情 報 保 護 學 會 誌
第17卷 第1號, 2007. 2

# 바이오 정보를 이용한 U-HealthCare 인증방안 연구

김재성*, 김영준**

요 약

본 논문에서는 바이오인식 정보 기술(얼굴, 정맥, 지문, 홍채)을 이용하여 신뢰성 있는 Ubiquitous-HealthCare(U-HC) 서비스를 지원하는 사용자 인증 메커니즘과 암호화 기법을 제안한다. U-HC 서비스에 태동 및 특징, 국내외 산업현황, 기대효과 등을 통해 U-HC서비스의 필요성을 강조하고 있다. 하지만 지능화 및 고도화된 기술을 통하여 개인 정보를 악의적인 의도로 유출하여 개인에게 육체적·정신적·경제적 피해를 주고 있다. 바이오인식은 이러한 피해를 막고 보안 및 프라이버시 측면의 취약점 및 공격들을 분석하여 효율적으로 방어함으로서 개인의 의료정보 및 바이오 정보를 보호하기 위한 대응책인 새로운 사용자 인증과 암호화 기법이다. 사용자 인증 기법은 다수의 바이오 정보들을 인증 시에 무작위로 선택하여 2개 이상 입력하는 방안이며 암호화 기법은 사용자 스토리(Story)식 암호화(Encryption) 기법을 제안한다. 이러한 방법론을 통하여 효율적이며 신뢰 성 있는 U-HC 서비스를 보장하고자 한다.

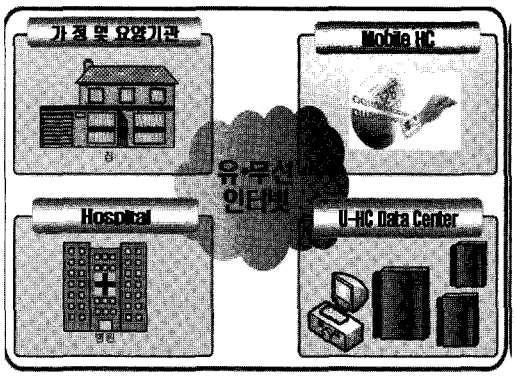
## Ⅰ. 서 론

최근 우리 사회는 '육체적·정신적 건강의 조화를 통해 행복하고 아름다운 삶을 추구하는 웰빙(Wellbeing)' 열풍에 휩싸여있다. 이러한 사회적 현상의 이면(裏面)에는 건강한 삶과 삶의 질 향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 사용자의 욕구를 반영한다. 이러한 시스템으로서 언제, 어디서나, 누구든지 의료 및 의료정보 서비스를 이용할 수 있는 Ubiquitous-Healthcare (U-HC)에 대한 관심이 높아지고 있다. 특히 한국은 세계 최고의 초고속 유무선 정보 통신망을 활용하여 시간과 장소에 구애받지 않고 의료서비스를 제공하는 시스템을 갖추고자 정부를 비롯하여 산학연이 하나가 되어 노력하고 있다. 특히 몇몇 지자체(부산, 대구)에서는 U-HC 산업 육성을 위한 지역혁신체계를 구축하고자 시범운영 센터를 구축 및 운영 중이며 산학연관 네트워크를 구축 하여 U-HC 상품 및 기술 개발, 전문 인력 양성, 관련 기업지원 서비스, 마케팅을 통하여 U-HC 산업 활성화에 박차를 가하고 있다[1]. 하지만 인간의 행복을 위한 삶의 질 향상을 목적으로 하는 U-HC 서비스의 이면(裏面)에는 개인 신상 및 바이오정보 유출 등 개인 프라이버시(Privacy) 침해 가능성을 지니고 있다. 이러한 침해 가능 정보는 개인 신상 정보뿐만 아니라 개인 의료정보 및 바이오 정보를 포함한 지극히 개인적인 정보들이기 때문이다. 특히 우려되는 점은 일부 악의적인 의도를 가진 전문가들이 지능화 및 고도화된 기술을 통하여 개인의 신상정보 및 바이오정보를 유출시켜 개인에게 육체적·정신적·경제적 피해를 주기 때문이다. 따라서 본 논문에서는 보안 및 프라이버시 측면에서 존재하는 취약점 및 공격들을 효율적으로 방어하여 개인의 의료정보 및 바이오 정보를 보호하기 위한 기술적인 대응책을 제안하고자 한다.

## Ⅱ. U-HC 서비스

다른 산업과 마찬가지로 U-HC 서비스 산업의 발전은 정부를 비롯하여 개인, 학교, 기업, 병원과의 유기적인 관계 속에서 이뤄진다. 일반적으로 정보통신분야와

* 한국정보보호진흥원(KISA) 바이오인식정보시험센터(K-NBTC) 팀장 (jskim@kisa.or.kr)
** 한국정보보호진흥원(KISA) 바이오인식정보시험센터(K-NBTC) 연구원 (yjkim412@kisa.or.kr)




〔그림 1〕 U-HC 개념도

보건의료분야의 단순한 연결이 아닌 관련된 모든 분야의 기술이 융합되어 서비스를 지원하는 "종합 의료 서비스 시스템"이라 정의하고자 한다. 기존의 종이차트로 관리되고 서비스 되던 "2차원적 의료 서비스"에서 EMR (전자의무기록), OCS(처방전달시스템), PACS(의료영상 저장전송시스템) 등 한 단계 발전된 의료정보 시스템을 통해 "3차원적 의료 서비스"를 제공하였다. 최근에는 유비쿼터스 관련 기술들을 의료 분야와 융합하여 "4차원적 의료 서비스"를 제공하는 U-HC서비스에 첫 걸음을 내딛었다. 이러한 U-HC의 개념도를 〔그림 1〕에서 간략히 보여준다.

### 2.1 U-HC의 태동(胎動) 및 특징

앞서 말했듯이 U-HC는 육체적·정신적 건강의 조화를 통해 행복하고 아름다운 삶을 추구하고자 하는 우리 사회의 삶의 풍토가 반영된 결과라 할 수 있다. 더욱 자세히 그 내면을 들여다보면 정보통신 기술발전과 의료 선진화를 앞당기기 위한 의료 분야의 열망과도 맞물려 있다. U-HC는 의료 시스템의 Overload, 사회 고령화, 의료비 상승 등의 문제점을 해결하는 핵심 역할을 담당한다. U-HC 개념은 기존의 사고를 탈피하고 이용자 중심의 편의를 증대시키기 위하여 원격진단 및 의료 등 물리적 공간의 제약을 극복하고 이용자가 원하는 장소와 시간에 서비스하고자 하는데 목적을 두고 있다. 이렇게 국내외에서 첫발걸음을 내딛게 된 U-HC의 장점을 크게 3가지로 간추려 보았다. 첫째, 시간과 비용의 절감, 둘째, 의료 과정의 첨단 시스템화를 통한 국제 경쟁력 향상, 셋째, 국민의 삶의 질 향상이다. 하지만 이러한 장점들의 이면(裏面)에는 심각한 보안상의 문제들이 존재한다.

### 2.2 U-HC 산업 현황

국내외 U-HC 산업은 RFID[2], ZigBee[2], 웨어러블 시스템[3], 각종 센서[4], 네트워크 기술 등 관련 주요 기술 및 산업과의 융합을 통해 성장하고 있다.

국외 현황을 살펴보기 위하여 미국 U-HC 시장의 발전 양상을 살펴보자. 미국 정부는 국가 수준의 의료 정보화 정책 등을 추진하여 IT, 통신, 의료 관련 대형 기업들을 중심으로 산업이 성장하고 있으며 의료 정보화 분야는 중소기업 위주로 성장하고 있다[5].

Elite care의 Oatfield Estates는 고령자를 대상으로 양로원을 운영하며 다음과 같은 서비스를 수행 중이다[6].

- 건강체크 변기센서
- 침대센서
- 약 복용 알림 시스템

Vetern Health Administration은 Health Buddy 시범 서비스를 실시하며 내용은 다음과 같다[5].

- 가정 내 디바이스를 통한 환자 관리 및 방문 간호사

그 외 진행되는 대표적인 관련연구는 조지아 공대는 Aware Home 시스템, 로체스터 대학의 Smart Medical Home 시스템, MIT는 FID 관련 U-HC 연구 들이 있다[5].

일본의 후생성은 소규모 다기능형 주택, 치매성 노인 그룹홈, 소규모 헬스케어 전용 특정 시설 등 홈 네트워크를 이용한 U-HC 시스템 구현에 박차를 가하고 있다[5]. 유럽은 2002년 5월부터 14개 기관에 의해 Mobile Health Project를 진행하여 모바일 헬스케어 시스템 개발에 대한 유용성 실험을 실시하였고 네덜란드 기반의 Helpt Elkander는 노인용 임대 아파트에 U-HC 서비스를 제공하고 있다[5].

국내 산업은 정부 육성 정책에 따라 정통부, 산자부, 복지부 등을 중심으로 U-HC 산업 육성 및 상용 서비스를 지원하고 있다. 또한 병원 및 관련 기업들 간의 제휴와 산학연을 통한 기술개발 등 U-HC에 관련 연구가 진행 중이다. 특히, 활발히 활동 중인 관련 기업 들 중 SK Telecom의 U-HC 서비스 분야를 살펴보면, 당뇨질환, 고혈압질환, 만성호흡기, 근골격계질환 관리 서비스, U-건강모니터링, U-원격의료, 웨어러블 기반 건강 모니터링 서비스 등 다각도로 연구가 진행 중이며 서비스를 제공하고자 관련 기관들과 시스템을 구축 중이다[6]. 지자체의 U-HC를 위한 산업 연구를 살펴보면 부산시는

'복지기관과 의료기관을 연계한 U-헬스 서비스', 대구시는 '웨어러블 컴퓨터 기반의 U-HC 서비스'등 상용 서비스를 제공하기위해 지역혁신체계를 구축 중이다[5]. 또한 병원들의 U-HC 서비스 제공을 위하여 관련 SI 업체들의 U-HC 시장 경쟁도 심화되고 있어 국내 산업 활성화 및 국제 경쟁력 향상에 많은 기여를 하고 있다.

### 2.3 U-HC 기대효과

우리 삶의 모든 공간에서 U-HC 서비스를 제공하기 위해서는 센서 및 모바일 관련 디바이스 기술, 대용량의 데이터 저장 및 처리 기술, 유무선 네트워크 기술 등 관련 산업의 지원이 필요하다. 이러한 기술적인 지원 하에 U-HC 서비스를 통하여 기대되는 효과는 많은 긍정적인 요소들을 포함하고 있다. 이용자 측면에서는 다양한 의료 정보 접근이 용이하며, 삶에 질 향상에 대한 욕구 충족 등과 같은 이용자 중심의 서비스 이용이 가능하다[7]. 의료기관 측면에서는 신속한 진료서비스 체계 구축, 쌍방향(기관 및 고객) 중심의 의료 서비스 제공, 진료서비스 수준 향상 등을 통한 수익 증대를 가져온다. 제약 및 제조사 등 관련 산업 측면에서는 거래 투명성 제고, 업무 프로세스 단축, 부대비용 절감에 따른 신제품 연구, 개발 투자여력 확보 등의 장점을 지닌다. 정보통신 사업자 측면에서는 의료시장 진출의 초석을 마련할 뿐만 아니라 의료 서비스와의 연계를 통한 신규 사업 창출을 통한 수익 증대의 장점을 지닌다. 특히 국가적 측면에서도 의료 IT화에 소요되는 총비용 절감, 의료서비스 국제 경쟁력 향상, 의료서비스 생산성 및 생산량 확대 등을 들 수 있다[7].

하지만 이러한 U-HC의 장점, 산업 활성화 및 그에 따른 기대효과를 얻기 위해 정부 및 의료 기관, 관련 연구기관, 기업, 학교 등 모든 곳에서 발을 벗고 앞서나가지만, 보이지 않는 이면에는 심각한 문제가 도사리고 있다. 특히 악의적인 의도로 사용자에 지극히 개인적인 신상 및 개인 병력, 개인 바이오 정보 유출 등을 통한 불법 사용에서 비롯되는 문제점들은 사회적으로 심각한 이슈로 대두된다. 본 논문에서는 이러한 보안상 취약점에 대한 요구를 살펴보고 그 대응책을 제시하고자 한다.

## Ⅲ. U-HC 보안 요구

개인 프라이버시 침해 가능성을 줄이고 신뢰성을 갖춘 U-HC 서비스를 제공하기 위하여 보안기능이 필수적이며 이러한 보안기술로서 PKI 및 암호화 기술들이 활용되고 있다[8]. 신뢰성있는 서비스를 지원하기 위해 미국의 경우 HIPAA의 Privacy & Security Rule 적용을 통해 모든 의료 정보 및 서비스에 대하여 보안 메커니즘을 필수적으로 적용하여 시행하고 있다[8]. 우리나라도 법적, 제도적 및 기술적 측면에서 개인 프라이버시 침해를 막고 신뢰성 있는 U-HC 서비스 지원을 통해 산업 활성화를 이루고자 온힘을 쏟고 있다. U-HC 서비스 상에서 개인 프라이버시 침해 가능성 있는 정보는 지극히 개인적인 신상정보, 가족력, 신체적 특징, 질병 정보, 바이오 정보 등이 있다. 본 장에서는 이러한 U-HC 서비스의 신뢰성을 보장하기 위한 보안상 요구사항을 유형별로 분석하였다.

### 3.1 U-HC 취약성, 침해 및 공격유형

U-HC 보안상 취약점은 다른 온라인 서비스들과 마찬가지로 기존 유무선 네트워크상에서 겪게 되는 다양한 취약성들이 존재하며 추가적으로 U-HC에 사용되는 새로운 장비들과의 네트워크상에서 존재하는 신규 취약성들이 존재한다. 이러한 서비스 취약점을 노린 공격 유형에는 첫째, 서비스를 지원하는 서버를 공격하는 DoS attack유형이 있다. 이러한 공격은 서비스 서버로의 사용자 접속을 막고 다른 위장 서버로 연결되도록 유도한 후 개인의 인증정보 등을 습득하여 악의적으로 이용하는 습법이다. 둘째, 바이러스/웜 해킹 공격 유형이다. 이러한 공격은 서비스 제공 서버에 정상적인 사용자로 위장하여 접속을 시도하여 실제 사용자들의 정보를 변경하거나 삭제 하여 U-HC 서비스 가입자들의 접속을 막는 유형이다. 셋째, 의료정보 도청/위변조 공격 유형이다. 의료 정보 및 서비스 결과 전송 시 의료 정보를 도청 및 감청 하여 정보를 수정하고 서비스 결과를 변조하여 전송하는 공격 유형이다. 넷째, 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형이다. 특히 유·무선 인프라를 통한 게이트웨이 나 다양한 서버들을 불법적으로 집중 공격하는 방법들이 있다. 다섯째, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기(센서, 의료기) 마비, 방해전파, 화재 와 같은 인재(人災) 또는 악의적인 행위를 통한 공격유형이다. 마지막으로 여러 가지 공격에 따른 대표적인 침해 유형을 살펴보면 다음과 같다. 첫째, 네트워크상에서 패킷을 캡쳐(Capture)하여 패

스워드, 중요 데이터 및 특정 서비스 기능에 관련된 정보를 도청하여 수집한다. 둘째, 프로토콜의 취약점을 이용(IP Spoofing, Prediction 등)하여 정당한 사용자나 시스템으로 신분 위장하여 각종 게이트웨이를 공격한다. 셋째, 게이트웨이나 무선AP를 대상으로 네트워크 사용량을 초과 하도록 대량의 메일을 보내거나 다량의 무선랜 접속 요구를 통해 서비스거부 공격을 한다. 마지막으로 서비스의 사용량 수집 및 개인 정보 수집을 통한 프라이버시 침해를 목적으로 하는 정보수집이 있다.

## Ⅳ. 침해위협에 따른 대응 방안

앞에서 살펴 본 침해위협에 따른 대응 방안을 2가지 측면에서 접근 하고자 한다. 첫째, 기존의 대응 방안들을 살펴본다. 둘째, 개인 프라이버시 침해 가능성이 큰 개인 신상 정보 및 의료 정보 보호를 위한 대응 방안을 새롭게 제안하고자 한다.

### 4.1 기존 대응 방안

첫째, 인증 프레임워크 메커니즘을 통한 다단계 서비스 접근인증 방법이 있다. 최종적으로 U-HC 서비스 및 기기 접근을 하기 위하여 외부 서비스 사업자를 통한 CP 서비스 접근인증, 사업자 인증 서버 접근을 위한 네트워크 사업자 제공 U-HC 서비스 접근인증 및 원격 접근 인증, 지역 인증 서버를 통한 원격 접근 인증, 홈 및 병원 내 게이트웨이나 서버에 보안기능을 탑재한 기기 접근 인증 방법이 있다. 이렇듯 인증·프레임워크 메커니즘을 통한 다단계 서비스 접근인증을 통한 신뢰성 확보 방안이 필요하다.

둘째, 기기 및 사용자 인증 메커니즘을 이용한 대응 방안이다. U-HC 디바이스를 이용한 서비스 이용 시 서버나 게이트웨이 접근 시 U-HC 기기와 서로 인증을 통한 서비스 허용 방법이다. 프로세스(Process)를 살펴보면 U-HC 디바이스 및 서버나 게이트웨이 간에 디바이스 등록 및 인증 요청, 키 교환, 디바이스 인증정보 전송, 인증 결과 전송 후 서비스를 제공한다. 사용자 인증 메커니즘도 동일한 방법으로서 서비스 요청 시 서버 인증서 전송, 인증 키 교환 과정을 수행 후 서비스를 이용한다.

셋째, 인프라 기반의 다양한 대응 방안들의 필요성을 살펴보자. 서비스 거부 공격에 대한 대응 방안으로서 단자함의 물리적인 보안을 통한 접근 제어에 있어서 서비스 액세스의 우선순위 지정과 같은 엄격한 인증 및 접근제어 방안이 필요하다. 또한 불법 접근 공격을 방어하기 위하여 기밀성을 제공하는 암호화 기법을 사용하여 인증 체계를 강화하는 방안이 필요하다. 또한 도난, 분실, 복제, 도청에 따른 인증 강화 대책이 필요하며 바이러스/웜, 해킹, 위/변조 공격에 대응하기 위하여 방화벽, VPN 등의 방어기술 및 보안이 강화된 인증 방법 도입이 절실하다[9].

따라서 이러한 침해위협에 대응하고자 기밀성, 무결성, 가용성을 제공하는 암호화 기법과 인증 강화 기법이 필요하다. 특히, 인증 방식에 대한 인증 서비스 신뢰성을 보장하기 위한 방안으로 바이오인식 정보를 이용한 사용자 인증과 암호화 기법을 제안하고자 한다.

### 4.2 사용자 인증 및 암호화 기법

바이오 인식 정보는 한 개인에게만 존재하는 독특한 정보이며 노출 위험도 적은 편이다. 하지만 개인의 바이오정보도 공인 인증서 기반이나, 비밀번호, 주민 번호와 같이 침해 가능성이 존재한다. 따라서 이러한 문제점을 해결하기 위한 방안으로 U-HC 의료서비스 및 정보 이용 시 2개 이상의 바이오 정보 입력 및 무작위 바이오 정보 선택 입력 방안을 제시한다. 우선 바이오 인식 정보에 대한 기술적인 면은 생략하고 사용자 인증 방법론에 대하여 논하고자 한다. 바이오 인식 정보에 주로 활용되는 생체 정보는 정맥, 홍채, 지문, 얼굴 등이 사용된다. 정맥 또한 열개의 손가락 정맥, 좌우 손등 정맥, 좌우 홍채, 열개의 손가락 지문 및 얼굴 등 다수의 바이오 정보들이 존재한다. 이러한 다수의 바이오 정보들을 인증 시에 무작위로 선택하여 2개 이상 입력하는 방안을 통하여 강화된 인증을 수행한다. 물론 이를 통해 기밀성 측면은 강화 되겠지만 성능 면에서 떨어지는 경우가 발생되며 수많은 바이오 정보를 저장하는 문제도 발생된다. 또한 무결성 측면은 좀 더 보완 연구가 필요하다. 하지만, 앞서 언급했던 가용성 측면에서의 문제는 하드웨어적인 기술요소(저장능력 및 성능)들이 발전함에 따라 자연스럽게 해결되리라 기대된다. 따라서 가용성 및 무결성 측면은 앞으로 개선되리라는 전제하에 기밀성 측면을 보완한 방안이다. 또한 바이오 정보 저장 및 전송 시 필요한 암호화 기법으로 기존의 공개키 알고리즘을 통한 암호화(PKI) 기법에 추가적인 이중 삼중 암호

화를 스토리(Story)식으로 추가하는 방안이다. 물론 이중 삼중 암호화를 하기 위하여 사용자 기기에서 사용될 고유 포트 번호 및 기기 ID를 활용하여 암호화에 적용하며, 개인의 요청에 따른 다양한 정보를 암호화에 사용하는 방식을 의미한다. 즉, 공개키 알고리즘을 통한 암호화 기법 내부에 개인별 보안 Process를 따로 만들어 이중 삼중의 암호화를 하는 방법으로서 개인만이 소유한 모든 정보를 이용하여 개인이 암호 할 정보를 Story식으로 입력하는 방안이다. 마지막으로 U-HC 서비스는 개인의 병력뿐만 아니라 신상정보, 바이오 정보, 가족력 등 매우 민감한 정보들이기 때문에 기밀성을 요하는 많은 부분에서 이러한 보안 메커니즘들이 적용될 수 있으리라 생각된다. 물론 가용성 측면에서 많은 문제들이 대두 되지만 이러한 문제들은 기술적인 진보에 따라 자연스레 해결되리라 고려되기 때문에 사용자 중심의 보안 메커니즘 방안이라 할 수 있다. 또한 빠른 성능을 원하는 사용자가 있다면 암호화 기법을 단순화한 방안을 사용하는 것도 권장된다.

## V. 결 론

본 논문에서는 바이오인식 정보 기술(얼굴, 정맥, 지문, 홍채) 시스템을 이용하여 신뢰성 있는 U-HC 서비스를 지원하는 사용자 인증 메커니즘과 암호화 기법을 제안하였다.

이 기법을 제안하기에 앞서 U-HC 서비스에 태동 및 특징에 대하여 간략히 살펴보았고 국내외 산업현황을 살펴봄으로서 서비스 필요성을 강조하였다. 또한 기대효과와 파급 효과를 통해 얻을 수 있는 장점들을 살펴보았다. 하지만 수많은 장점들 이면에는 심각한 보안상 문제가 도사리고 있다. 특히 악의적인 의도로 사용자의 지극히 개인적인 신상 및 개인 병력, 개인 바이오 정보 유출을 통한 불법적인 사용에서 비롯되는 문제점들은 사회적으로 심각한 상황으로 대두된다.

본 논문에서는 이러한 보안상 취약점에 대한 요구를 살펴보고 그 대응책을 제시하였다. 보안 및 프라이버시 측면의 취약점 및 공격들을 분석하여 효율적으로 방어함으로서 개인의 의료정보 및 바이오 정보를 보호하기 위한 대응책으로서 새로운 사용자 인증과 암호화 기법을 제안 하였다. 사용자 인증 기법은 다수의 바이오 정보들을 인증 시에 무작위로 선택하여 2개 이상 입력하는 방안이며 암호화 기법은 사용자 스토리(Story)식 암호화(Encryption) 기법으로서 사용자가 원하는 다양한 정보를 스토리 식으로 적용하는 방안이다. 이러한 기법을 통하여 효율적이며 신뢰성 있는 U-HC 서비스를 보장하고자 한다.

향후 이러한 사용자 인증 기법과 스토리(Story)식 암호화 기법에 대한 기술적인 연구를 수행하여 기밀성, 무결성, 가용성 측면에서 타당성을 검증하고자 한다.

## 참고문헌


[1] 전계록. "고령친화 U-Health Care 산업 육성을 위한 지역혁신체계 구축," 부산대학교병원 RIS 사업단

[2] 김진태, 권영미, "RFID와 ZigBee를 이용한 유비쿼터스 U-Health 시스템 구현," 전자공학회 논문지 제 43권 TC편 제1호, Jan 2006.

[3] 손미숙, "U-Health 서비스 지원을 위한 웨어러블 시스템," 전자통신동향분석 제21권 제3호 June 2006.

[4] 이정환, "유비쿼터스 센서기술과 u-Health," www.fkii.or.kr

[5] "U-Health 시장 현황 및 전망," MindBranch Asia Packfic Co. Ltd, Oct 2005.

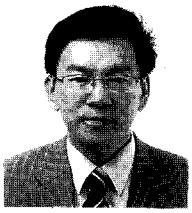
[6] http://www.sktuhealth.co.kr/

[7] 지경용. "국내 U-city에서 u-Health 사업 환경 분석," 네트워크 경제연구팀 한국전자통신연구원, 2005.

[8] 송지은, 김신효, 정명예, 정교일, "U-헬스케어 보안 이슈 및 기술 동향" 전자통신동향분석, 제22권 제1호 Feb 2007.

[9] 김재성, "생체인식시스템 표준적합성 및 보안성 평가모델," 박사학위논문, Aug 2005.

## 〈著者紹介〉

**김 재 성 (Kim Jason) 정회원**

86년 3월 : 인하대학교 전자계산학과 학사
89년 3월 : 인하대학교 이학석사
05년 8월 : 인하대학교 공학과 박사
89년12월 : LG 정보통신 중앙연구소 TDX-10 개발(연구원)
90년~95년 : 한국전자통신연구원(ETRI) 이동통신연구소(선임연구원)
96년 7월~현재 : 한국정보보호진흥원 산업지원팀 바이오인식정보시험센터(팀장)
02년 2월~현재 : TTA PG103 국내표준화 의장, 산자부 기표원 SC37-Korea 전문위원
03년 7월~현재 : ISO SC37 · ITU-T SG17 국제표준 프로젝트 에디터
03년 7월 ~ 현재 : ABF(아시아) · UK BWG(영국) · EBF(유럽) 바이오인식기술 전문위원
관심분야 : 정보보호, 바이오인식정보, 패턴인식 등

**김 영 준 (Kim Youngjun)**

02년 8월 : 홍익대학교 공학과 졸업
06년 2월 : 한국정보통신대학교(ICU) 공학과 석사
06년 12월 ~ : 한국정보보호진흥원(KISA)
관심분야 : 정보보호, 바이오인식정보, 시스템&네트워크 등