내용 암호화, 중요정보 암호화 등을 위해서 사용되는 암호기술은 검증되고 충분히 안전한 알고리즘 등을 사용해야 한다. 이는 AES, SEED 등 검증된 암호 알고리즘이 사용되어야 하며, 키의 길이가 128비트 이상이어야 함을 의미한다. 또한 음성 암호화, 메시지 암호화, 중요정보 암호화 등 암호화기술이 적용될 때는 검증된 키 관리기법이 사용되어야 한다.

12. 프로토콜 구현의 정확성

○ 요구사항: mVoIP 소프트웨어는 SIP 등 VoIP 프로토콜을 국제 표준 규격에 맞게 정확하게 구현해야 한다.

○ 요구사항 설명: 이 요구사항은 SIP 메시지 플러딩 등의 공격에 대응하는 하나의 방편이다. 즉, mVoIP 소프트웨어 구현시 발생할 수 있는 구현 오류를 줄이는 것은 이와 같은 프로토콜 구현의 취약성을 이용한 위협으로부터 피해를 최소화하는 것이다.

제 4 장 mVoIP 정보보호 대응방안

○ mVoIP 정보보호 대응방안은 mVoIP 요구사항을 근거로 작성되며, 도청, 중요정보 유출, 서비스 거부 공격 등 정상적인 mVoIP 서비스를 방해하는 보안위협을 최소화하는 역할을 함

○ mVoIP 정보보호 점검항목을 통해 mVoIP 이용자를 보호하고 mVoIP 서비스 환경의 안전성을 제공하기 위해서 필요한 정보보호 대책이 조치되었는지 점검할 수 있음

○ *키워드: mVoIP 정보보호 조치, mVoIP 정보보호 점검항목*

제 1 절 mVoIP 정보보호 조치

1. 개요

본 장에서 설명하는 mVoIP 정보보호 조치는 mVoIP 소프트웨어 개발사가 실행할 수 있는 내용이다. 앞서 도출한 mVoIP 정보보호 요구사항을 근거로 (그림 4-1)과 같이 정보보호 대책을 도출하였다.

2. 사용자 인증

○ 관련 보안위협: 사용자 위장

○ 관련 정보보호 요구사항: 사용자 인증

○ 정보보호 조치: 비인가 사용자의 mVoIP 서비스 접근을 차단하기 위해서 사용자 인증은 필수적이다. 특히 mVoIP의 경우에는 앱을 통해서 전화 서비스를 이용하기 때문에 최초 로그인 과정을 반드시 거치는 경우가 대부분이다. 이에 따라 최소한 ID/패스워드 방식의 인증 메

커니즘을 적용함으로써 사용자 위장 보안위협을 최소화 해한다.

▶ 정당한 사용자인지 검증하기 위한 사용자 인증 메커니즘을 mVoIP 클라이언트에 적용해야 한다.

▶ 최소한 ID/패스워드 기반 인증 메커니즘을 적용해야 한다.

▶ ID/패스워드 기반 인증 메커니즘에서 mVoIP 클라이언트에서 서버로 ID/패스워드를 전송할 때 평문으로 전송해서는 안된다. 이 때, mVoIP 환경에서는 TLS(SSL) 이용이 권고된다.

(그림 4-1) mVoIP 정보보호 대책

3. 중요정보 암호화

○ 관련 보안위협: 중요정보 유출

○ 관련 정보보호 요구사항: 중요정보 암호화

○ 정보보호 조치: 중요정보는 mVoIP 소프트웨어의 DB 내에 저장되게 되며, DB는 스마트폰 등에 파일 형태로 저장된다. 중요정보의 보호를 위해서는 이와 같은 DB를 암호화해야 한다. 이 때, 외부의 공격자가 DB의 내용을 추측하는 것을 좀 더 어렵게 하기 위해서는 파일 이름(DB 이름)을 암호화하고 동시에 그 내용을 암호화해야 한다. 또한 ID/패스워드, 통화 기록 및 내용, 메시지 송수신 기록 및 내용 등의 중요정보는 DB에만 저장되는 것이 아니라, 디버그 등을 위해서 사용되는 로그 파일, 에러 메시지 등에도 기록될 수 있다. mVoIP 소프트웨어 개발자는 중요정보가 기록되는 모든 파일을 암호화해야 한다. 이 때, 암호화에 적용되는 기술은 앞서 살펴본 음성이나 메시지 암호화와 마찬가지로 검증된 알고리즘과 안전한 키 길이를 사용해야 한다.

한 편, 이와 같은 중요정보를 암호화하게 되면 이 정보를 다른 어플리케이션과 공유할 수 없음에 주의해야 한다. 스마트폰 등에서는 다른 어플리케이션과의 연동을 위해서 일부 정보는 스마트폰에 설치된 모든 어플리케이션이 접근할 수 있는 공유 DB에 기록할 수 있다. 그러나 암호화된 정보는 다른 어플리케이션과 공유될 수 없다.

▶ mVoIP 운용을 위해서 사용되는 앱 DB는 파일명을 포함해서 암호화해야 한다.

▶ 앱 DB 이외에도 기록 유지, 디버그 등을 목적으로 사용되는 로그 파일 등에도 중요정보가 포함될 수 있음으로 암호화 해야 한다.

▶ 이 때 안전성이 검증된 알고리즘(AES, SEED 등) 및 안전한 키 길이(128비트 이상) 사용이 권고된다.

▶ 또한 PC나 서버 등에 비해서 컴퓨팅 자원(CPU 속도, 메모리 용량)이 부족한 스마트폰에서 암호 알고리즘이 사용됨을 고려해야 스마트폰에 최적화된 암호 알고리즘 구현이 필요하다.

▶ 또한 암호화에 사용되는 암호키 관리 기법 역시 검증된 메커니즘이 사용되어야 한다.

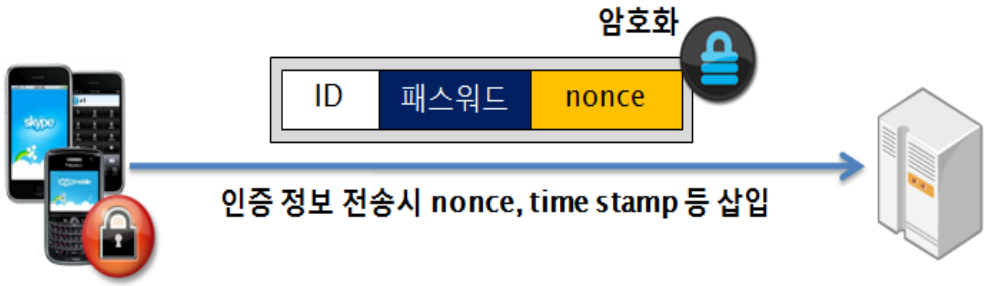
4. 사용자 인증정보 재사용 방지

○ 관련 보안위협: 인증정보 재사용

○ 관련 정보보호 요구사항: 인증정보 재사용 방지

○ 정보보호 조치: 인증정보 재사용 보안위협은 공격자가 mVoIP 서비스 운용에 사용되는 인증정보를 탈취하여 이를 재사용하여 정상이용자의 서비스를 사용하는 것을 의미한다. 예를 들어 암호화된 계정 및 패스워드 정보를 탈취하여 그 내용을 파악하지 못한다 하더라도 다른 스마트폰이나 PC에 복사하여 정상이용자로 위장하여 mVoIP 서비스에 로그인할 수 있다.

이와 같은 보안위협을 최소화하기 위해서는 인증정보가 사용될 때, 재사용이 불가능한 정보를 함께 사용해야 한다. 예를 들어 ID/패스워드와 함께 시각정보, 난수 등을 함께 사용하면 재사용 위협을 최소화할 수 있다((그림 4-2) 참조).



(그림 4-2) 인증정보 재사용 방지 기법

▶ 인증정보를 사용할 때, 공격자가 ID/패스워드를 모르는 상태에서 암호화된 결과만을 재사용해서 인증에 성공하지 못하도록 해야 한다.

▶ 이를 위해서는 암호화된 ID/패스워드를 보낼 때마다 그 값이 다르도록 해야 한다. 임의의 값(nonce), 타임스탬프 값 등을 사용해서 이와 같이 구성할 수 있다.

5. 음성 암호화(네트워크)

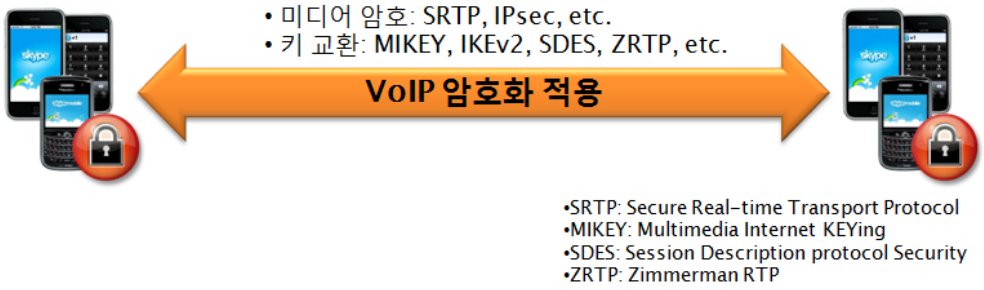
○ 관련 보안위협: 음성 도청

○ 관련 정보보호 요구사항: 음성 암호화

○ 정보보호 조치: 네트워크상에서의 통화 내용 도청을 방지하기 위해서 모든 음성통화를 암호화해야 한다. 기술적으로는 VoIP 프로토콜에서 통화내용을 전달하는 역할을 하는 RTP(Real-time Transport Protocol) 수준에서 데이터를 암호화해야 한다. 네트워크에서의 음성 암호화는 Wi-Fi 보안이 적용되는 것과 독립적으로 실시되어야 한다. 즉, Wi-Fi 보안 취약점으로 인해 무선 구간에서 Wi-Fi 보안이 적용되지 않는다고 가정하고 통화 내용을 암호화해야 한다((그림 4-3) 참조).

암호기술을 적용할 때는 검증된 암호 알고리즘 및 키 길이를 이용해야 한다. 예를 들어 SEED, AES 등은 검증된 알고리즘이다. 그리고 외부의 공격으로부터 안전성을 확보하기 위해서는 128비트 이상의 암호키를 사용해야 한다.

음성 암호화에는 mVoIP 미디어신호 암호화 이를 위한 키 관리 및 암호통신 호환성 보장 등이 포함된다. 또한 통화내용 보호를 위해서는 기본적으로 정당한 이용자만이 서비스를 이용할 수 있는 이용자 인증이 이루어지고 있음을 전제해야 한다.



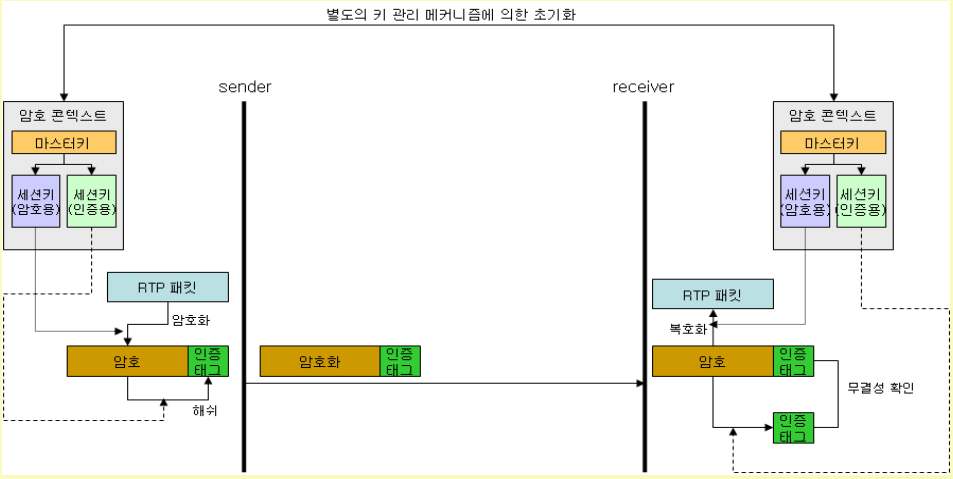
(그림 4-3) 음성 암호화

▶ 가장 대표적인 음성통화 암호기술은 SRTP이다.

▶ SRTP는 RTP 트래픽과 RTP에 대한 관리 트래픽인 RTCP (Real-time Transport Control Protocol)에 대해서 기밀성, 메시지 인증 및 재전송 방지 등의 보안서비스를 제공하는 RTP의 확장이다.

▶ SRTP는 이와 같은 보안서비스를 제공함과 동시에 실시간 트래픽의 특성을 고려하여 보안서비스를 위해서 필요한 부하를 최소화하여 높은 성능을 보장하는 것으로 목표로 하고 있다.

▶ SRTP의 구조는 (그림 4-4)와 같다. RTP 패킷에 대해서 암호 및 해쉬함수를 적용하여 SRTP 패킷을 생성해내는 비교적 간단한 구조로 구성된다.



(그림 4-4) SRTP 구조

6. 레코딩 API 차단

○ 관련 보안위협: 음성 단말 도청

○ 관련 정보보호 요구사항: 레코딩 API 차단

○ 정보보호 조치: mVoIP는 기존 유선 VoIP와는 달리 단말에서의 음성 도청위협이 매우 높다. 단말에서의 음성도청은 스마트폰 등에서 제공되는 녹음(recording) API를 사용해서 이루어진다. 음성도청이 성공하기 위해서는 통화 시작시점과 종료시점을 정확하게 알 수 있어야 하며, 녹음 API에 접근이 가능해야 한다. 일반적인 경우, 통화 시작시점과 종료시점은 mVoIP 소프트웨어가 기록하는 로그로 파악이 가능하다. 이와 같은 로그는 사용자에게 통화 기록을 제공하기 위해서 기록이 불가피하다. 따라서 단말에서의 도청을 막기 위해서는 녹음 API를 사용하지 못하도록 설정해야 한다((그림 4-5) 참조).

단말에서의 음성 암호화 역시 기본적으로 정당한 이용자만이 서비스를 이용할 수 있는 이용자 인증이 이루어지고 있음을 전제해야 하며, mVoIP 미디어 신호 암호화 이를 위한 키 관리 및 암호통신 호환성 보장 등이 포함된다.

(그림 4-5) 단말 도청 방지방안

▶ 현재, 단말 도청을 방지하기 위해서는 악성코드가 레코딩 API에 접근하지 못하도록 차단하는 방법을 사용해야 한다.

▶ 또는 악성코드가 음성통화 시작시점과 종료시점을 알지 못하도록 할 수도 있다.

▶ 기본적으로 악성코드에 의한 단말 음성 도청을 방지하기 위해서는 악성코드 설치를 차단할 수 있는 수단을 강구해야 한다.

7. 메시지 암호화(네트워크)

○ 관련 보안위협: 메시지 도청

○ 관련 정보보호 요구사항: 메시지 암호화

○ 정보보호 조치: mVoIP의 응용·부가 서비스의 하나인 텍스트 메시지 전송은 VoIP 프로토콜을 이용하지 않는다. 따라서 네트워크에서 메시지 도청 보안위협에 대응하기 위한 메시지 암호화는 음성 암호화와는 다른 기술을 사용해야 한다. 메시지는 인터넷 기술(TCP/IP)을 통해서 전송된다. 따라서 메시지 보호를 위해서 적용할 수 있는 가장 일반적인 기술은 TLS(Transport Layer Security)이다((그림 28) 참조). 네트워크에서의 메시지 암호화 역시 Wi-Fi 보안이 적용되는 것과 독립적으로 실시되어야 한다. 즉, Wi-Fi 보안 취약점으로 인해 무선 구간에서 Wi-Fi 보안이 적용되지 않는다고 가정하고 텍스트 메시지 내용을 암호화해야 한다. 메시지 암호화 역시 기본적으로 정당한 이용자만이 서비스를 이용할 수 있는 이용자 인증이 이루어지고 있음을 전제해야 한다.

(그림 4-6) 메시지 암호화 방안

▶ mVoIP에서의 암호화는 기본적으로 인터넷에서의 데이터 보호 메커니즘과 동일한 방식으로 동작한다.

8. mVoIP 관리 메시지 보호

○ 관련 보안위협: 서비스 거부 공격, 세션 가로채기

○ 관련 정보보호 요구사항: mVoIP 관리 메시지 암호화

○ 정보보호 조치: mVoIP 관리 메시지는 VoIP 프로토콜에서 사용되는 SIP 메시지를 의미한다. mVoIP 관리 메시지가 보호되지 않으면, 공격자가 관리 메시지를 조작하여 서비스를 불능상태로 만들거나 다른 사용자로 위장하는 공격 등이 가능하다.

따라서 통화내용이나 메시지 암호화와 함께 mVoIP 관리 메시지에 대한 기밀성 및 무결성이 보장되어야 한다. 이는 VoIP 기술에서 제공되는 관리 메시지 암호화기법을 적용함으로써 가능하다.

또한 mVoIP 클라이언트는 수신되는 mVoIP 관리 메시지가 관련 규격에 적합한지 그렇지 않은지 여부를 판단하여 적합하지 않은 메시지를 차단하는 mVoIP 관리 메시지 필터링 기능을 제공해야 한다.

▶ 관리 메시지 보호라 함은 VoIP SIP 메시지 보호를 의미한다.

▶ 즉, SIP 메시지에 대한 암호화를 통하여 홉간 신뢰구간을 형성하며, SIP 메시지의 기밀성과 무결성을 제공해야 한다.

▶ 이는 TLS 또는 IPSec, S/MIME 등의 정보보호 메커니즘을 통해서 제공 가능하다. TLS와 IPSec의 경우에는 홉간 보안을 보장하며, 종단간 보안을 위해서는 S/MIME을 사용할 수 있다.

9. 스팸 차단

○ 관련 보안위협: mVoIP 콜 스팸, mVoIP 프레즌스 스팸

○ 관련 정보보호 요구사항: 중요정보 재사용 방지

○ 정보보호 조치: mVoIP 스팸은 기존의 휴대폰 스팸과 e-mail 스팸의 특성을 모두 가지고 있으며, 인터넷에 접속할 수 있는 모든 곳에서 발송이 가능하다. 또한 웜・바이러스와 결합하는 경우, 그 피해는 더욱 커질 수 있다.

▶ 스팸 보안위협을 최소화하기 위해서는 기술적 보호조치와 관리적 보호조치가 함께 수행되어야 한다. 이를 위해서 mVoIP 제작업체에서 취할 수 있는 세부적인 조치는 다음과 같다.

▶ 서비스 제공자는 mVoIP 클라이언트에서 이용자의 불법스팸 간편 신고가 활용 가능하도록 해야 한다.

▶ 서비스 제공자는 이용자가 스패머를 차단할 수 있도록 블랙리스트 설정 기능이나 스패머 신고 및 처리 등이 가능하도록 관련 인프라를 제공해야 한다.

▶ 서비스 제공자는 한국인터넷진흥원 등 정부기관과 협조하여 불법 스팸정보에 대한 공유체계를 마련한다.

▶ 서비스 제공자는 이용자에게 서비스 이용시 유의사항 및 대처요령에 대한 가이드를 공지한다.

▶ 스팸차단 보안대책에는 메시지 콘텐트 검사, 스팸 간편 신고시스템, 블랙리스트 관리, 화이트리스트 관리, 스팸 전송패턴 탐지, 스팸 피해사례 전파 등이 포함된다.

10. 악성코드 차단

○ 관련 보안위협: 악성코드 전파

○ 관련 정보보호 요구사항: 악성코드 차단

○ 정보보호 조치: 공지사항 전파, 환경설정 전파 등의 목적으로 mVoIP 클라이언트와 mVoIP 클라이언트 제작업체 간의 직접적인 통신이 이루어질 수 있다. 이 과정에서 악성코드가 이용자의 단말로 전파될 수 있다. 이러한 보안위협을 최소화하기 위해서 mVoIP 클라이언트 제작업체는 자신의 서버를 보호해야 하며, 네트워크 보안 기술을 적용해야 한다. 여기서 서버보호는 기본적인 시스템 보안을 의미하며, 네트워크 보호는 TLS 등 네트워크 보안 프로토콜을 적용하는 것을 의미한다.

▶ 악성코드 차단의 가장 기본적인 대처방안은 mVoIP 소프트웨어 제작업체의 서버를 외부의 공격으로부터 안전하게 보호하여 제작업체 서버로부터 악성코드 전파가 불가능하도록 하는 것이다.

▶ 이를 위해서 제작업체는 방화벽 등 보호수단을 적용해야 한다.

▶ 이와 함께 스마트폰용 악성코드 탐지 프로그램의 개발 및 보급이 활성화되어야 한다. 스마트폰용 악성코드 탐지 프로그램을 통해서 단말 도청 등 다른 보안위협도 함께 해결할 수 있다.

11. mVoIP 정보보호 대책 요약

mVoIP 정보보호 요구사항을 반영하고 보안위협에 대처하기 위한 mVoIP 정보보호 대책은 다음과

[표 4-1] mVoIP 정보보호 대책 요약

위협 / 보안대책	LAN 도청 (음성/메시지 네크워크 도청)	단말 도청	세션 가로 채기	서비스 거부	Call 스팸	IM 스팸	프레즌스 스팸	사용자 위장
제어신호 암호	O		O					
미디어 신호 암호	O							
키 관리	O							
사용자 인증	O							O
간편신고 시스템								
블랙/화이트 리스트 관리					O	O	O	
스팸 피해사례 전파					O	O	O	
레코딩API 차단		O			O	O	O	
앱DB 암호화								
로그 파일 암호화								
중요정보 사용시 nonce 활용								
제어신호 필터링				O				
표준 규격 구현				O				
악성코드 차단								

제 2 절 mVoIP 정보보호 점검항목

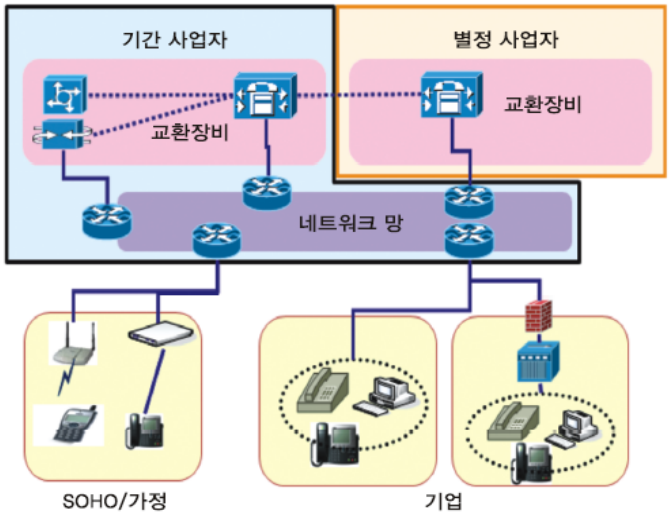
본 절에서는 mVoIP 이용자를 보호하고 mVoIP 서비스 환경의 안전성을 제공하기 위해서 필요한 정보보호 대책이 조치되었는지 점검할 수 있는 점검목록을 제공한다.

일련번호	분류	점검내용
1	사용자 인증	최소한 ID/패스워드에 의한 사용자 인증 기능을 제공하는가?
2		ID/패스워드를 이용한 사용자 인증 기능을 제공하는 경우, ID/패스워드 보호 메커니즘(예: TLS)이 적용되는가?
3		ID/패스워드를 이용한 사용자 인증 기능을 제공하는 경우, 충분히 복잡한 패스워드(예: 8자 이상의 패스워드 요구, 특수문자 요구 등)의 입력을 요구하는가?
4		ID/패스워드를 이용한 사용자 인증 기능을 제공하는 경우, 패스워드 입력 횟수 제한 기능을 제공하는가?
5	중요정보 암호화	앱 DB, 로그 파일 등 중요정보가 저장되는 파일 이름의 암호화 기능이 제공되는가?
6		앱 DB, 로그 파일 등 중요정보가 저장되는 파일 내의 정보가 암호화되는가?
7	사용자 인증 정보 재사용 방지	사용자 인증 과정에서 사용되는 인증 정보의 재사용 방지를 위한 메커니즘이 적용되고 있는가?
8	레코딩 차단	단말에서 레코딩 API 차단을 통해 음성 녹음을 방지하는가?
9		레코딩 API를 차단하지 않는 경우, 다른 음성 녹음 방지 대책이 적용되고 있는가?
10	음성 암호화	무선랜 구간에서의 도청 방지를 위한 트래픽 암호화를 적용하고 있는가?
11		mVoIP 소프트웨어 내에 음성 암호화 기능을 설정/해제하는 기능을 제공하는가?
12		mVoIP 소프트웨어 내에 음성 암호화 기능을 설정/해제하는 기능을 제공하지 않는 경우, 음성은 항상 암호화 되는가?

13		음성이 암호화되지 않는 경우, 이에 대한 경고 메시지를 출력하는가?
14	메시지 암호화	무선랜 구간에서의 도청 방지를 위해 메시지 암호화를 적용하는가?
15		mVoIP 소프트웨어 내에 메시지 암호화 기능을 설정/해제하는 기능을 제공하는가?
16		mVoIP 소프트웨어 내에 메시지 암호화 기능을 설정/해제하는 기능을 제공하지 않는 경우, 음성은 항상 암호화 되는가?
17		메시지가 암호화되지 않는 경우, 이에 대한 경고 메시지를 출력하는가?
18	제어신호 보호	mVoIP 클라이언트 소프트웨어가 비정상적인 mVoIP 메시지를 오류 처리할 수 있는가?
19		mVoIP 클라이언트 소프트웨어가 사용하는 mVoIP 제어 신호에 암호화가 적용되는가?
20	스팸 차단	단말 내에 스팸 차단을 위한 관리 기능이 제공되는가? 이는 스팸 신고, 필터링 등을 포함한다.
21	악성코드 차단	악성코드를 차단하기 위하여 mVoIP와 통신하는 서버의 시스템 보안 및 네트워크 보안이 이루어지고 있는가?
22		mVoIP 소프트웨어가 제작업체의 서버와 통신할 때, 서버 인증을 수행하는가?
23		mVoIP 클라이언트 소프트웨어의 주기적인 보안 점검 및 패치가 이루어지고 있는가?
24	정확한 프로토콜 구현	mVoI 소프트웨어가 VoIP 기술을 구현하는데 있어서 국제/국내 표준 규격을 정확하게 적용하였는가?
25	사용된 암호기술	사용된 암호기술은 검증된 알고리즘과 안전한 크기의 키를 사용하고 있는가?
26		사용된 암호기술에서 검증된 키 관리 기법을 적용하고 있는가?
27		mVoIP 클라이언트 소프트웨어에서 사용자가 암호화 알고리즘을 선택하는 기능을 제공하는가?
28		mVoIP 클라이언트 소프트웨어에 대한 보안 적합성 검토가 수행되었는가?

제 5 장 VoIP 사업자 보안모델

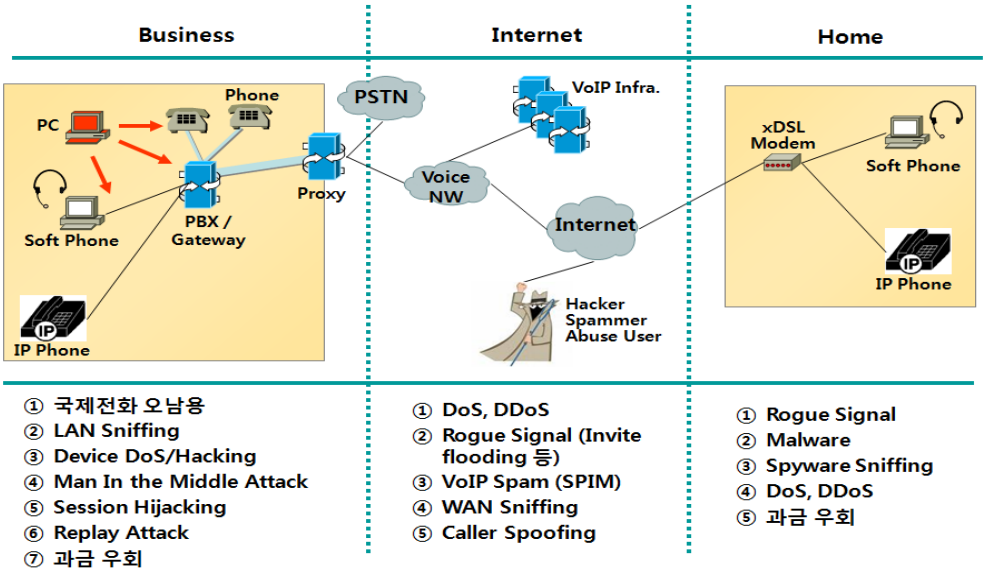
제 1 절 VoIP 서비스 사업자 구분



(그림 5-1) VoIP 서비스 사업자 구분

VoIP를 서비스하는 사업자는 기간 사업자와 별정 사업자로 구분되는데 기간 사업자란 인터넷망(백본망, 가입자 망 등)과 VoIP 설비(서버, 라우터, G/W, G/K 등)를 설치/보유하고 이를 이용하여 인터넷전화 기간통신역무를 제공하는 사업자를 말한다. 별정 사업자는 별정 1호와 별정 2호로 구분되는데 별정 1호 사업자는 PSTN망과 접속 또는 연동할 수 있는 G/W와 G/K, 프록시(Proxy) 서버, 소프트스위치(SSW) 등 호처리용 교환설비를 자체보유하고, 기간통신사업자의 전기통신회선설비 등을 이용하여 인터넷전화 기간통신역무를 제공하는 사업자를 말한다. 별정 2호 사업자는 자체적인 교환설비를 보유하지 않고, 기간통신사업자의 통신회선설비 및 기간/별정통신사업자의 교환설비를 이용하여 인터넷전화역무를 제공하는 사업자를 말한다.

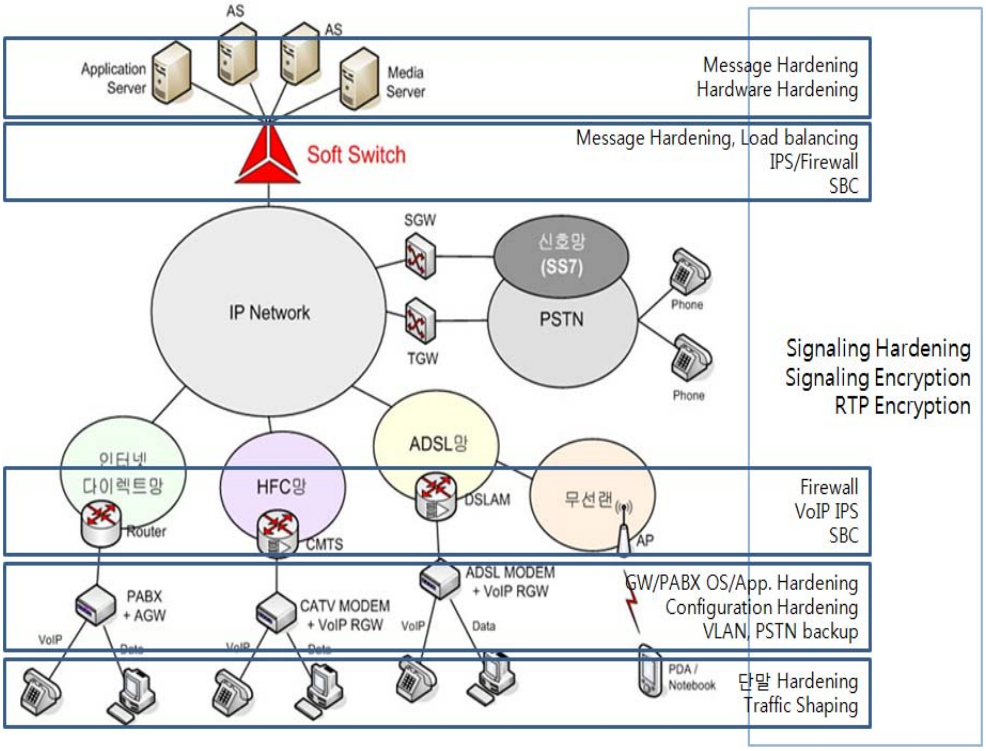
제 2 절 VoIP 보안위협



(그림 5-2) VoIP 보안위협

VoIP에 대한 보안위협에는 도청, 서비스 거부 공격, 서비스 오용 공격, VoIP 스팸을 들 수 있다. 도청이란 호 설정 메시지나 통화내용을 중간에 가로채는 것을 말한다. 서비스 거부 공격은 DoS/DDoS 공격수단으로 SIP 메시지를 사용해 VoIP 시스템의 자원을 고갈하거나 통화 시도 중이거나 통화 중인 단말에 SIP 메시지(BYE, CANCEL)를 전송하여 통화를 방해하는 공격을 말한다. 서비스 오용 공격은 정상적인 사용자의 등록정보 등을 위조하여 시스템을 불법적으로 사용하는 것을 말하며, VoIP 스팸은 자동화된 도구를 이용하여 불특정 다수에게 스팸전화를 발송하는 공격방법이다.

제 3 절 VoIP 사업자 보안모델



(그림 5-3) VoIP 사업자 보안모델

(그림 5-3)은 앞서 2절에서 설명한 VoIP 보안위협들을 방어하기 위한 보안모델을 도식화한 것이고, [표 5-1]은 보안위협에 대한 사업자별 보호대책을 설명한 표이다.

[표 5-1] 보안위협에 대한 사업자별 보호대책

보안위협	기간사업자 보호대책	별정사업자 보호대책
DDoS	VoIP-IPS+F/W+SBC 구축 DDoS 전용장비 도입 Sink hole, Rate-limit 회선 이중화	Sink hole, Rate-limit 회선 이중화

도청	암호화(TLS, SRTP)	암호화(TLS, SRTP)
서비스 오용	사용자 인증 강화 Topology Hiding 기기인증서 기반 기기인증	사용자 인증 강화
VoIP 스팸	VoIP-IPS, SBC 구축 Black/White list	Black/White list

1. DDoS 대응방안

[표 5-1] DDoS 대응방안

위협	대응방안	대상
DDoS	교환시스템인증	교환시스템, 단말
	불법 메시지 차단(단말)	단말
	MAC 주소인증 및 접근차단	랜 네트워크(독립시스템)
	VoIP 방화벽	사업자, 랜 네트워크
	기존 방화벽	랜, 사업자 네트워크
	불법 메시지 차단(서버)	기타 서버
	스푸핑 방지	라우터
	악의적 VoIP 공격 탐지	사업자, 랜 네트워크
	웜・바이러스 탐지/차단	단말, 서버
	시스템 장애 탐지/대응	서버
	중요시스템 이중화	사업자, WAN
	음성망 분리	랜, 사업자 네트워크
	우회경로 확보	백본네트워크
	트래픽 대역폭 제한	라우터 등 네트워크 장비
	트래픽 모니터링(관제)	사업자 네트워크
	통합관리	사업자 네트워크

2. 도청 대응방안

[표 5-2] 도청 대응방안

위협	대응방안	대상	비고
도청	제어신호 암호	교환시스템, 단말	TSL, IPSec
	미디어 신호 암호	교환시스템, 단말	SRTS
	사용자 인증	인증, 교환시스템, 단말	
	메시지 인증	교환시스템, 단말	
	MAC 주소인증 및 접근차단	랜	
	불법 메시지 차단(단말)	단말	
	보안패치 및 안티바이러스	단말, 교환시스템	
	웜・바이러스 탐지/차단	단말, 교환시스템	
	시스템 장애 탐지/대응	단말, 교환시스템	
	음성망 분리	사업자, LAN	논리적인 분리(사설망, VAN)
	더미허브 사용금지	랜	

3. VoIP 스팸 대응방안

[표 5-3] VoIP 스팸 대응방안

위협	대응방안	대상	비고
스팸	간편신고 시스템	사업자 네트워크, 단말	독립시스템
	제어 메시지 컨텐츠 검사	교환시스템, 독립시스템	IM, Presence 스팸
	스팸 차단	사업자 네트워크	블랙, 화이트 리스트
	스팸 전송 탐지/대응	사업자, 랜 네트워크	독립시스템

4. 세부 대책

[표 5-4] 보안위협 별 세부대책

대상	대책	기본	강화
단말	암호	제어신호 암호	미디어신호 암호
		관리신호 암호	키관리(음성 암호키)
			암호통신 호환성보장
	인증	사용자 인증	
		관리자 인증	
	접근제어	불법메시지 차단(단말)	교환시스템 인증/차단
		단말 관리시스템 인증/차단	
	침입탐지/대응	보안 취약점 점검	웜바이러스 탐지/차단
	스팸대응	간편신고	
교환 시스템	암호	제어신호 암호	키관리(음성 암호키)
		관리신호 암호	암호통신 호환성보장
	인증	사용자 인증	
		관리자 인증	
	접근제어	불법메시지 차단(교환시스템)	교환시스템 인증/차단
			발신경로 인증/차단
	침입탐지/대응	웜바이러스 탐지/차단	악의적 컨텐츠 탐지/차단
		보안 취약점 점검	
		감사 및 레포팅	
네트워크	암호	관리신호 암호	

장비	인증	관리자 인증	
	접근제어	네트워크 장비 접근제어	
		스푸핑 패킷차단	
		널라우팅(Black Hole)	
		트래픽 제한	
	침입탐지/대응	보안 취약점 점검	
		감사 및 레포팅	
LAN	접근제어	침입차단(기존 방화벽)	MAC 주소인증 및 접근차단
		사설망	VLAN
		스위치 시스템 적용	VoIP 방화벽
	침입탐지/대응	침입탐지(기존 IDS)	VoIP 공격 탐지
사업자 네트워크	접근제어	침입차단(기존 방화벽)	VoIP 방화벽
			논리적 망분리(VLAN)
	침입탐지/대응	침입탐지(기존 IDS)	VoIP 공격 탐지
		중요시스템 이중화(교환장비)	VoIP 트래픽관제
			VoIP 보안 통합관리
	스팸대응		스팸 탐지 (Call, IM, Presence)
			스팸 차단
			블랙리스트 관리 및 전파
WAN 네트워크	접근제어	침입차단(기존 방화벽)	

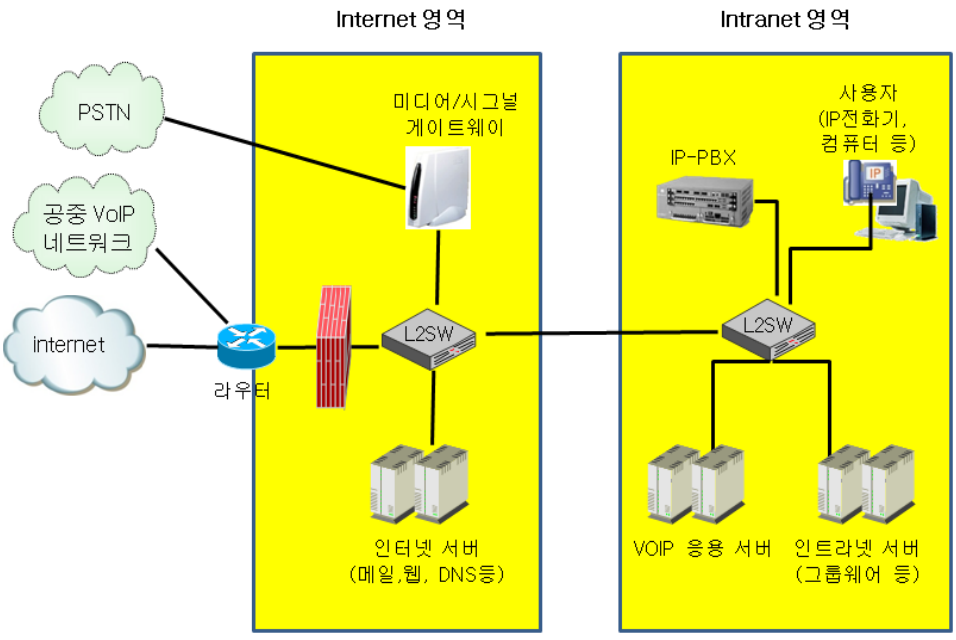
	침입탐지/ 대응	공격탐지 (비정상 트래픽)	음성데이터 차별대응
		우회경로 확보	
		중요시스템 이중화(라우터 등)	
		트래픽 관제 및 대응	
WAN 연동구간	접근제어	WAN 네트워크 인증/차단	
	침입탐지/ 대응	공격탐지 (비정상 트래픽)	음성데이터 차별대응
		우회경로 확보	
		중요시스템 이중화(라우터, 회선)	
		트래픽 관제 및 대응	
사업자 연동 구간	접근제어		사업자 네트워크 인증 /차단
	침입탐지/ 대응	침입탐지(기존 IDS)	VoIP 공격탐지
		중요시스템 이중화(교환장비, 회선)	VoIP 트래픽관제
			VoIP 보안통합관리

제 4 절 VoIP 서비스 보안모델

1. 소규모 기업 VoIP 구성 모델

소규모 기업은 동일 건물 및 장소에 위치한 기업을 말하며, VoIP 시스템 모델은 (그림 5-4)와 같이 구성된다. 안전한 VoIP 서비스를 위한 전체 시스템은 인터넷 영역과 인트라넷(내부망) 영역으로 나뉜다. 인터넷 영역에서, PSTN과 공중 VoIP 네트워크에 대한 인터페이스는 인터넷전화기 없이 일반적으로 소규모 네트워크에 부가된다. 인트라넷 영역에서, IP 전화기와 가상 LAN(Virtual LAN)이 제공된다.

인터넷 영역과 인트라넷 영역은 방화벽을 사용하여 논리적으로 분리한다. 인터넷에 연결된 엣지 라우터 및 방화벽 등은 보안사고 혹은 시스템 고장 등의 장애시 대역폭 확보 및 서비스 품질을 보장하고 지속적인 서비스를 제공하기 위해 이중으로 설치하는 것을 권고한다.



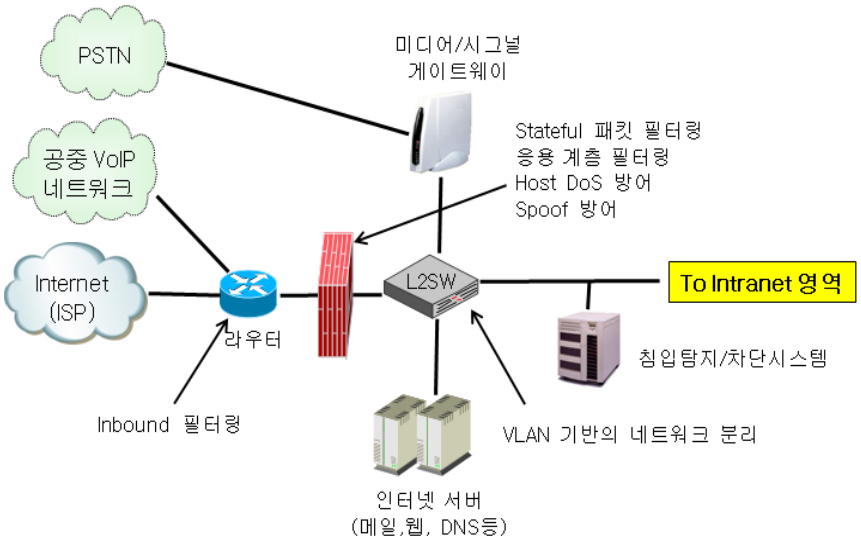
(그림 5-4) 소규모 기업 VoIP 모델

가. 인터넷 영역

인터넷 영역은 내부 사용자들이 인터넷, PSTN과 공중 VoIP 네트워크에 연결할 수 있게 해준다. 이 영역은 인터넷 서버(메일 서버, 웹 서버 등)상의 정보에 대한 내부 사용자의 접근을 제공하며, 데이터와 음성 네트워크를 분리해 준다.

인터넷 영역의 주요 구성요소는 (그림 5-5)와 같이 라우터, 방화벽(인터넷전화 기능 제공), 침입탐지/차단시스템 그리고 VoIP 게이트웨이(미디어/시그널 게이트웨이) 등이다.

기업 네트워크에 위치하는 엣지 라우터는 서비스 제공업자가 제공하는 연결 형태에 따라 다른 종류의 인터페이스를 가질 수 있다. VoIP 기능을 제공하는 방화벽은 자원에 대한 네트워크 레벨의 방어, 트래픽에 대한 stateful 필터링 그리고 음성 서비스를 제공한다. 가상 LAN(VLAN)을 제공하는 계층2 스위치(L2SW)는 계층 2 서비스를 데이터와 음성장치에 제공한다. 인터넷 서버와 VoIP 게이트웨이는 DMZ 영역에 위치한다. VoIP 게이트웨이는 PSTN과 연동하기 위해 설치된다.



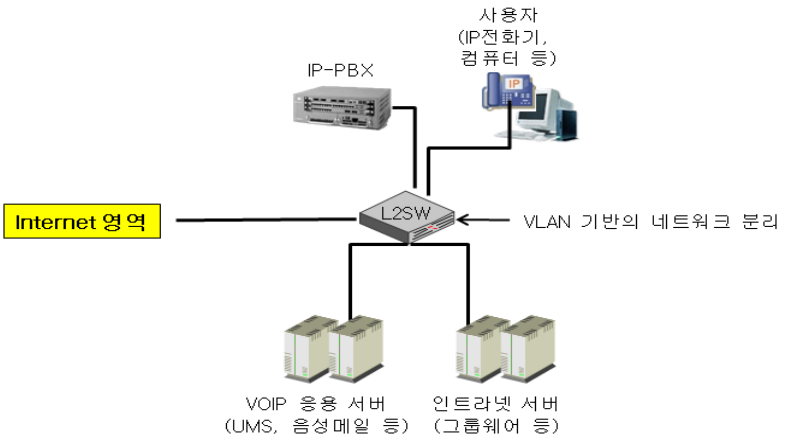
(그림 5-5) 소규모 기업용 인터넷영역 구성도

나. 인트라넷 영역

인트라넷 영역은 IP-PBX, VoIP 응용서버, IP 전화기 및 컴퓨터 등을 포함한다. 이 영역은 인터넷 영역을 통해 인터넷을 사용한다.

인트라넷 영역의 주요 구성요소는 (그림 5-6)과 같이 VLAN 기능을 제공하는 계층 2 스위치(L2SW), IP-PBX, VpIP 용용서버, PC 등이다.

이 영역에 있는 모든 엔터티는 계층 2 스위치를 통해 연결된다. 일반적으로 네트워크는 크게 2개의 네트워크, 즉 데이터와 음성 네트워크로 나뉜다. IP-PBX와 IP 전화기는 음성 네트워크에 포함되며, 응용서버와 사용자 PC는 데이터 네트워크에 포함된다.



(그림 5-6) 소규모 사무실용 인트라넷영역 구성도

2. 대규모 기업 VoIP 보안모델

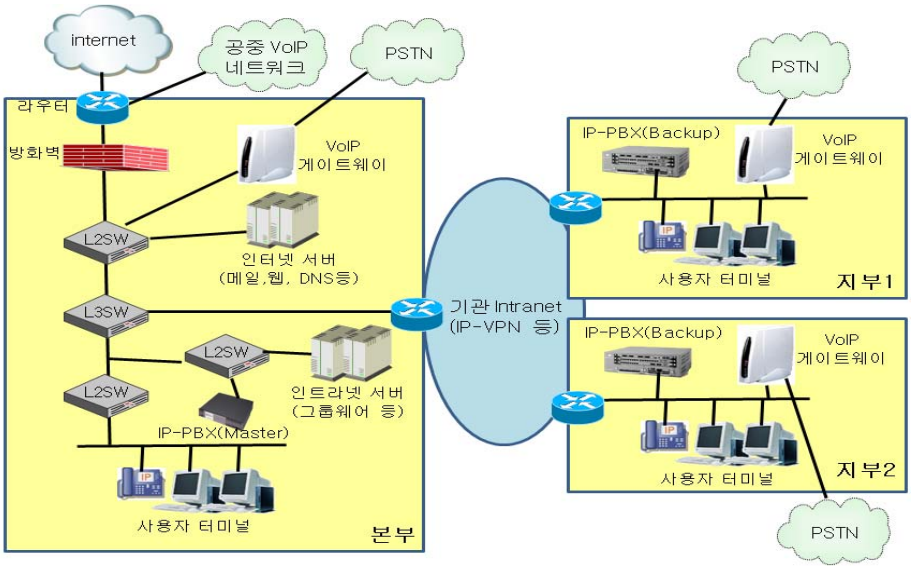
대규모 기업을 위한 VoIP 시스템 모델은 2가지로 나눌 수 있는데, 하나는 중앙집중형 IP-PBX 모델이고 다른 하나는 분산형 IP-PBX 모델이다. 중앙집중형 모델은 IP-PBX가 본부(본청) 혹은 데이터 센터와 같은 중앙의 하나의 장소에 설치된다. 지부(지청)의 직원들은 그들의 사무실에 별도의 IP-PBX를 설치할 필요 없이 원격지의 사무실에서 본부(본청)에 설치된

IP-PBX에 접근할 수 있다. 분산형 모델은 IP-PBX가 본부(본청) 및 지부(지청)에 각각 설치된다. 이들 모델의 각각은 장단점이 존재한다. 어떤 모델을 기업에 적용할 것인지는 해당 기업의 규모와 어떻게 VoIP를 운영할 것인지, VoIP의 보안 요구조건 등을 기반으로 선택한다.

인터넷과 인트라넷(내부망)을 방화벽을 이용하여 논리적으로 분리한다. 인터넷에 연결된 엣지 라우터 및 방화벽 등은 보안사고 혹은 시스템 고장 등의 장애 시 대역폭 화보와 서비스 품질을 보장하고 지속적인 서비스를 제공하기 위해 이중으로 설치하여야 한다.

가. 중앙 집중형 인터넷전화(IP-PBX) 모델

이 모델에서, VoIP 서비스는 본부에 설치된 IP-PBX와 서버들에 의해 제공된다. 119와 같은 긴급전화를 고려하여 본부 및 지부들은 PSTN 네트워크와 인터페이스를 가지고 있어야 한다. 이 모델의 전체 시스템 구성도는 (그림 5-7)과 같이 4개의 영역, 즉 인터넷 영역, 중앙 서버 팜, 본부 그리고 지부로 나뉜다.

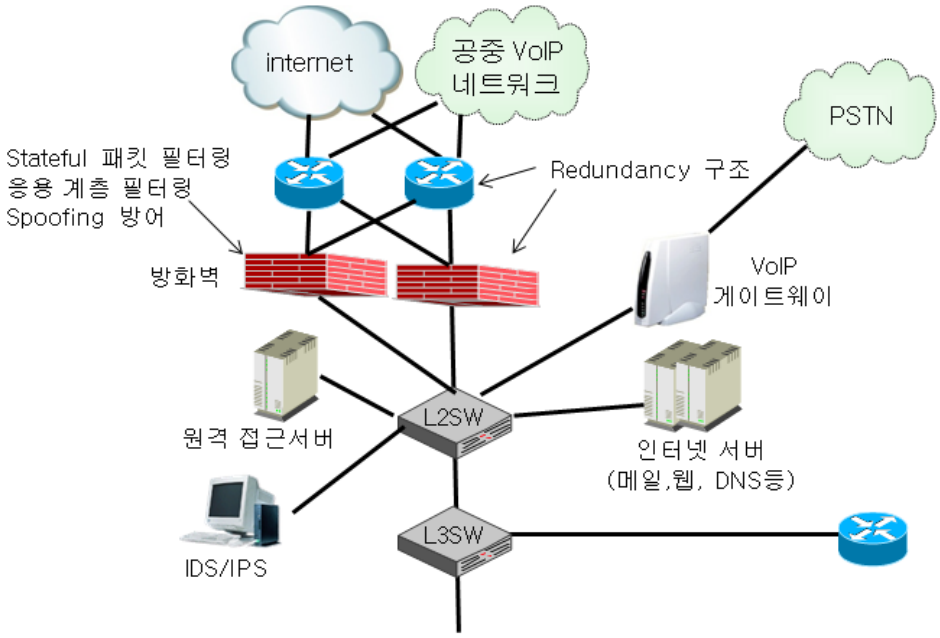


(그림 5-7) 중앙집중형 IP-PBX 모델

(1) 인터넷 영역

인터넷 영역은 내부 사용자들에게 인터넷, PSTN 그리고 공중 VoIP 네트워크와의 연결을 제공한다. 또한 내부 사용자들에게 인터넷 서버들 그리고 데이터와 음성 세그먼트 사이의 영역에 있는 정보에 대한 접근을 제공한다.

인터넷 영역의 주요 구성요소는 (그림 5-8)과 같이 VoIP의 인식 및 처리하는 방화벽, 네트워크 기반의 IDS/IPS 등의 보안시스템, 원격지 접근서버 등이다.



(그림 5-8) 중앙집중형 모델의 인터넷영역

이 영역내의 구성요소는 소규모 VoIP 구성 모델의 인터넷 영역과 유사하다. 기업이 크면 클수록 VoIP 시스템의 사용효과는 훨씬 더 크게 된다. 이와 같은 경우, 몇몇 노드들은 보안사고 혹은 시스템 고장을 방지하

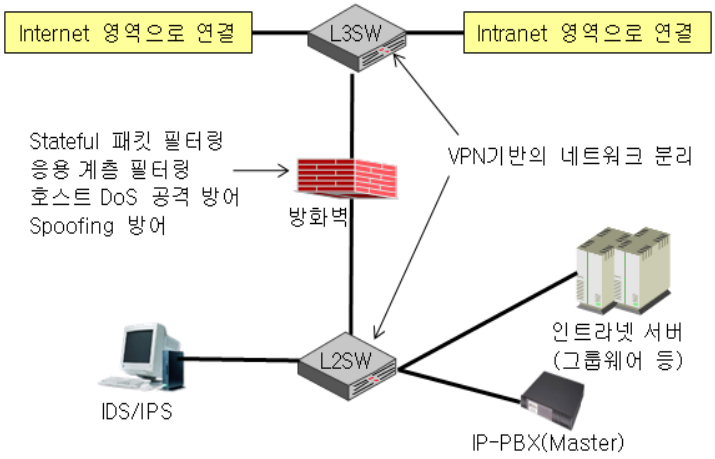
기 위해 이중으로 설치되어야 한다. 공개 가능한 인터넷 서버(웹 서버, 메일 서버 등)를 위한 IDS/IPS가 이미 설치되어 있을 때 몇 가지 경우가 존재한다. VoIP 트래픽은 존재하는 IP 네트워크 인프라구조를 통해 다른 외부경로가 생긴다. 따라서 IDS/IPS는 발생하는 공격과 부적합한 트래픽 흐름을 탐지해야만 한다. 만약 IDS/IPS가 네트워크에 없다면, IDS/IPS는 공격으로 인한 피해를 완화하기 위해 설치되어야 한다. 원격지 접근 서버는 이 영역에 설치될 수 있다. 인터넷으로부터 VoIP 시스템에 대한 사용자의 접근은 원격 접근 서버를 통해 허용된다. 이러한 통신 방법은 사용자들이 LAN(인트라넷)에 있다면 네트워크에 접근할 수 있게 허용한다.

(2) 기업의 서버 팜

기업 내부 사용자들이 사용하는 응용 서버들과 IP-PBX는 기업의 서버 팜 내에 설치된다. 기업의 보안정책에 의해 접근이 허용된 원격지 이동 근무자/재택근무자들을 제외한 인터넷 사용자들은 기업의 서버 팜에 직접적으로 접근할 수 없다.

이 영역의 주요 구성요소는 (그림 5-9)와 같이 VoIP(음성)를 지원하는 방화벽, 네트워크 기반의 IDS/IPS 같은 보안시스템, 계층3과 계층 2 스위치 등이다.

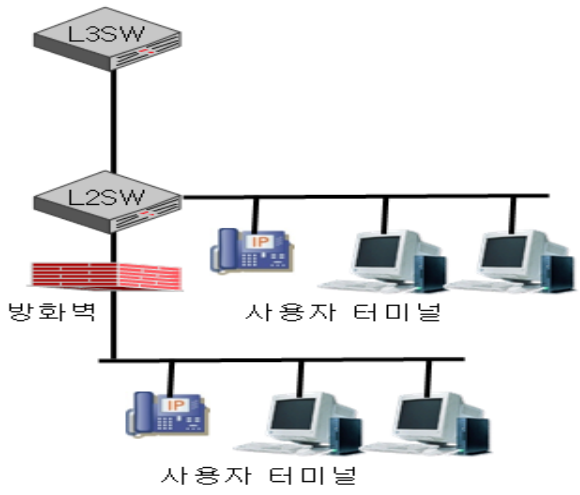
사용자에게 컴퓨터와 전화의 통합 응용을 제공하는 IP-PBX와 서버는 이 영역에 존재한다. 데이터 네트워크에 사용된 서버(그룹웨어 서버, 내부 메일서버 등) 또한 이 영역에 존재한다. 데이터와 음성 세그먼트는 논리적으로 혹은 물리적으로 분리되어야 한다. 만약 데이터와 음성이 물리적으로 분리될 수 없다면 VLAN 등과 같은 방법을 사용해서 논리적으로 분리하여야 한다.



(그림 5-9) 중앙집중형 모델의 기업서버 팜 구성

(3) 본부 사무실

본부 사무실은 기업의 본부 근무자의 사용자 터미널(IP 전화기 및 사용자 컴퓨터 등)을 위한 영역으로 (그림 5-10)과 같다. 몇몇 세그먼트는 전체 네트워크로부터 이 영역을 분리하기 위해 계층 3 스위치 혹은 라우터와 연결된다.



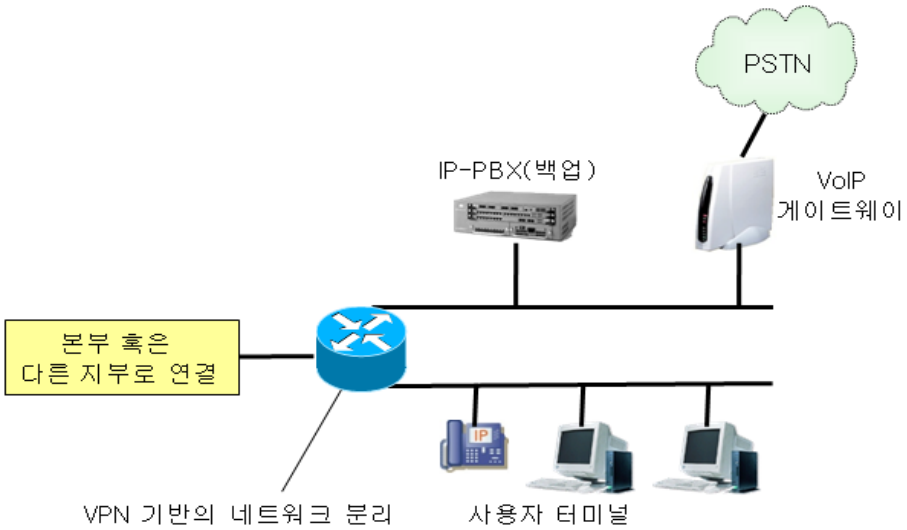
(그림 5-10) 중앙집중형 모델의 본부사용자 영역

(4) 지부

이 영역은 이 모델에서 원격지에 있는 기업의 사무실이다. 이 지부 사무실 영역의 주요 구성요소는 (그림 5-11)과 같이 IP-PBX(Backup), VoIP 게이트웨이, 사용자 터미널 등이다.

백업 IP-PBX는 본부의 서버 팜에 있는 IP-PBX를 위해 failover 리던던시를 제공하기 위해 사용될 수 있다. 이 영역의 네트워크는 서버와 클라이언트 네트워크로 나누어야 한다. 백업 IP-PBX와 VoIP 게이트웨이는 서버 영역에 설치되어야 한다. 라우터는 이 영역의 인입 단에 설치된다. 이 영역의 엣지 라우터는 VPN에서 제공한 연결 형태에 따라 다른 종류의 인터페이스를 가질 수 있다.

지부에는 두 개의 네트워크 세그먼트(서버와 클라이언트 세그먼트)가 존재하며, 방화벽은 서버 세그먼트 앞단에 설치될 수 있다. 만약 전체 지부가 다른 보안 레벨을 가지고 있다면, 방화벽은 지부 네트워크 앞단에 설치하는 것을 권고한다.

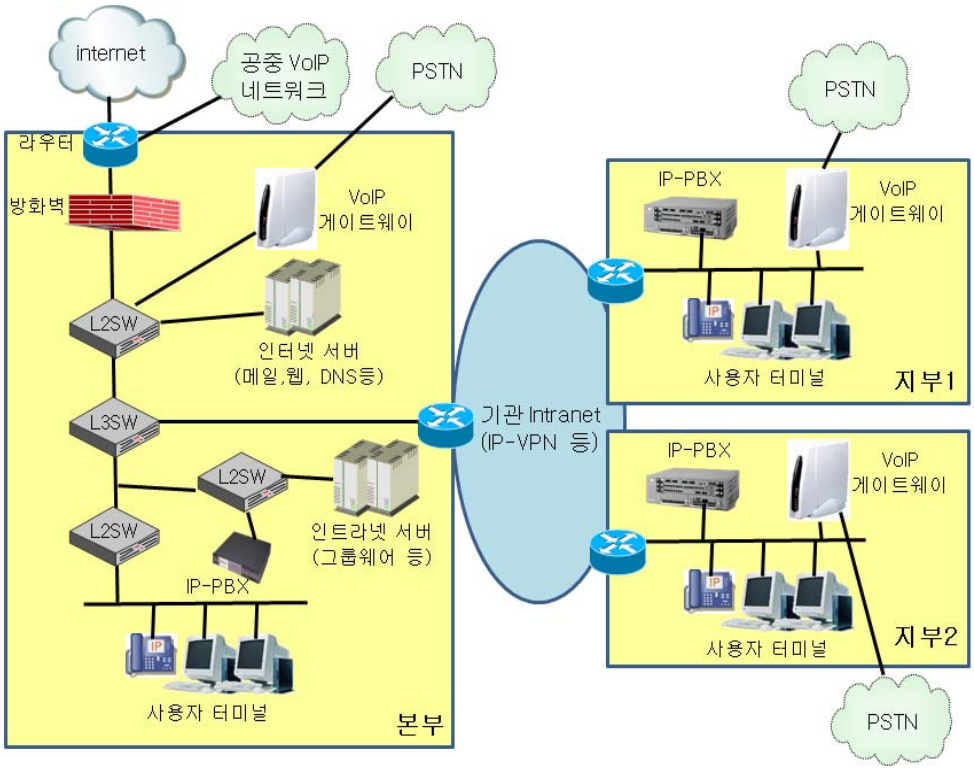


(그림 5-11) 중앙집중형 모델의 지부 구성도

나. 분산형 인터넷전화(IP-PBX) 모델

분산형 IP-PBX 모델의 보안 메카니즘은 중앙집중형 IP-PBX 모델과 거의 유사하다. 이 모델의 전체 구성도는 (그림 5-12)와 같다. 이 모델과 중앙집중형 모델과의 차이점은 다음과 같다.

- IP-PBX(그리고 관련 응용 서버들)는 지부에도 설치된다.
- 본부의 IP-PBX는 본부 사용자들을 위해 사용되며, 본부의 IP-PBX는 본부의 사용자들과 통신하며, 그리고 원격지 사무실에 있는 IP-PBX와 통신한다.



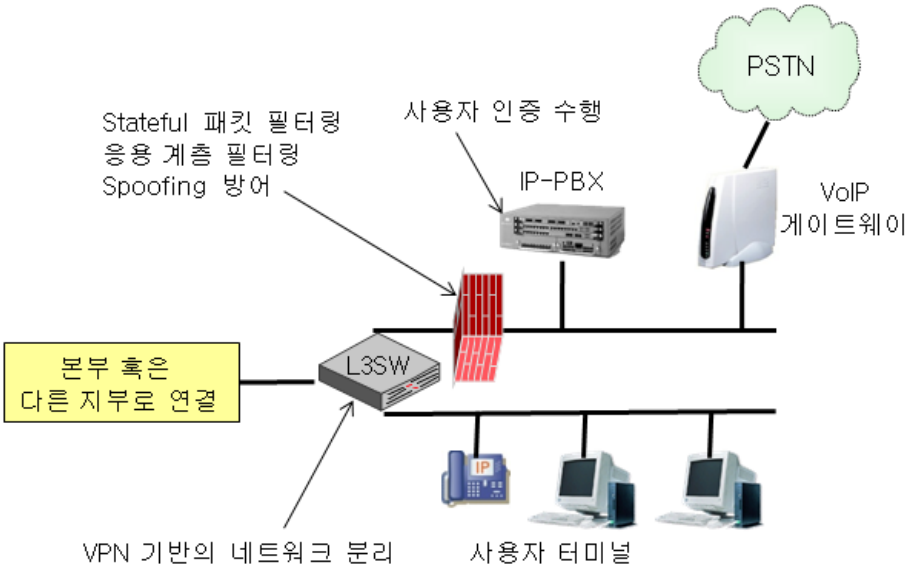
(그림 5-12) 분산형 IP-PBX 모델

(1) 지부(Branch Office)

분산형 IP-PBX 모델의 지부는 (그림 5-13)과 같이 구성된다. IP-PBX는 각 지부의 한곳에 설치된다. 이것이 중앙집중형 모델과의 주요 차이점이다. 분산형 모델의 지부는 소규모 VoIP 구성모델과 유사하지만, 이 모델에서는 인터넷과의 연결을 제공하지 않는다.

이 지부 영역의 주요 구성요소는 IP-PBX, VoIP 게이트웨이, 방화벽, VLAN을 제공하는 계층 2 스위치 등이다. IP-PBX와 VoIP 게이트웨이는 지부에 근무하는 사용자들에게 VoIP 서비스를 제공한다. 어떤 지부에 근무하는 사용자는 다른 지부 혹은 본부에 있는 사용자들과 통신하기 위해 자신의 지부에 설치된 IP-PBX에 연결된다.

사무실에는 두 개의 네트워크 세그먼트(서버와 클라이언트 세그먼트)가 존재하며, 방화벽은 서버 세그먼트 앞단에 설치된다. 만약 전체 지부가 다른 보안 레벨을 가지고 있다면, 방화벽은 지부 네트워크 앞단에 설치되어야 한다.



(그림 5-13) 분산형 모델의 지부 구성도

3. 물리적인 네트워크 분리기업의 VoIP 구성모델

기업의 네트워크를 다양한 위협으로부터 안전하게 운영하기 위해 인터넷 영역과 인트라넷(내부망) 영역을 물리적으로 분리한 기업에 적용하는 VoIP 구성모델이다. 기업 내부사용자들은 각각 인터넷 접속용 컴퓨터 그리고 인트라넷 접속용 컴퓨터를 별도로 설치하여 사용하는 환경이다. 이들 기업에서 VoIP 서비스는 인터넷 영역에 VoIP 시스템을 설치하여 제공하는 방법과 인트라넷 영역에 인터넷전화 시스템을 설치하여 제공하는 방법으로 나눌 수 있다.

물리적으로 네트워크를 분리한 기업의 특성은 다양한 위협으로부터 내부의 자원을 안전하게 보호하기 위해 보안을 우선으로 하는 정책을 가지고 있으며, VoIP 서비스도 물리적인 네트워크 분리 운영정책에 맞추어 제공하는 것이 타당하다. 따라서 VoIP의 보안위협으로부터 인트라넷을 안전하게 보호하기 위해서는 물리적으로 분리된 인터넷 영역에 VoIP 시스템을 구축하여 서비스를 제공하는 것이 바람직하다. 단, 기업 사용자들에게 인터넷 영역에서 VoIP 서비스를 안전하게 제공할 수 있는 별도의 보안대책을 강구하여야 한다.

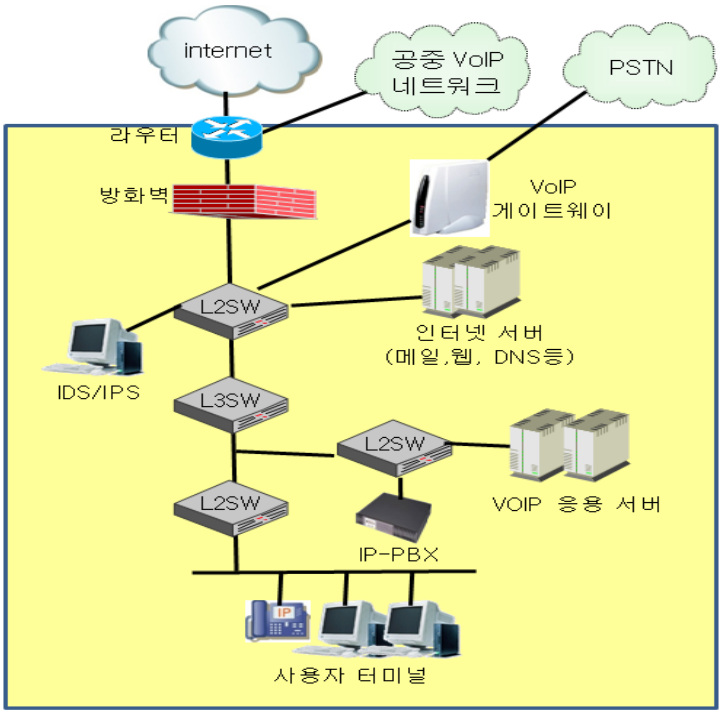
물리적으로 네트워크를 분리한 기업의 인터넷 접점에 설치된 방화벽은 안전한 VoIP 서비스 제공을 위해 VoIP를 인식 및 처리 가능한 응용계층 게이트웨이, stateful 패킷 필터링 및 spoofing 공격을 방어할 수 있어야 한다.

인터넷에 연결된 엣지 라우터 및 방화벽은 보안사고 혹은 시스템 고장 등의 장애 시 대역폭 및 서비스 품질을 보장하고 지속적인 서비스를 제공하기 위해 이중으로 설치되어야 한다.

가. 소규모 기업 VoIP 구성모델(인터넷 영역)

인터넷 영역과 인트라넷 영역을 물리적으로 분리한 소규모 기업의 VoIP 구성모델은 (그림 5-14)와 같다. (그림 5-14)는 소규모 기업의 인터넷

영역에 VoIP 시스템을 설치하여 사용자들에게 VoIP 서비스를 안전하게 제공하는 모델이다. 각 구성요소 및 용도 등의 자세한 사항은 앞에서 설명한 내용과 동일하지만, 단지 사용자들에게 VoIP 서비스를 제공하기 위한 VoIP 응용서버를 인터넷 영역의 안전한 장소에 설치한 것이 큰 차이점이다. 모든 사용자는 인터넷 영역에 설치된 IP-PBX를 통해 VoIP 서비스를 제공받는다.

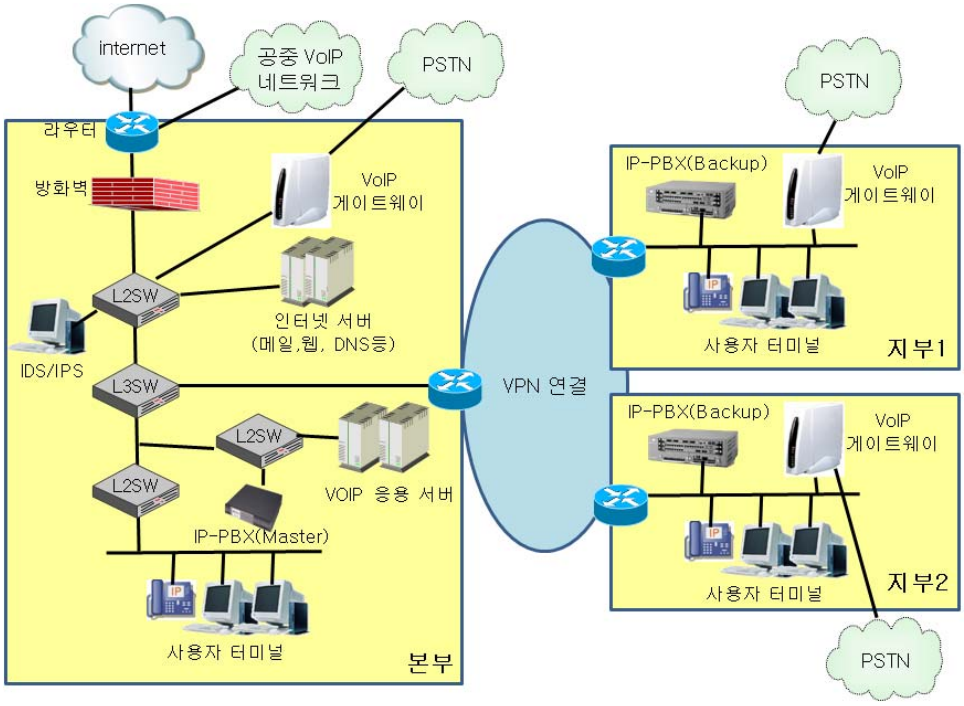


(그림 5-14) 소규모 기업의 VoIP 구성모델

나. 대규모 기업의 중앙집중형 VoIP 구성모델(인터넷 영역)

인터넷과 인트라넷을 물리적으로 분리한 대규모 기업의 중앙집중형 VoIP 구성모델은 (그림 5-15)와 같다. (그림 5-15)는 대규모 기업의 본부에 위치한 인터넷 영역에 VoIP 시스템을 설치하여 사용자들에게 VoIP 서비스를 안전하게 제공하는 모델이다. 각 구성요소 및 용도 등의 자세한 사항은

앞에서 설명한 중앙집중형 IP-PBX 구성모델과 동일하지만, 단지 사용자들에게 VoIP 서비스를 제공하기 위해 VoIP 응용서버를 인터넷 영역의 안전한 장소에 설치한 것이 큰 차이점이다. 이 모델은 기업의 본부 및 지부의 모든 사용자는 본부의 인터넷 영역에 설치한 IP-PBX(Master)를 통해 VoIP 서비스를 제공받으며, 각 지부에 설치된 백업 IP-PBX는 본부에 설치된 IP-PBX의 고장 및 장애 등으로 서비스 제공이 불가능할 경우 사용하게 된다.

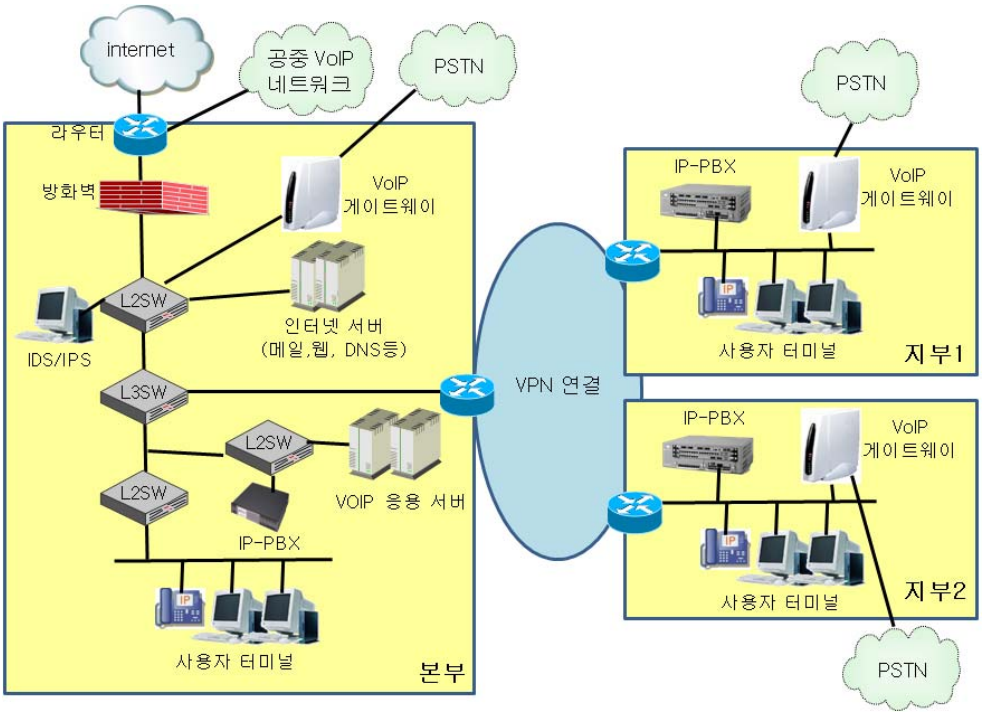


(그림 5-15) 대규모 기업의 중앙집중형 VoIP 구성모델

다. 대규모 기업의 분산형 VoIP 구성모델(인터넷 영역)

인터넷과 인트라넷을 물리적으로 분리한 대규모 기업의 분산형 VoIP 구성모델은 (그림 5-16)과 같다. (그림 5-16)은 대규모 기업의 본부에 위치한 인터넷 영역에 VoIP 시스템을 설치하여 사용자들에게 VoIP 서비스를 안

전하게 제공하는 모델이다. 각 구성요소 및 용도 등의 자세한 설명은 앞에서 설명한 중앙집중형 IP-PBX 구성 모델과 동일하지만, 단지 사용자들에게 VoIP 서비스를 제공하기 위해 VoIP 응용서버를 인터넷 영역의 안전한 장소에 설치한 것이 큰 차이점이다. 이 모델에서 VoIP 서비스의 제공을 위해 본부의 사용자는 본부의 IP-PBX에 연결이 되고, 각 지부의 사용자는 본인이 근무하는 지부에 설치된 IP-PBX에 연결이 된다.



(그림 5-16) 대규모 기업의 분산형 VoIP 구성모델

제 6 장 결 론

본 보고서에서는 mVoIP 이용자를 보호하고 특히 국내 mVoIP의 안전성을 향상시키기 위해서 필요한 mVoIP 정보보호 대책에 대해서 살펴보았다. 본 보고서에서 제시한 mVoIP 정보보호 대책은 이용 주체에 따라 각각 다음과 같이 활용될 수 있다.

○ 이용자
- 안전한 mVoIP 어플리케이션을 선택하는데 참고할 수 있다.
- mVoIP 어플리케이션을 안전하게 이용하기 위해서 필요한 소프트웨어 설정, 무선 네트워크(Wi-Fi) 설정, 스마트폰 설정 등에 활용할 수 있다.

○ mVoIP 어플리케이션 개발 업체
- 안전한 mVoIP 어플리케이션을 개발하는데 활용할 수 있다.
- 안전한 mVoIP 어플리케이션 개발을 통해 사용자의 신뢰를 얻을 수 있다.
- 국산 mVoIP 솔루션의 경쟁력을 강화하는데 활용할 수 있다.

○ 정부
- mVoIP 운영정책을 수립하는데 활용할 수 있다.
- 전체 스마트폰 이용환경의 보안정책을 수립하는데 활용할 수 있다.

한 편, 본 보고서에서 제시한 mVoIP 정보보호대책의 효과를 극대화하기 위해서 다음과 같은 후속조치가 필요하다.

우선 정부에서는 단순히 정보보호대책을 mVoIP 어플리케이션 개발 업체에 제시하는 것을 넘어서서, 이와 같은 정보보호대책의 필요성을 적극적으로 이해시켜야 한다. 이를 위해서는 도청 등 실제 사고사례와 현재

서비스 중인 mVoIP 어플리케이션 등을 대상으로 한 테스트 결과를 제시해야 한다. 또한 안전한 mVoIP 어플리케이션 개발 가이드를 제시하고 나아가 암호 라이브러리 등 필요한 기술을 개발하여 제공해야 한다. 이를 통해 mVoIP 어플리케이션 제작업체의 적극적인 참여와 공감을 얻어낼 수 있다.

또한 사용자를 대상으로 해서는 관련기관 홈페이지 등을 통해서 검증된 mVoIP 어플리케이션 목록을 공개해서 이용자가 안전한 mVoIP 서비스를 선택할 수 있도록 유도할 수 있다. 그리고 동시에 발견된 mVoIP 보안 취약점을 공개함으로써 이용자의 주의 깊은 mVoIP 서비스 이용을 유도할 수 있다. 이와 함께 이미 제공되고 있는 '스마트폰 보안 10계명'과 같은 'mVoIP 사용 가이드'를 개발하여 이용자에게 제공함으로써 이용자의 정보보호의식을 함양할 수 있다.

mVoIP 어플리케이션 개발업체의 경우에는 mVoIP 정보보호 대책이 자신들의 서비스를 확대하는데 반드시 필요한 조치를 인식하고 정부의 정보보호 활동에 적극적으로 참여해야 한다. 이를 위해서 업체에서 발견한 악성행위 및 취약점을 정부 및 타 업체와 적극적으로 공유할 필요가 있다. 또한 스패머 정보 등도 공유함으로써 전체 mVoIP 이용 환경의 안전성과 신뢰성을 향상시킬 수 있다.

스마트 환경 시대의 도래와 함께 mVoIP의 이용은 더욱 확대될 것으로 기대되고 있다. mVoIP의 활성화를 위해서는 서비스 초기 단계인 지금부터 안전성 확보를 위한 노력을 기울여야 한다. 이를 위해서 본 보고서에서 제시한 mVoIP 정보보호 대책을 기반으로 한 다양한 mVoIP 정보보호 연구 및 개발 활동이 이루어져야 하며, 이를 통해서 국내 mVoIP 산업의 국제 경쟁력 확보를 이뤄낼 수 있다.

참고문헌

[1] 강유리, “국내・외 주요 이동통신 사업자들의 mVoIP 대응 동향 및 시사점”, 방송통신정책 제23권 10호, 2011.6.1

[2] 이주영, “해외의 모바일 VoIP 서비스 제공 현황”, 정보통신정책연구원 방송통신정책 제21권 9호, 2009. 6

[3] http://www.seoul.co.kr/news/newsView.php?id=20110323001012

[4] Mary Meeker, Scott Devitt, Liang Wu, "Internet Trends", Morgan Stanley, 2010. 4.

[5] 지순정, 정수연, 이종화, “스마트폰의 기회와 위협”, 인터넷 & 시큐리티 이슈, 한국인터넷진흥원, 2009. 3.

[6] Davi Barrera, P.C. van Orchot, "Secure Software Installation on Smartphones", IEEE Security and Privacy, 2010. 11

[7] J. Adnerson, J. Bonneau, F. Stajano, "Inglorious Installer: Security in the Application Marketplace", Proceeding of the 9th Workshop on the Economics of Information Security, 2010

[8] W. Enck, M. Ongtang, P. McDaniel,"Understanding Android Security", IEEE Security & Privacy, 7(1):50-57, 2009

[9] 김욱준, 정승원, “mVoIP 확산 요인 및 패턴에 관한 개괄적 조사연구”, 방송통신정책 제22권 23호, 2011. 12

[10] Morgan Stanley, "Internet Trend", 2010. 4

[11] Mike Dolan, "Truphone reduces mobile VoIP prices", Fierce Wireless, 2010. 9

[12] Stephan Beckert, "International phone traffic growth slows, while skype accelerates", TeleGeography, 2010. 1

[13] 매일경제, 2011. 1. 3

“이 페이지는 공백임”

부록 A. VoIP 정보보호 점검항목

부록 B에서는 mVoIP 정보보호 대책의 이해를 돕기 위해서 기존 VoIP 정보보호 점검항목을 소개한다. 특히 관리적 보호조치, 물리적 보호조치는 mVoIP 정보보호 대책에는 포함되지 않은 내용이나, mVoIP 소프트웨어 제작업체나 이동통신사에서는 보다 안전한 mVoIP 운용환경 구축을 위해서 이 내용을 참조할 수 있다.

제 1 절 기술적 보호조치

1.1	네트워크 보안	1.1.1	VoIP 트래픽 모니터링 및 보안 관리	VoIP 트래픽을 모니터링 하고 관리할 수 있는 시스템을 운영하고 있는가?
		1.1.2	침입 탐지 및 대응	VoIP 보안 장비들에 대한 통합보안 관리시스템을 운영하고 있는가?
				특정 회선이 장애가 발생하여 트래픽이 전달되지 못하는 상황에 대비한 우회경로를 확보하였는가?
				DoS/DDoS 등의 공격에 대비하여 서비스 가용성을 보장하기 위한 대응 기술을 적용하였는가?
		1.1.3	네트워크 및 단말 접근제어	음성망과 데이터망을 물리적 또는 논리적으로 분리하여 운영하는가?
				접근 권한이 없는 VoIP 단말 및 장비의 접근 차단을 실시하고 있는가?
		1.1.4	도청 방지	LAN/WAN 구간에서의 도청 방지를 위한 기술적 대책을 적용하고 있는가?
		1.1.5	스팸 대응	VoIP 스팸 대응 시스템이 구축 및 운영되고 있는가?

1.2	단말 보안	1.2.1	단말기	단말의 펌웨어 및 전용 어플리케이션 등을 주기적으로 갱신 및 관리하고 있는가?
		1.2.2	계정 관리	사용자 아이디 및 패스워드 관리가 이루어지고 있는가?
		1.2.3	암호 기술	제어 메시지 및 통화내용 암호화 기능이 제공되고 있는가?
		1.1.1	스팸 대응	단말 내 스팸 차단을 위한 관리 기능이 제공되고 있는가?
1.3	VoIP 설비 보안	1.3.1	침입 탐지	백도어 및 해킹을 위한 에이전트 설치 및 불필요한 서비스 활성화 여부 점검이 이루어지고 있는가?
				VoIP 교환 장비들의 VoIP 전용 사용 및 이를 보호하기 위한 보안 장비가 운용되는가?
		1.3.2	접근제어 및 계정 관리	VoIP 교환 장비 관리자를 인증할 수 있는 인증 메커니즘이 적용되고 있는가?
				관리자 계정의 Default password는 유추하기 어려운 비밀번호로 변경하여 사용되고 있는가?
		1.3.3	로그 및 보안패치 관리	운영자 시스템 이상 징후 등에 대한 로그를 남기고 이를 주기적으로 점검하고 있는가?
				장비 보안 패치의 주기적인 갱신 및 관리가 이루어지고 있는가?
		1.3.4	암호기술	제어 메시지 및 통화 내용 암호화 기능을 제공하는가?
1.4	사용자 정보보호	1.4.1	개인정보 취급 관리	개인정보 저장 및 전송시 유·노출을 방지하기 위한 보안기술을 적용하였는가?
				개인정보 관련 DB 및 처리 시스템에 대한 접근통제 기술을 적용하였는가?

제 2 절 관리적 보호 조치

2.1	정보보호 조직의 구성/운영	2.1.1	정보보호 조직의 구성	인터넷전화 보안을 위한 정보보호 책임자, 정보보호 관리자, 정보보호 담당자로 구성된 정보보호 조직이 운영되고 있는가?
		2.1.2	정보보호 책임자의 지정	정보보호에 대한 업무를 총괄 책임지는 정보보호 책임자가 지정되어 있는가?
		2.1.3	정보보호 조직 구성원의 역할	인터네전화 정보보호 업무와 조직을 총괄 지위하는 책임자가 지정되어 있는가?
				인터넷전화 정보보호 업무의 실무를 총괄하는 관리자가 지정되어 있는가?
				인터넷전화 정보보호 업무의 분야별 실무담당자가 지정되어 있는가?
2.2	정보보호 계획 등의 수립 및 관리	2.2.1	정보보호 방침의 수립・이행	회사의 정보보호의 목적, 범위, 책임 등을 포함한 정보보호방침(Policy)을 수립하였으며, 인터넷전화 관련된 내용이 포함되어 있는가?
				정보보호방침은 최고경영층(임원급 이상)이 승인하였는가?
		2.2.2	정보보호 실행계획의 수립 및 이행	정보보호방침을 토대로 예산, 일정 등을 포함한 당해 연도의 인터넷전화 정보보호 실행계획을 수립하고 있는가?
				최고경영층이 실행계획을 승인하고 정보보호 책임자가 추진 상황을 매 반기마다 점검하는가?
				인터넷전화 설비 및 시설에 대한 기술적・관리적・물리적 보호 조치의 구체적인 시행 방법・절차 등을 규정한 정보보호실무지침을 마련하고 있는가?
		2.2.3	네트워크 및 단말 접근제어	음성망과 데이터망을 물리적 또는 논리적으로 분리하여 운영하는가?
				접근권한이 없는 VoIP 단말 및 장비의 접근 차단을 실시하고 있는가?

2.3	안전보안	2.3.1	내부인력 보안	임직원의 정보 또는 퇴직시 즉시 관련 계정 등에 대한 접근권한을 제거하는가?
				임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천 수칙 보급 등)를 실시하는가?
				정보보호 조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호 교육을 실시하는가?
		2.3.2	외부인력 보안	자사 직원이 아닌 자를 업무에 활용할 경우 보안서약을 징구하는가?
		2.3.3	위탁운영 보안	전산업무를 외부에 위탁할 경우, 보안계약서 또는 서비스수준협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 중단에 따른 비상대책' 등을 반영하는가?
2.4	이용자 보호	2.4.1	정보보호 정보 제공	이용자에게 침해사고 예·경보, 보안취약점, 계정·비밀번호 관리 방안 등의 정보를 지속적으로 제공하는가?
2.5	침해사고 대응	2.5.1	침해사고 대응 계획의 수립·이행	침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응 방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한 침해사고 대응 계획을 마련·시행하는가?
2.6	정보보호 조치	2.6.1	보호조치의 자체 점검	정보보호 관리자는 매년 동지침 및 정보보호실무지침의 기준에 따라 자체적으로 인터넷전화 정보보호 현황을 점검하는가?
2.7	정보자산 관리	2.7.1	VoIP 설비 및 시설의 현황 관리	VoIP 망 구성도를 마련하고 변경사항이 있을 경우, 보완·관리하는가?
				VoIP 설비 및 시설의 목록(용도 및 위치 등 포함) 작성·관리를 하는가?

제 3 절 물리적 보호조치

3.1	출입 및 접근보안	3.1.1	VoIP 시설의 출입	비인가자가 출입할 수 없도록 잠금장치를 설치하고 있는가?
				출입자의 출입 기록을 일정 기간 이상 유지·보관하고 있는가?
3.2	시설 운영/ 관리	3.2.1	백업설비 및 시설 설치·운영	정전 및 회선 장애 발생에 대비하여 VoIP 서비스를 지속적으로 제공할 수 있는 백업설비 및 시설을 설치·운영하고 있는가?
3.3	기타	3.3.1	기타	VoIP 시스템 관리를 위해 전용 소프트웨어 및 웹 인터페이스를 사용할 경우, VoIP 서비스 제공업체의 정책에 따른 대책이 강구되어 있는가?
				중요정보를 포함한 매체의 폐기시 저장된 정보를 안전하게 삭제하는가?
				이용자 개인정보 등 중요한 정보를 저장하고 있는 저장 매체를 폐기할 때, 사전에 기록된 내용을 완전히 삭제하고 복구 불가능 상태임을 확인한 뒤에 물리적으로 파기하는가?

“이 페이지는 공백임”

부록 B. 정보보호관리체계/개인정보보호관리체계

제 1 절 ISO/IEC 27001

1. 의의

국제 표준화 기구 ISO/IEC JTC 1/SC27에서는 국제 사회에서 글로벌하게 사용될 수 있는 IT 보안 기술 분야의 다양한 표준을 제정하는 역할을 하고 있다. ISO/IEC 27001과 27001은 영국 BSI(British Standard Institute)에서 개발한 BS 7799의 Part 1과 Part 2를 표준화 한 것으로, 먼저 Part 2가 ISMS의 요구사항에 대한 표준인 27001로 표준이 되고, 이후에 Part 1이 실행지침인 27002로 표준화되었다. 현재 정보보호분야의 공식적인 인증제도로 자리 잡은 ISO/IEC 27001은 ISMS에 대한 이해, 감시 및 검토, 유지, 개선 등에 대한 요구사항을 정의하며, 조직의 정보자산에 대한 보호 및 관리를 위해 ISMS를 수립·운영하기 위한 정형화된 프로세스인 PDCA, 절차, 정보보호 통제(27001) 등으로 구성된 정보보호 관리체계를 갖추었는지를 평가하고 인증하는 표준이다.

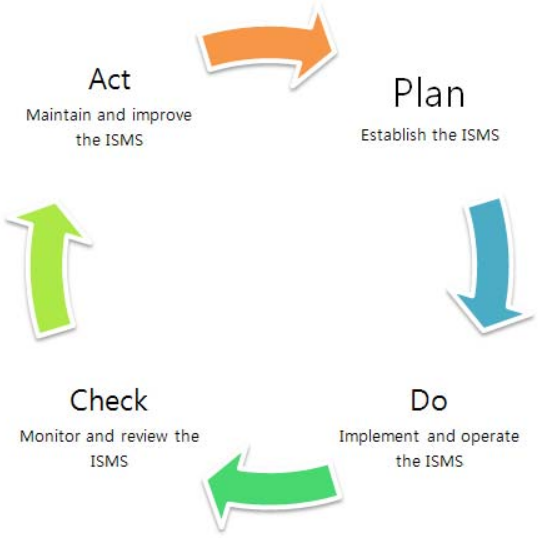
2. 목적

ISO/IEC 27001은 국제표준화기구(ISO)의 공동기술위원회 ISO/IEC JTC1와 정보기술 소위원회 SC27에서 공동으로 개발한 국제 정보보호관리체계의 표준규격으로 위험관리·보안정책·정보보호사고 대응 등 다양하고 엄격한 심사와 검증을 통해 조직의 위험관리 수준을 일정수준 이상으로 향상시킬 수 있다. 정보보호관리체계 인증을 통해 조직은 조직의 정보자산을 균형 잡힌 보안통제를 통해 관리하고 있음을 공인받고 고객 신뢰도 향상 및 회사 안정성 제고를 달성할 수 있다.

조직의 서비스를 효과적으로 제공하기 위하여 조직 내의 다양한 활동을 파악하고 관리해야 한다. ISO/IEC 27001:2006 정보보호관리체계(ISMS:Information Security Management System)는 정보보호관리의 전반적인 업무와 관련된 정보보호 요구사항 및 정책과 목표 수립의 필요성의 이해를 돕고, 조직의 전반적인 업무와 관련된 위험 관리를 위한 통제사항을 제시한다.

3. 대상, 범위 및 특징

정보보호 관리시스템은 모든 유형의 조직(예를 들면 상업적 기업, 정부, 비영리 조직 등)을 대상으로 조직의 전반적인 업무활동 및 조직이 직면한 위험들과 관련하여 정보보호 관리시스템을 문서화하고, 정보보호 관리시스템의 수립·실행·운영·모니터링·검토·유지 및 개선하기 위해 프로세스 접근방식인 PDCA 모델을 기반으로 한다. PDCA 모델을 통해 조직은 정보보호와 관련된 전반적인 업무를 프로세스화하여 각 프로세스간의 상호작용을 통하여 조직의 정보보호관리체계에 대한 지속적인 위험관리 및 지속적 개선이 가능하도록 한다.



(그림 B-1) PDCA 모델

2005년 발표된 ISO/IEC 27000 시리즈는 27000:2009 ISMS에 대한 개요 및 용어정리, 27001:2005 ISMS의 PDCA(Plan-Do-Check-Act) 프로세스에 기반한 정보보호 요구사항 정의, 27002:2005 ISMS의 정보보호 관리를 위한 실행지침서, 27003:2010 ISMS에 대한 구현 가이드라인, 27004:2009 정보보호관리에서의 정보보호 매트릭스와 측정에 관한 표준, 27005:2008 정보보호 위험관리에 대한 표준, 27006:2007 ISMS의 감사 및 증명 제공을 위한 인증기관에 대한 요구사항, 27011:2008 ISO/IEC 27001에 기반한 정보통신업체를 위한 정보보호관리 가이드라인 등이 국제 표준으로 제정된 상태이다.

4. 지표 구성

통제분야	통제항목	세부통제항목
1. 보안정책	1	2
2. 정보보안 조직	2	11
3. 자산 관리	2	5
4. 인원 보안	3	9
5. 물리적 환경적 보안	2	13
6. 통신 및 운영 관리	10	32
7. 접근 통제	7	25
8. 정보시스템 취득, 개발, 유지보수	6	16
9. 보안 사고 관리	2	5
10. 사업 연속성 관리	1	5
11. 준거성	3	10
소계	**39**	**133**

(그림 B-2) ISO 27001 평가 지표

제 2 절 K-ISMS

1. 의의

K-ISMS는 2002년 ISO/IEC 27001을 기반으로 국내 실정에 맞도록 개발된 정보보호 관리체계 인증제도(Information Security Management Systems)이다. 정보보호 관리체계 인증제도란 정보통신서비스제공자가 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 수립·운영하고 있는 기술적·물리적 보호조치를 포함한 종합적 관리체계를 말한다.

2. 목적

본 제도는 “정보통신망이용촉진및정보보호등에관한법률” 제47조, “정보통신망이용촉진및정보보호등에관한법률시행령” 제50조, 정보보호관리체계인증 등에 관한 고시(제2008-11호)에 근거하여 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화 하고 지속적으로 관리·운영하는 시스템을 운영하는 조직에 대해 안전성을 보장하는 인증서를 발급하고 있다.

- o 데이터의 기밀성(Confidentiality) : 정보가 특정 권한을 부여받은 인가된 사용자에만 접근 및 공개됨을 보장해야 한다.
- o 데이터의 무결성(Integrity) : 정보가 부적절한 방법에 의해 데이터가 변경되지 않았음을 보장한다.
- o 데이터의 가용성(Availability) : 정보가 적절한 방법을 통해 특정 권한을 부여받은 인가된 사용자에게만 제공됨을 보장해야 한다.

정보보호 관리체계 인증제도는 한국인터넷진흥원이 제3자의 객관적이고 독립적인 입장에서 평가 대상 적합한 정보보호를 위해 정책 및 조직 수립,

위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 통해 정보보호대책들이 적절성에 대해 평가하고, 정보보호 관리체계 인증제도기준에 대한 적합성 여부를 보증함으로써 조직의 정보자산의 신뢰성 향상 및 정보보호관리에 대한 인식 제고와 더불어 국제적 신뢰도 향상시킨다. 나아가 본 제도의 활성화를 통하여 정보보호서비스 산업의 활성화를 도모함을 목적으로 한다.

3. 대상, 범위 및 특징

정보보호 관리체계 인증제도는 개인정보를 취급하고 있는 모든 민간기업을 대상으로 하고 있다. 예를 들면 공공기관의 입찰에 참여하는 기업·금융·교육·의료기관·통신업체 등 주요자산을 취급하는 기업, 또는 이들 기업의 정보를 위탁·관리·가공·이용하는 아웃소싱업체들 또한 그 대상이 될 수 있다.

인증 범위는 전체 조직을 대상으로 하는 정보보호 관리체계 인증을 권고하지만, 조직의 상황에 따라 그 범위를 조직의 일부로 제한할 수 있다. 단, 한 조직이 조직의 일부를 추가로 인증 받는다고 해서 인증서의 개수가 증가되는 것은 아니며 기존 인증서의 인증 범위가 확대되게 된다.

K-ISMS는 15개 영역 120개의 통제항목과 396개의 세부통제항목으로 구성되어 있고, 기존 ISO/IEC 27001과의 비교해볼 때, 국내 실정을 반영하기 위하여서 정보보호 교육 및 훈련, 암호통제, 전자거래보안 영역 등이 추가되었다. 인증 제도의 활성화를 위해 인증서를 획득한 기업들에게는 정보보호 관련 보험 가입 시 요금 할인, 가산점 부여, 정보보호 안전진단 면제 등의 혜택이 주어지고 있으며, 2010년부터는 매출액 50억 미만이나 종업원 수 50명 미만인 업체가 ISMS를 취득할 경우 최대 50%의 인증수수료를 인하하여 비용적 측면에서 부담이 되는 소규모 사업자의 참여를 지원하고 있다.

4. 지표구성

통제분야	통제내용	통제사항 수	세부통제사항 수
정보보호대책	1. 정보보호정책	5	10
	2. 정보보호조직	4	11
	3. 외부자 보안	4	8
	4. 정보자산 분류	4	7
	5. 정보보호 교육 및 훈련	4	14
	6. 인적 보안	5	18
	7. 물리적 보안	12	36
	8. 시스템개발 보안	13	53
	9. 암호 통제	3	6
	10. 접근 통제	14	38
	11. 운영관리	22	99
	12. 전자거래 보안	5	21
	13. 보안사고 관리	7	20
	14. 검토, 모니터링 및 감사	11	37
	15. 업무 연속성 관리	7	18
	소계	**120**	**396**

(그림 B-3) K-ISMS 평가 지표

제 3 절 BS 10012

1. 의가. 의의

BS 10012는 DPA(Data Protection Act 1998)의 요구사항에 대한 컴플라이언스 향상과 유지를 위하여 조직이 개인정보경영시스템(PIMS: Personal Information Management System)의 수립과 운영을 규정하기 위한 규격으로 BSI(British Standard Institute)에서 업계, 정부, 학계 및 소비자 단체 관계자를 포함하는 전문가 패널에 의해 개발 되었으며, 2009년 5월 31일에 발표되었다.

2. 목적

개인정보보호 관리를 기본 체계 및 신뢰를 제공하고, DPA 컴플라이언스에 대한 평가를 위해 내부 및 외부 평가가 효과적으로 이루어질 수 있도록 하며, 조직 내 PIMS에 대한 수립, 책임, 구현 및 유지를 하기 위한 것이다.

3. 대상 및 범위

PIMS의 적용 범위는 민간, 공공 등에 제한이 없으며, 조직의 규모에도 제한이 없다.

4. 특징

ISO/IEC 27001처럼 PDCA 모델이 적용되어 있으며, BS 10012에는 명시되어 있지는 않으나, 'DPA외의 법규(예:Freedom of Information Act 2000)에 대해서도 반드시 확인해야 한다.'라고 되어 있다.

제 4 절 PIMS

1. 의의

PIMS는 방송통신위원회에서 민간 사업자를 대상으로 사업자가 개인정보를 안전하게 보호할 수 있는 환경조성하고 이를 검증받을 수 있는 인증제도이다. 이 인증을 획득하는 기업은 개인정보 수집·이용·보유·제공·파기 등 전체 라이프사이클 전 과정에서 개인정보에 대한 안전성과 신뢰성 및 이용자 권리보호를 위한 전사적인 활동을 323개의 평가항목을 통해 공인받게 된다.

2. 목적

개인정보 보호 활동을 체계적이고 지속적으로 수행하기 위한 개인정보 보호 유관 법적 요구사항을 기반으로 전사적인 기술적·관리적 요구사항을 제시하고 한다.

3. 대상 및 범위

정보보호 관리체계 인증제도는 개인정보를 취급하고 있는 모든 민간 기업을 대상으로 하고 있다.

인증범위는 조직에서 취급하는 개인정보 현황을 파악하여, 개인정보를 취급하는 모든 부서 및 시스템, 취급자를 포함한다. 전체 조직을 대상으로 하는 정보보호 관리체계 인증을 권고하지만, 조직의 상황에 따라 그 범위를 조직의 일부로 제한할 수 있다. 단, 한 조직이 조직의 일부를 추가로 인증 받는다고 해서 인증서의 개수가 증가되는 것은 아니며 기존 인증서의 인증 범위가 확대되게 된다.

4. 특징

PIMS는 생명주기 준거 요구사항 영역을 마련하여 개인정보의 수집부터 파기까지의 절차에 별도로 관리할 수 있도록 하고 있다. 이 영역은 ISO/IEC 27001과 K-ISMS에 존재하지 않는 영역이다. 방송통신위원회는 2010년 하반기부터 본 인증을 적용할 예정이다.

통제분야	통제내용	통제사항 수	점검항목 수
개인정보보호 대책요구사항	1. 개인정보수집에 따른 조치	7	17
	2. 개인정보 이용 및 제공에 따른 조치	16	49
	3. 개인정보 관리 및 파기에 따른 조치	5	12
	소계	**28**	**78**

(그림 B-4) 생명주기 준거 요구사항

제 5 절 K-ISMS와 PIMS 비교

정보보호관리체계(ISMS)는 주요 정보 자산을 보호하기 위해 정보보호 관리 절차 및 대책을 체계적으로 수립하여 지속적으로 관리·운영하기 위한 종합적인 체계이고 개인정보보호관리체계(PIMS)는 기업이 개인정보보호를 위해 무엇을, 어떻게 조치하여야 하는지에 대한 기준으로 차이점을 보이고 있다. 하지만 두 체계 모두 위험이나 문제점을 파악하여 해결방안을 마련할 수 있도록 위험관리방법 및 대책을 제공한다는 점에서 같은 목표를 가지고 있다. 두 체계를 비교한 표는 아래와 같다.

(표 B-1) 체계 비교 분석

	ISMS	PIMS
시행근거	정보통신망법 제47조 동법 시행령 50조	방통위 의결(2010.11.15.)
시행년도	2002년	2011년
인증단계	준비단계-심사단계-인증단계-사후관리단계	준비단계-심사단계-인증단계-사후관리단계
인증기관	KISA	KISA
점검항목	137개 항목 (세부 항목 446개)	118개 항목 (세부 항목 325개)

ISMS와 PIMS의 점검항목을 비교해 보면 공통 항목 78개, ISMS의 고유 항목 59개, PIMS의 고유 항목 40개로 나타난다. 공통 항목은 관리적 대책이나 IT 인프라에 대한 기술적 보호대책에 관한 항목이고 ISMS의 고유 항목은 시스템 가용성, 서비스 안정성 그리고 업무연속성 유지와 관련된 보호대책들이 고유 항목으로 나타났다. 그리고 PIMS의 고유 항목은 개인정보 생명주기와 관련한 법적 요구사항으로 나타났다.

각각의 항목을 살펴보면 아래 표 와 같다.

(표 B-2) PIMS 항목

공통항목	o 개인정보보호관리체계 수립에 필수적인 관리과정 o 정책관리, 조직구성, 인적보안, 정보자산식별, 교육 및 훈련, 침해사고 대응 등 관리적 보호대책 o 접근통제, 암호통제, IT 인프라 운영통제, 개발보안 등 기술적 보호대책
ISMS 고유항목	o 시스템 성능·용량·백업 및 복구·장애·로그관리, 네트워크 모니터링 등 가용성 보호대책 o 서비스 안정성을 위한 업무연속성 계획 수립 및 유지·관리 보호대책 o 데이터센터내 장비 배치, 내부설비, 항온·항습 등 물리적 보호대책
PIMS 고유항목	o 개인정보 생명주기에 따른 개인정보개인정보 수집→이용·제공→관리·파기에 관한 내용(개인정보 관련 법적 준수사항 위주) o CPO 지정, 개인정보흐름분석, 개인정보취급자 관리, 개인정보 열람 및 처리 기록 검토

“이 페이지는 공백임”

부록 C. 정보보호관련 표준화 동향

제 1 절 ITU-T SG 17

현재 진행 중인 표준화 프로젝트는 X.isgf(information security governance framework, editor: 김정덕, 한국), X.ismf(information security management framework, editor: Chen, 중국), X.amg(Asset management guidelines in telecommunication organizations, editor: 이진태, 정태인, 한국), X.sgsm(Information security management guidelines for small and medium-sized telecommunication organizations, Wataru Senga, 장항배, 정정윤) 등 4개 프로젝트가 진행 중이며 신규 프로젝트로서 1) 클라우드 보안관리, 2) IPv6에서의 보안관리, 3) X.1051 사용자 지침, 4) 개도국 CIRT 보안 핸드북 등 4개 항목이 지난 일본에서 개최된 Q.3 임시회의에서 승인되어 진행될 예정이다.

특히 X.isgf 와 클라우드 보안관리는 JTC1 SC27과 공동 작업으로 진행되고 있다는 점을 주목할 필요가 있다.

X.amg와 X.ismf는 2011.4월에 국가별 의견수렴(Consent)으로 승인될 예정이며, X.sgsm은 2011.8월에 Consent를 추진 예정으로 작업 중에 있다. X.isgf는 2012년에 국제표준으로 최종 결정(determination)될 예정이다.

(표 C-1) 개발 권고안 현황

Acronym	주제 (Title)	에디터 (Editor)	문서번호 (Text)	승인시기 (Timing)
X.isgf	Governance of information security	Jungduk Kim	TD1969	2012-02 (Determination)
X.sgsm	Information security management guidelines for small and medium telecommunication organi	Hangbae Chang Chungyun Chung Sangsoo Jang	TD2184R1	2012-02 (Consent)

	zations	Wataru Senga Jintae Lee		
X.mgv6	Security Management Guideline for implementation of IPv6 environment in Telecommunications Organizations	Koji Nakao Jungsuk Song	TD1803	201
-	Security handbook on information security incident management for developing countries	Edward Humphreys Koji Nakao Damir Rajnovic Miho Naganuma JD. KIm M. Njiraini	-	2012-09
X.rmsm	Information security management reference model for small and medium telecommunication organizations	Hangbae Chang Chungyun Chung Sangsoo Jang	COM17-R 24 Annex C Attachment 1	TBD
-	User's guide for X.1051	Wataru Senga	TD2256	2012-02

- X.isgf : Determination(TAP), 나머지 과제는 Consent(AAP)

- TBD : To Be Developed

제 2 절 ISO/IEC JTC 1/SC 27

1. ISO/IEC 27000:

27000 패밀리 표준을 위한 주요 63개 용어 정의 및 전체 구조를 보여주는 문서로 2009년에 국제표준으로 발표되었다. 현재는 WG 4의 작업내용을 포함하고 새롭게 개정된 ISO Guide 73 등 새로운 용어 정의의 필요성이 있어 개정 작업 중에 있다. WG 4 표준화 프로젝트와의 일관성을 유지하기 위해 WG 4에서 Study Period를 가지기로 하였다. 폴란드의 Elzbieta와 스웨덴의 Anders가 editors로 활동하고 있다.

2. ISO/IEC 27001:

ISMS의 요구사항을 포함하는 가장 중요한 문서로서 2005년도에 국제표준으로 발표되었지만, 현재는 새로운 요구사항을 반영하기 위해 개정작업 중에 있다. 2011년 3월 현재 4th WD 문서 상태이다. 회의에서는 정보보호 통제를 수록한 부록(Normative Annex)을 유지할지 아니면 폐지할지에 대해 논란이 있었으며, 최종 결론은 부록을 유지하기로 결정하였다. 또한 ISO/TMB JTCG 작업반(TF 1 : 구조, TF 3 : 용어정의)의 중간결과물인 공통경영시스템표준(Common Management System Standard: CMSS)문서의 공통적인 main/sub-clause 제목 (1. Context of Organization, 2. Leadership 3. Planning, 4. Support, 5. Operations, 6. Performance Evaluation, 7. Improvement)에 따라 27001 수정 작업을 진행하기로 최종 결정하였다. 4th WD는 새로운 구조로 재 작업된 문서이다.

3. ISO/IEC 27002:

정보보호 통제/실무규정을 포함하는 문서로서 역시 2005년도에 국제표

준으로 발표되었지만, 현재는 개정작업 중에 있다. 2011년 3월 현재, 3rd WD 문서로 앞으로도 참가국의 가장 높은 관심과 가장 많은 기고문이 예상된다. 지난 회의에서도 약 800여개의 코멘트를 회의기간 중 처리하지 못하여 회의 종료 후 전자회의 등을 통해 처리할 정도이다. 문서 제목도 과거의 정보보호관리(Management) 실무규약(Code of Practice)에서 정보보호통제(Control) 실무규약으로 변경하였다.

4. ISO/IEC 27005:

정보보호 위험관리에 대한 과정을 전반적인 위험관리 과정에 기초하되 정보보호의 특성을 고려하여 작성된 문서로서 2008년도에 국제표준으로 발표되었지만, 현재는 ISO 31000, Guide 73이 개정됨에 따라 27005의 개정작업 중에 있으며 Fast track으로 작업을 진행하기로 결정되었다. 따라서 현재 FCD문서인 27005를 Final DIS/DTR 투표를 위해 회람 중에 있다.

5. ISO/IEC 27007:

ISMS 심사시 사용할 수 있는 지침 성격의 문서로 ISO 19011과 17021-1의 내용을 ISMS 환경에 적합하도록 수정한 3rd CD 문서이다. 매우 안정된 상태이며 따라서 final CD로 등록하고 투표에 회부 중에 있다. 2012년에는 국제표준으로 발표될 예정이다.

6. ISO/IEC 27008:

ISMS 통제 구현 여부에 대한 기술적 평가를 위한 Technical Report로서 ISMS 심사인이 사용할 수 있는 지침이다. Anders Carlstedt(스웨덴)가 편집인으로 현재 PDTR 상태이며 Final DIS/DTR 투표를 위해 회람 중에 있다. 문서 제목을 Guidelines for auditors on information security controls로 수정하였다.

7. ISO/IEC 27010:

주요 정보통신시설을 운영하는 산업간 그리고 조직간 침해사고 정보 등 민감한 정보(Sensitive Information)를 공유할 수 있는 신뢰 구조(TICE: Trusted Information Communication Entity)의 구축 등을 주요 내용을 다루고 있다. 섹터간의 보안정보(위험지식, 배포 및 유통, 모니터링 등)를 교환, 공유할 경우 적용될 요구사항과 통제를 포함하고 있다. 27001에서의 요구사항 외에 추가적인 요구사항을 규정하고 있으며 27002에서의 보안 통제 외에 추가적인 통제를 규정하고 있다. 현재 1st CD 상태이다.

8. ISO/IEC 27013:

ITSM과 ISMS을 통합해서 개발할 경우에 적용되는 문서로 영국 BSI에서 "ISMS for Service Sector: Integrated Implementation of ISO 20000-1 and ISO27001"을 제안하여 지난 레드몬드 회의에서 새로운 프로젝트로 결정되었고 현재 2nd WD 상태이다. 주요 내용은 상호 관련이 있는 두 개의 경영시스템을 통합해서 구현할 경우의 이로운 점, 계획 수립, 기타 충고사항 등을 포함하고 있다. editor로 영국의 Bridget Kenyon이 활동 중에 있다.

9. ISO/IEC 27014:

정보보호의 효과적인 구현을 위해 최고경영층의 정보보호에 대한 전략과 통제체계를 규정하고 있는 정보보호 거버넌스에 관한 표준으로서 현재 1st CD 상태인 문서이다. ISMS는 주로 정보보호를 실행하는 측면에서 계획, 구현, 평가 등 정보보호 담당자 또는 정보보호 관리자가 참조할 수 있는 프로세스를 제시하고 있는 반면, 27014는 비즈니스와 정보보호와의 연계성 및 가치 전달을 위해 ISMS를 적절히 지휘 및 통제할 수 있는 원칙, 과정, 활동 등을 포함하고 있다. Editor로 김정덕(한국, 중앙대), Kei

Harade(일본, IPA)가 활동하고 있다. 이 표준은 SC 27과 ITU-T SG 17에서 공동으로 진행하고 있다.

10. ISO/IEC 27015:

미국 ANSI에서 제안하였고 주도하고 있는 금융서비스 조직의 정보보호관리에 관한 문서로 법적인 측면, 추가적인 구현 지침, 추가적 통제항목 등을 포함하고 있는 문서이다. 현재 2nd WD 이며 27001과 27002 외에 추가적인 요구사항과 통제를 포함할 예정이다. 룩셈부르크의 Benoit Poletti와 David Prendergast가 편집인으로 결정되었고 editor와 NB로부터 적극적인 기고문 작성이 필요하다.

11. ISO/IEC 27016:

경제학적 관점에서 정보보호관리 제반 이슈 (ISM-Organizational Economics)에 관한 지침으로서 지난 베를린 회의에서 신규 프로젝트로 결정되었다. 현재 1st WD 문서로 보안통제평가, 위험평가, 보안측정 등에서의 경제학적 의미와 접근방법을 보여주고 있으며, ROI 등 정보보호 경제모델을 제시하고 있다.

12. 예상 신 프로젝트 - 클라우드 보안 및 프라이버시:

베를린 회의에서 일본의 주도로 관련 국제표준 동향 등 발표가 있었고 최종적으로 WG 1, 4, 5와 공동으로 국제표준화를 위한 Study Period를 통해 새로운 프로젝트로 상정될 가능성이 높다.

(표 C-2) 현재 개발 중인 국제표준

ISO 과제번호	제목	표준화 진행상태		
		제정	제42차 ('10)	제43차 ('11.10)
ISO/IEC 27000	ISMS - Overview & vocabulary	IS (2009년)	3rd WD	1st CD
ISO/IEC 27001	ISMS - Requirements	IS (2005년)	1st CD	1st CD
ISO/IEC 27002	Code of practice for information s ecurity controls	IS (2005년)	4th WD	1st CD
ISO/IEC 27003	ISMS Implementation guidance	IS (2010년)		
ISO/IEC 27004	ISMS measurement	IS (2009년)	3rd CD	
ISO/IEC 27005	Information Security Risk manage ment	IS (2011년)		
ISO/IEC 27006	Requirement for bodies providin g audit and certification of infor mation security management syst ems	IS (2007년)	DIS	IS (예정)
ISO/IEC 27007	Guidelines for information secur ity management systems auditin g		FDIS	IS (예정)
ISO/IEC 27010	Information security manageme nt for inter-sector and inter-org anizational communications		FCD	FDIS
ISO/IEC 27011	Information security manageme nt guidelines for telecommunication s organizations based on ISO/IEC 27002(x.1051/27011)	IS (2008년)		
ISO/IEC 27013	Guidelines on the integrated im plementation of ISO/IEC 27001 and ISO/IEC 20000-1	-	1st CD	DIS
ISO/IEC 27014	Governance of information secu rity	-	2nd CD	DIS
ISO/IEC 27015	Information security manageme nt guidelines for financial servic es		3rd WD	1st CD
ISO/IEC 27016	Information security manageme nt - organizational economics		2nd WD	3nd WD
ISO/IEC 27017	Guidelines on information secur ity controls for the use of cloud computing services based on IS O/IEC 27002		NWIP	

“이 페이지는 공백임”

부록 D. 일본의 개인정보관리체계

프라이버시 마크(Privacy Mark System) 제도는 (재)일본 정보 처리 개발 협회 (JIPDEC)가 1998년부터 실시하고 있는 개인 정보 보호 사업자 인증 제도이다. 프라이버시 마크제도는 일본 공업 규격에서 정한 JIS Q 15001 (개인정보보호 경영시스템 - 요구 사항)에 근거하여 개인 정보에 대해 적절한 보호조치 등의 체제를 갖추고 있는 사업자인지 심사하여 인증하고 해당 사업자의 사업 활동에 대하여 개인정보보호 마크의 사용을 허용하고 있다. 대상이 되는 개인정보는 온/오프라인 등의 입수 경로에 상관없이 고객정보뿐이 아닌, 직원정보, 채용정보 등 당사에서 보유한 모든 개인정보가 적용된다.

(그림 D-1) 개인정보보호 마크

프라이버시 마크 시스템은 기업의 관리자 및 고용자들에게 개인정보 유출의 위험관리에 대한 인식을 높여주고 개인정보의 유출을 방지하는 조치를 강구하도록 하는 기능을 하며, 개인 정보보호 마크 시스템을 수여하는 기관은 개인정보 보호의 관리에 있어서 적절한 지식과 전문성이 있는 집단으로 인정받게 되는 의의를 지닌다.

제 1 절 인증기준 (JIS Q 15001:2006)

JIS Q 15001:2006(개인정보보호 경영시스템 - 요구 사항)은 사업자가 업무상 취급하는 개인정보에 대하여 안전하고 적절하게 관리하는 표준으로서 재단법인 일본규격협회의 원안으로 책정된 일본 공업규격이다.

이 표준은 사업자가 보유한 개인정보를 파악하고 검색 및 이용을 하는데 앞서 개인정보에 대한 본인동의, 사업자가 개인정보보호를 위한 조직을 설립, 그 체제를 정기적으로 검토 및 개선, 그리고 이들을 실천하기위한 시스템 (개인정보보호 경영시스템)을 가지도록 요구 하고 있다.

1. JIS Q 15001:2006의 규격 내용

JIS Q 15001:2006의 舊(구) 규격은 JIS Q 15001:1999(개인정보보호에 관한 컴플라이언스 프로그램의 요구사항)이며, "민간부문에서의 전자계산기 처리와 관련된 개인정보보호에 관한 가이드라인"을 기초로 1999년에 제정되었다. 2005년에 "개인정보의 보호에 관한 법률"이 제정되고, 동 년 4월부터 전면 시행됨에 따라 이러한 환경 변화를 반영한 재검토의 필요성이 부각되면서 현재의 JIS Q 15001:2006으로 개정하게 되었다. 따라서 JIS Q 15001:2006은 "개인정보의 보호에 관한 법률"에 기초한 규격이라 볼 수 있다. 본 규격은 다음과 같이 구성되어 있다.

(표 D-1) JIS Q 15001:2006

구성	내용
1. 적용범위	개인정보를 사업용으로 이용하는 모든 종류의 사업자에 적용
2. 용어 및 정의	"개인정보의 보호에 관한 법률"에서 정의한 용어를 그대로 준용함

3. 요구 사항	일반 요구사항		사업자는 개인정보보호 경영시스템을 확립하여 시행·유지·개선해야 함
	개인정보보호 방침		사업자는 개인정보보호 방침을 제정하고, 이를 시행·유지해야 함
	계획		관련 법령 등, 위험관리, 리소스관리, 내부 규정화, 교육, 감사, 긴급대응체계 등을 포함해야 함
	실시 및 운용	운용 절차	개인정보보호 경영시스템을 실행하기 위한 운용 절차를 마련해야 함
		취득, 이용 및 제공에 관한 원칙	이용목적 범위의 특정, 합법적인 수집, 목적범위 내 이용, 본인동의 후 제공 등이 실행되어야 함
		적정관리	안전관리 조치, 종업원 감독, 위탁업체 감독 등을 수행해야 함
		개인정보에 관한 본인의 권리	개인정보 소유자로부터 개시, 변경, 정지 등의 요청 시 처리해야 함
		개인정보 보호 관리 시스템 문서	관리대상 문서, 문서관리절차, 기록관리 등을 위한 절차를 수립해야 함
		고충 및 상담에 대한 대응	개인정보 소유자로부터 고충 및 상담 요청시 신속하게 대응해야 함
		점검	본 규격의 준수여부 확인을 위한 점검 및 정기감사 등을 시행해야 함
		시정조치 및 예방 조치	지적사항에 대한 조치 및 예방을 위한 활동을 시행해야 함
		사업자의 대표자에 의한 재검토	감사결과, 환경변화 등을 고려하여 개인정보보호 경영시스템을 정기적으로 재검토해야 함
4. 해설			본 규격의 항목을 설명하는 것이며 규격에 포함되지 않음

※ JIS Q 15001:2006 규격은 [붙임] 참고

2. 프라이버시 마크와의 관계

(재)일본 정보처리 개발협회(JIPDEC)는 JIS Q 15001의 요구사항을 충족시키고 개인정보보호에 대한 적절한 조치를 수행하고 있다고 판단되는 사업자에 대해 프라이버시 마크 사용을 허용한다.

프라이버시(Privacy) 마크의 알파벳 P 모양의 로고를 인가받은 사업자는 자사의 웹 사이트 및 간행물 등을 통해 개인정보의 안전한 운용을 대외적으로 광고할 수 있다.

제 2 절 프라이버시 마크 제도의 운영체계

프라이버시 마크 제도는 아래와 같이 2개의 기관으로 구성・운영된다.

- 프라이버시 마크 부여 기관 (부여 기관)
- 프라이버시 마크 부여 인증 지정 기관 (지정 기관)

부여기관은 (재)일본 정보처리 개발협회(JIPDEC)이며, 인증지정기관은 지역별 및 심사대상 사업자마다 여러 심사기관이 지정되어 운영되고 있으며, 다음과 같이 구성된다.

(표 D-2) 프라이버시 마크제도 운영체계

구 분	기 관
프라이버시 마크 부여 /감독 기관	(재)일본 정보처리 개발협회(IIPDEC)
프라이버시 마크 부여 인증 지정 기관	- 정보 서비스 산업 협회 - 일본 마케팅 리서치 협회 - 전국 학원 협회 - 전 일본 관혼상제 상조회 협회 - 일본 그래픽 서비스 산업 협회 - 일본 정보시스템 사용자 협회 - 일본 통신학회 - 컴퓨터 소프트웨어 협회 - 일본 인쇄 산업 연합회 - 방송 보안 센터 - 의료 정보시스템 개발 센터 ※ 의료 복지 관련 업종이 신청 대상 - 홋카이도 IT 추진 협회 ※ 홋카이도에 본사가 있는 회사가 신청 대상 - 특정 비영리 활동 법인 미치노쿠 정보 보안 추진 계획 ※ 동북 지방에 본사가 있는 회사가 신청 대상 - 중부 산업 연맹 ※ 아이치현, 기후현, 미에현, 도야마현, 이시카와현에 본사가 있는 회사가 신청 대상

	- 간사이 정보 산업 활성화 센터 ※ 오사카부, 교토부, 후쿠이현, 시가현, 효고현, 나라현, 와카야마현에 본사가 있는 회사가 신청 대상 - 쿠마모토 테크노 산업 재단 ※ 규슈 오키나와 지역에 본사가 있는 회사가 신청 대상 - 시코쿠 경영시스템 추진기구 ※ 중국 시코쿠 지방에 본사가 있는 회사가 신청 대상

1. 신청 자격 및 절차

프라이버시 마크를 취득하기 위해서는 일본 공업규격(JIS)인 JIS Q 15001:2006(개인정보보호 경영시스템 - 요구사항)의 요구사항에 따라 개인정보보호 체계를 구축・운영하는 것이 필요하다.

가. 신청 자격

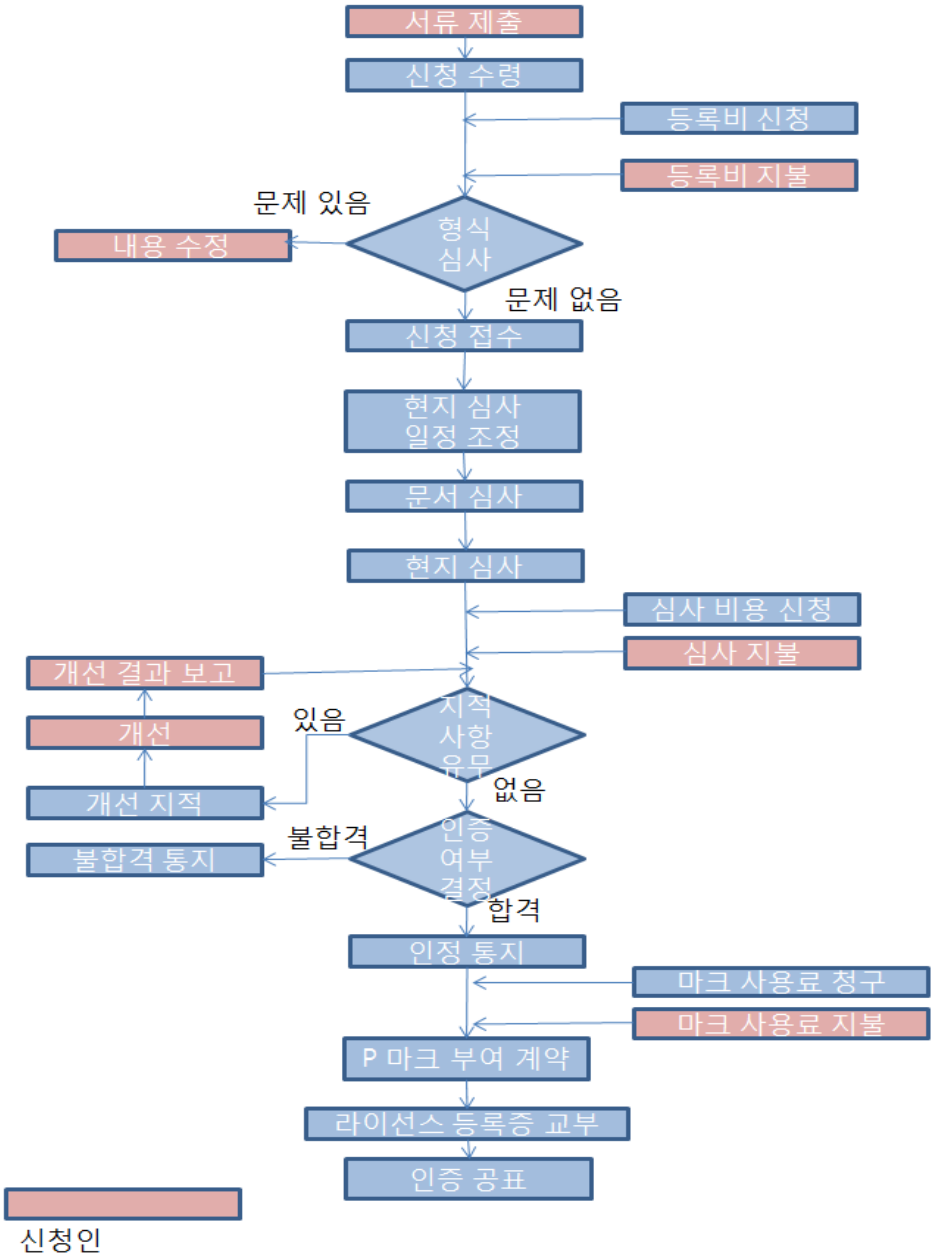
프라이버시 마크 인증을 신청할 수 있는 사업자는 원칙적으로 일본 국내에 활동 거점이 있는 민간 사업자로 정의된다. 다만, 지방자치단체 중 JIS Q 15001:2006에 따른 개인정보보호 경영시스템을 구축・운영하고 있는 경우에는 지방자치단체에서도 신청이 가능하다.

프라이버시 마크에 대한 인증은 기업 단위로 이루어지며, 기본적으로 JIS Q 15001:2006(개인정보보호 경영시스템 - 요구사항)에 따른 개인정보보호 경영시스템(PMS)을 구축・운영하고 있는 기업이어야 한다.

나. 신청 절차

신청 절차는 다음 그림과 같이 이루어진다. 신청인이 신청서류를 작성하면 신청서류에 대한 심사를 수행한다. 서류에 문제가 없으면 문서심사와 현지실사를 수행하고, 신청인이 이에 대한 심사비용을 지불하면 심사

결과를 받을 수 있다. 심사인증이 통과되면 프라이버시 마크 사용에 대한 계약을 체결한다.



(그림 D-2) 신청절차

다. 심사기준

프라이버시 마크 인증을 신청하는 기업들은 JIS Q 15001의 요구사항과 산업계 가이드라인(JIS Q 15001, 4.4.1)의 요구사항을 충족하는 준수 프로그램의 구성, 실행, 운영, 개선 부문에 대해 평가를 받게 된다.

프라이버시 마크 인증심사는 공식시험, 예비시험, 주 시험으로 구성되며, 일단 시험을 통과하면 인증서 부여기관인 일본 정보처리 개발협회(JIPDEC)와 프라이버시 마크의 사용에 대한 라이센스 계약을 체결하게 된다. 인증심사의 주요 내용은 다음과 같다.

(표 D-3) 인증심사내용

구 분	내 용
개인정보보호 정책 (JIS Q 15001)	다음 사항에 대한 정책 수립, 공표, 실행 및 운영 - 개인정보의 적절한 관리 - 개인정보의 불법 접근, 파괴, 유출, 손실 - 개인정보의 수정 - 개인정보와 관련된 법률 및 규제에 대한 엄격한 준수 - 내부 준수 프로그램의 지속적인 개선
계획 (JIS Q 15001)	- 개인정보와 위험에 대한 사항 - 개인정보와 관련된 법과 기타 규제 - 개인정보와 관련된 준수 프로그램의 실행에서 기업 내부의 개인 정보나 데이터를 보호하기 위한 내부 통제 - 관련 부서의 교육 및 감사와 관련된 기본 계획
시행과 운영 (JIS Q 15001)	- 개인정보보호 정책, 내부 통제, 그리고 다양한 계획과 연계한 준수 프로그램을 적절하게 시행하는지 여부
감사 (JIS Q 15001)	- 준수 프로그램의 운영 상태에 대한 감사
사업자 대표자를 통한 검토 (JIS Q 15001)	- 준수 프로그램의 주기적인 검토

2. 프라이버시 마크 부여 비용

(표 D-4) 프라이버시 마크 사용료

신규			
	사업자의 규모별 요금 (엔)		
	소규모 사업자	중소 사업자	대규모 사업자
등록비	50,000	50,000	50,000
심사비용	200,000	450,000	950,000
마크사용료	50,000	100,000	200,000
합계	300,000	600,000	1,200,000
갱신			
	사업자의 규모별 요금 (엔)		
	소규모 사업자	중소 사업자	대규모 사업자
등록비	50,000	50,000	50,000
심사비용	120,000	300,000	650,000
마크사용료	50,000	100,000	200,000
합계	220,000	450,000	900,000

프라이버시 마크를 사용하기 위해 지불해야 하는 비용은 위의 표와 같으며 인증서 유효기간은 2년이며, 갱신은 2년마다 이루어진다. 프라이버시 마크 사용료는 해당 사업자가 직접 프라이버시 마크 부여 기관(JIPDEC)에 납부해야 한다. 사업자 규모의 구분에서 대형 사업자는 중소 사업자 규모 이상의 사업자를 말하며, 소규모 사업자는 직원 수가 20명 이하의 사업자에 해당된다. 특히, 서비스업에 속하는 경우에는 5인 이내를 말한다.

(표 D-5) 사용료 부여 기준

	제조업 기타	도매업	소매업	서비스업
자본금	3억엔 이하	1억엔 이하	5천만엔 이하	5천만엔 이하
직원	300명 이하	100명 이하	50명 이하	100 이하

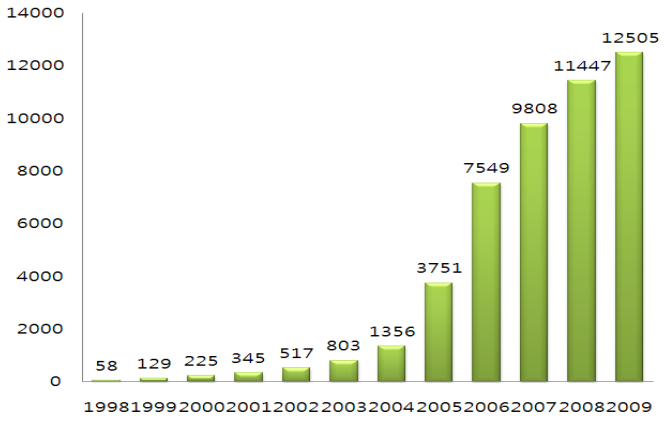
3. 프라이버시 마크 만료 취소

프라이버시 마크를 갱신하기 위한 절차는 마크의 유효기간 만료 전 4개월 이내 3개월 전에 신청서류를 지정기관에 제출하여 갱신을 위한 심사를 받아야 한다. 제출서류, 심사방법은 기본적으로 신규신청 시와 동일하며, 프라이버시 마크 제도의 운영에 문제가 있는 사업자는 비록 유효기간 내라고 하더라도 프라이버시 마크 인증을 해지할 수 있다.

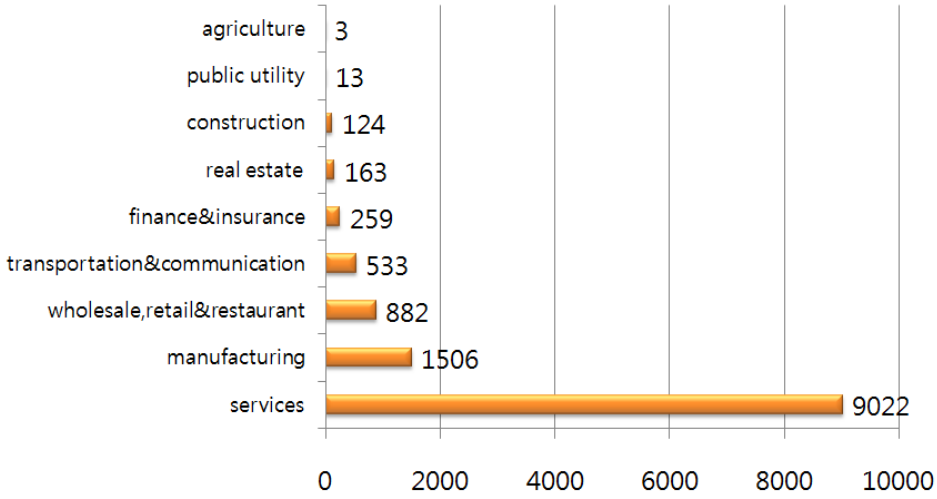
4. 프라이버시 마크 인가 현황

현재 프라이버시 마크를 입찰 조건이나 계약자 선정의 기준으로 하는 사례가 증가하고 있어 프라이버시 마크를 사용하는 기업들이 빠르게 증가하고 있다. 아래 그림에서와 같이 1998년 프라이버시 마크 취득 기업 수는 58개였으나, 2009년 기준으로 12,505개로 증가하였다.

또한 산업별 동향을 살펴보면 서비스분야의 프라이버시 마크 취득이 전체의 72%를 차지하여 서비스분야의 산업이 개인정보보호에 가장 앞장서고 있으며, 제조(12%), 도·소매 유통 및 음식점(7%)이 그 뒤를 차지하고 있다.



(그림 D-3) 프라이버시 마크 취득 현황



(그림 D-4) 산업별 프라이버시 마크 인가 현황

인터넷전화(VoIP) 사업자 정보보호 모델 연구

인 쇄 : 2011 년 12 월
발 행 : 2011 년 12 월

발행인 : 서 종 렬
발행처 : 한국인터넷진흥원(KISA, Korea Internet&Security Agency)
서울시 송파구 중대로 109 대동빌딩
Tel: (02) 4055-114
인쇄처 : 한 터
Tel: (042) 825-1484

<비매품>