JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 11 : 2683~2688 Nov. 2015

IoT 환경의 의료 정보보호와 표준 기술

우성희*

Medical Information Security and Standard Technology On IoT Environment

Sung-hee Woo*

Department of Medical Information & Technology Engineering, Korea National University of Transportation, Chungbuk, 368-701, Korea

요 약

사물인터넷은 다양한 기술을 융・복합적으로 사용하여 사용자에게 편리하고 다양한 서비스를 제공한다. 그중 의료서비스 분야와의 융・복합이 주목을 받고 있다. 하지만 이런 사물인터넷의 등장 및 성장과 함께 의료서비스가 진화할수록 개인의료정보의 유출로 인한 보안문제는 더 심각해질 것이다. 특히 유헬스 의료기기 등은 개인의 건강정보를 주로 다루기 때문에 의료 정보 만큼의 높은 수준의 개인정보보호 및 보안이 요구된다. 따라서 헬스케어 산업에 사물인터넷의 도입은 의료정보보안이 전제 조건이 되어야 할 것이다. 본 연구에서는 사물인터넷의 보안동향과 의료분야의 개인정보 유출사례, 개인의료정보의 생명주기에 따른 의료정보보호 방안과 표준기술을 분석한다.

ABSTRACT

Internet of Things(IoT) using a variety of technologies in combination provides a convenient, elevated range of services to users. IoT has been noted in combining the fields of medical service in particular. However, with the advent and growing of IoT, the more medical services are evolving, security problems caused by leakage of personal health information will become more serious. U-Health and medical devices, which deal mainly the personal health information, is required to a high level of privacy and security of health information. Therefore, the introduction of the IoT in the healthcare industry requires the medical information security as a prerequisite. This study analyzes security status and trend of IoT, personal medical information leakage cases, the health information protection measures in accordance with the life cycle of medical information, and the standardized protection technologies.

키워드 : IoT, 의료정보보안, 의료정보기술 표준, 사물인터넷 보안

Key word : Internet of Thing, Medical Information Security, Medical Information Standard Technology, IoT Security

Received 02 October 2015, **Revised** 30 October 2015, **Accepted** 09 November 2015

* **Corresponding Author** Sung-Hee Woo(E-mail:shwoo@ut.ac.kr, Tel:+82-43-820-5323)
Department of Medical Information & Technology Engineering, Korea National University of Transportation, Chungbuk 368-701, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.11.2683 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

의료 서비스 품질 향상에 대한 요구와 관심이 증가하면서 헬스케어 업계에 사물인터넷 도입으로 의료비 절감과 서비스 제고의 시도가 활발히 이루어지고 있다. 그 예로, 전 세계 병원들을 중심으로 사물인터넷(Internet of Things, IoT) 기술을 도입해 스마트 병원 시스템을 구축하는 사례가 증가하고 있다. 미국의 대형 병원들은 실시간 추적 시스템을 통해 환자·의료진·설비의 위치와 동선 및 특정 움직임을 모니터링하고 의료 데이터로의 접근을 종합적으로 관리하는 시스템을 구축하였으며 프랑스, 인도에서는 스마트폰, 태블릿 PC, 웨어러블 단말 등을 이용해 원격 환자 모니터링, 고령자들의 홈케어, 만성질환 치료 및 관리와 같은 개인적인 의료 서비스 부문에 접목함으로써 소비자 의료비 절감과 품질 향상 등의 효과를 창출하고 있다. 그러나 사물인터넷의 도입이 긍정적이지만은 않다. 그것은 개인 의료 정보의 침해의 위험성을 높인다는 부정적 측면을 가지고 있기 때문이다. 개인 의료정보는 개인의 건강정보를 다루기 때문에 유출에 따른 피해의 파급효과가 클 것이다. 따라서 헬스케어 산업에 사물인터넷의 도입[1]은 의료정보보안이 전제 조건이 되어야 할 것이다. 본 연구의 2장에서는 사물인터넷을 위한 보안 관련 국내외 동향과 기술, 3장에서는 개인정보 유출사례, 4장에서는 의료정보의 생명주기에 따른 침해위협요소들과 보호방안 그리고 표준화기구들의 의료정보보호표준기술을 분석한다.

Ⅱ. 사물인터넷과 보안

2015년 가장 큰 이슈는 사물인터넷이다. 기기와 네트워크, 사물과 사람, 사물과 사물을 연결하는 기술로 우리의 삶을 더 편리하게 하였지만 홈 가전 시스템의 해킹으로 사생활 노출 위험, 스마트 TV나 스마트 냉장고 정보가 스팸메일 발송, 스미싱등 범죄에 악용되거나 자동차나 병원 의료기기 시스템의 정보가 유출되어 생명의 위협까지 받을 수 있는 상황이 될 수 있다. 사물인터넷 시대는 이러한 보안 문제가 반드시 전제되어야 할 것이다.

예로 지난해 11월 인터넷과 연결된 가정용 CCTV가 해킹되어 러시아의 특정 사이트에서 생중계되는 일이 있었고 6,000여 대의 우리나라 CCTV도 타켓이 되었다. 지난해 4월에는 유무선 공유기 해킹으로 1,700여 명의 개인정보가 유출되기도 하였다. 사물인터넷 기기를 이용한 디도스 공격과 악성코드 유포도 예측된다. 사물인터넷 간 디바이스 공격 유형의 예로는 다음 표 1에 표시된 공격 이외에도 Interface/Jamming/Collision, Sybil, Traffic Analysis, De-synchronization, Spooling등 많은 IoT 디바이스 공격 유형[2]들이 존재한다.

Table. 1 Attack types of IoT devices

공격명	설 명
Dos	주변 노드에 지속적인 광고패킷을 송신, 반복수정, CRC 반복체크로 시스템에 무리를 주거나 주파수 잼을 통해 신호 송수신 방해
Wormhole	통신이 허가되지 않은 두 장치의 무선통신 모듈, 통신 라우팅을 고의로 변경하거나 악성코드 배포 경로로 이용
Tampering	단말에 저장된 데이터 혹은 송수신 데이터를 임의로 위변조
Eavesdropping	암호화 되지 않은 디바이스와 게이트 웨이간 정보 도청

따라서 업체들은 별도 보안 조직을 운영하거나 사용자 인증을 강화하고, 제품 기획과 설계 단계에서 정보보호를 위한 연구를 하고 있으며 정부는 지난해 10월 사물인터넷 정보 보호 로드맵을 발표하고 핵심기술 개발, 사물인터넷 보안 산업 경쟁력 강화 등을 추진하고 있다. 특히 가전·의료기기 및 자동차 등 사물인터넷의 활용 분야가 우리 실생활의 모든 사물에 접목될 수 있기 때문에 사물인터넷 보안위협은 사람의 생명도 위협할 만큼 큰 피해를 가져올 수 있다. 이러한 피해 예상 규모는 2020년까지 17조 7천억 원으로 추산된다. 이러한 보안위협에 대응하고 보다 안전한 사물인터넷 환경을 조성하기 위해서는 이와 관련한 법규제와 표준, 그리고 관련기술 개발 및 정책 가이드가 필요하다. 이러한 상황에서 국내외 대형 IT기업들은 사물인터넷 보안시장을 선점하기 위한 인증·암호화 분야의 신규 보안 솔루션을 개발·출시하고 있으며 관련 업체 인수를 통해 사업 영역 확대와 협력체계를 구축하고 있다. 이와 함께 전 세계적으로 IoT 보안정책 수립은 아직 초기 단계이지만 미국, 유럽 등 주요 선진국은 IoT 산업진흥과 이용

자 보호를 함께 고려한 균형 잡힌 규제방안을 정부 차원에서 검토 중이다.

특히 IoT 기반의 다양한 서비스에 보안원칙을 적용하도록 하고 있으며 관련한 지침을 개발·보급하는 등 시장 자율규제 중심의 정보보호 정책·제도를 수립하고 있다. 다만, 인간의 생명과 직결되는 의료 등의 분야에서는 의무적으로 보안을 적용하고 있다. 또 한편으로 보안을 강화하기 위해 선행되어야 할 조건이 있다면 바로 통신규격의 표준화이다. 의료정보보호 영역도 의료서비스를 위한 표준화의 한 영역으로 구분하고 ISO/TS 2220, 사용자식별, ISO/TS 22600, 사용자 인증 및 접근제어, ISO/IEC 27799 정보보호 관련체계, ISO/TS 25237 익명화 등의 표준화를 추진하고 있고, 국내의 경우는 국가 기술 표준원으로 부터 국가표준(KS) 개발, 관리 업무 활성화를 위해 표준개발협력기관(COSD, Co-operation Organization or Standards Development)을 지정하여 표준을 제정하였다.

Ⅲ. 개인의료정보 유출사례

분야별 개인정보 유출 사고의 예로 미국 비영리단체인 ITRC (Identity Theft Resource Center)의 조사 결과[3]을 보면, 그림 1과 같이 의료 분야의 개인 정보 유출 사고가 다른 산업 분야 보다 더 많은 것으로 나타났다. 또한 2015년 3월 보안뉴스에서 실시한 '보안위협 개인정보 유출 우려 분야 설문조사' 결과[3] 다음 그림 2.와 같이 1위는 금융, 2위는 의료 분야로 조사되었다. 금융 분야의 경우 작년 카드사 고객 정보 유출 사고 이후 많은 대책이 나오면서 보안 조치가 강화되고 있다. 하지만 의료 분야의 정보들은 중요도나 민감도가 금융 정보보다 더 중요 함에도 상대적으로 보호 대책이 매우 소홀한 상황이다.

개인정보 유출 문제는 항상 존재해 왔지만 의료 분야의 개인정보 유출 사례는 최근 증가하고 있다. 이유는 개인 의료기록은 보험 상품 및 진료 위치 추적 등의 용도로 활용될 수 있고 처방 약품 시장 현황, 매출 추이 분석, 주요 질병 발생 추이 등 다양한 형태로 가공되어 제약사 영업 전략과 신약 개발 방향 등을 수립하는데 활용 될 수 있기 때문이다. 따라서 개인 의료기록은 제약사들에게 매우 가치 높은 정보인 것이다.

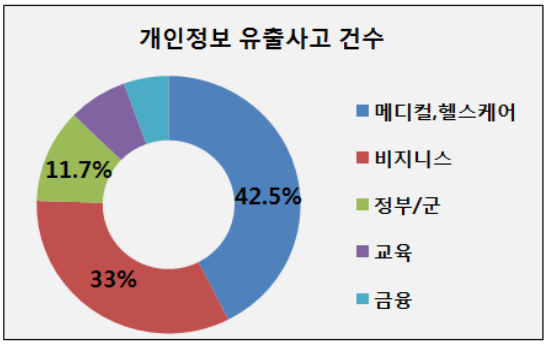

Fig. 1 Private information leakage accidents of US

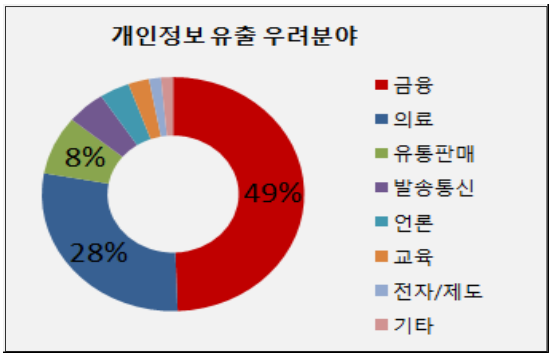

Fig. 2 The concerned field of personal information leakage in Korea

또한 해커들이 개인 정보를 거래하는 암시장에서 신용카드로 5~20 달러에 거래된다면, 개인 의료정보는 10배로 거래된다고 한다.

유출자는 의료기관 직원, 시스템개발 및 보수유지 업체이며 금전이나 호기심을 목적으로 지인과 채권추심업체, 의료정보 컨설팅 업체에게 전달된다. 이처럼 개인 의료정보는 그 가치가 높은 만큼 유출 시에 발생하는 비용도 다른 정보에 비해 높은 것으로 조사되었다. 2013년 개인 정보 보호 협회의 '개인 정보의 가치와 개인 정보 침해에 따른 사회적 비용 분석 보고서'[4]에 따르면 헬스케어 분야의 정보 유출 사고 시 가장 많은 사고 대응 비용이 소요된다고 한다. 우리나라의 의료정보 유출사고 사례[5, 6]을 보면 다음 표 2와 같다.

우리나라 건강보험 심사평가원의 년간 심사 건수가 14억 건 정도에서 5억 건 정도의 의료정보 유출은 카드사의 개인정보 유출사고 보다 더 큰 대형 유출 사고라 할 수 있다.

Table. 2 Private Medical information leakage accidents

년도	유출 사례
2001	연애인 A씨 지방 흡입 기록 공개
2006.10	채권추심원이 건보사이트 통해 14058여명 정보 불법조회
2007	건보 직원 대선주자 의료정보 무단 열람
2008.4	건보개인정보 75만건 유출 채권 추심에 사용
2011	청구 sw 업체 A사 EMR내 정보 9만건 무단 유출
2013.12	약학정보원 처방전 정보, 주민번호 7억원 판매목적 불법수집
2015	미국 의료보험업체 앤섬 고객정보 7천만건 해킹 사고 발생
2015	심사청구 sw업체 진료기록 5억건 의료정보 컨설팅업체 유출

또한 현재 건강보험 청구 SW를 개발 및 서비스하는 업체는 100여 곳 정도로 해당 업체들의 취약한 보안 관리에 따른 시스템 해킹에 의한 유출 사고나 내부 임직원에 의한 의도된 유출 사고는 언제든지 발생할 수 있다. 게다가 정부에서 추진하고 있는 원격 진료, 의료정보 빅데이터 활용, 사물인터넷 기반의 스마트 헬스등 다양한 의료서비스 또한 의료정보 유출 위험이 예상된다. 따라서 사전에 발생 가능한 위협 요인을 식별하여 대응 방안을 마련하고, 개인 정보 보호법 등 관련법에 따른 보안 요구 사항을 준수하여 유출 사고 예방 및 유출 시 피해를 최소화해야 할 것이다.

Ⅳ. 의료정보 보호 방안과 보호기술표준

4.1. 의료정보 침해위협과 보호방안

개인 의료정보는 병원 홈페이지, EMR(Electronic Medical Recording, 전자의무기록), OCS(Order Communication System, 처방전달시스템), PACS(Picture Archiving and Communication System, 의료영상저장정보시스템) 등의 의료정보 시스템을 통해 온/오프라인으로 수집 및 저장되고 병원 내 다수 부서에서 활용되다가 시간이 지나면 파기된다. 이 정보는 또한 보건복지부, 질병관리본부, 건강보험공단, 심사평가원, 검찰/경찰 등 다양한 유관 기관으로 전송된다. 개인 의료정보의 노출은 이러한 수집, 저장, 이용, 파기의 생명주기 동안 일어날 수 있다. 개인 의료 정보의 생명주기와 주기별 침해위험 요소와 보안관리 방법[5, 6]은 다음 표 3, 표 4와 같다.

Table. 3 Leakage risks according to life cycle of medical information

생명주기	침해 위험
수집	환자나 보호자의 동의가 누락 및 , 목적 외 이용, 홈페이지 통한 예약 접수 시 외부 오픈 시스템 해킹, 개인 PC와 수집 시스템 간 통신 시 암호화 부재로 해킹 또는 훔쳐보기 등으로 인한 개인 ID나 비밀번호 누출가능성
보관 및 관리	데이자 저장 시 암호화 누락, DB접근 로그 부재, 인터넷 메일, 웹하드, P2P, 메신저등을 통한 개인정보 유출 가능성
이용	외부에서 홈페이지 접근시 관리자 페이지 인터넷 노출, 이용자에게 과도한 권한부여, 개인정보 접근 모니터링 미흡, 유지보수 업체 불법 유출, DB서버에 대한 로그관리 미흡, 유출사고 발생시 책임 추적성 확보 어려움, 패스워드 유추하여 개인정보 해킹
제공	외부 전송시 암호화 누락, 법적 근거 없는 외부 제공, 정보주체의 동의 없이 제3자에게 제공
파기	완전 삭제나 폐기되지 않아 외부에서 데이터 복구 등을 통한 유출 가능성, 이용 목적된 정보 미파기, 사용 만료된 정보 미파기로 법적 분쟁 의 가능성

Table. 4 Security management according to life cycle of medical information

생명주기	의료정보보안관리
수집	최소정보수집, 수집동의, 처리방침게시, SSL, 동의기록 관리, 웹방화벽, DB보안, NAC, 바이러스, 백신, 스팸 및 스파이웨어 차단 솔루션, VPN
보관 및 관리	DB 암호화, 서버 DRM, PC DRM, 암호화 툴킷, 보안 USB, 문서고 출입통제, 웹 방화벽, UTM, PMS, 보안 OS, PMS
이용	내부관리계획, 서버보안, DB접근제어, 방화벽, 권한 최소화, SSO/IAM, 로그관리 시스템, IDS/IPS, DB보안, 사용자 인증솔루션, DRM, SBC, 사용자 인증 시스템, 바이러스 백신, 스팸 및 스파이웨어 차단 솔루션, VPN, NAC, PC보안 통합 솔루션,
제공	제3자 제공동의, SSL, DRM, 외부전송모니터링, 암호화 툴킷, 보안USB
파기	데이터 완전삭제, DRM, 문서파쇄기

4.2. 의료정보보호 기술 표준

한편으로 의료정보보호기술 또한 표준화 되어야 한다. 국제표준화기구인 ISO의 보건의료정보기술위원회인 TC215의 보안 분야 워킹 그룹인 WG4[7]의 내용과 ASTM E31.20[8] 헬스케어 정보 기술 위원회의 의료정보보안관련 표준기술 내용, SIG의 HL7[9]관련기술 표준내용[10]을 보면 다음 표 5, 표 6, 표 7과 같다.

Table. 5 ASTM E31.20

ASTM E31.20	설 명
E1714-00	환자에 대한 식별성 제공, 보안기술이 적용되는 의료정보속성
E1762-95	디지털 서명 과정의 특성, 속성, 최소 요구사항을 정의, 의료서비스에 활용 가능한 서명 기술
E1869-04	기밀성, 프라이버시, 접근 그리고 개인 식별을 위한 의료정보 보안 원칙
E1985-98	의료정보시스템 사용자 인증, 의료정보 문서의 접근이나 권한제어 내용
E1986-98	건강정보와 관련된 환자 및 제공자의 권리
E1987-98	의료정보와 관련된 모든 개인에 대한 권리와 권리운영절차
E2084-00	서명 및 해시 알고리즘, 공개키/비밀키의 관리, 암호키 및 인증서의 형식, 의료정보문서에 대한 서명방법
E2085-00a	의료정보의 상호 운용성 지원 프로토콜과 메시지 형식으로 기존 표준의 재사용 및 확장
E2086-00	네트워크에서의 의료정보 보호 방법

Table. 6 ISO/TC215 WG4

ISO/TC215 WG4	설 명
ISO/DIS 17090-1	헬스케어 환경의 PKI에 대한 기본 정의, 컴포넌트 정의, 상호 호환성보장을 위한 요구사항, 보안서비스 시나리오, PKI에서 사용하는 인증서 종류 및 공개키 암호기술
ISO/DIS 17090-2	의료정보시스템 환경의 특성을 반영한 PKI 인증서 프로파일 명세서
ISO/DIS 17090-3	헬스케어 PKI 구축 및 운영 가이드라인(인증서 정책의 구조 및 요구사항, 인증서 정책의 구조, 요구되는 보안 레벨, 보안정책 내에 포함되어야 할 요구사항)
ISO/DIS 27799	의료정보 시스템 환경에서 요구되는 보안기술에 대한 표준문서(보안의 목표, 보안대상 자원, 발생 가능한 공격 및 취약점, 요구되는 기술)
ISO/DIS 22600-1	다자간 의료정보의 전달 및 공유가 이루어지는 환경정보에 관한 권한 관리 및 접근제어 방법, 관리대상 데이터 분석, 권한 관리 시나리오 등
ISO/DIS 22600-1	의료정보 권한관리 모델(도메인 모델, 정책모델, 위임모델, 접근제어 모델) 제시

Table. 7 HL7 SIG

HL7 SIG	메시지가 라우터 중계로 통신시 발생 가능한 보안위협을 계층에 따른 위협으로 분류
	인증, 권한관리와 접근제어, 무결성 및 기밀성 보장, 부인 방지 등 보안서비스 요구사항

부인기술과 관련하여 현재 HL7의 ver 3.0내에서 주고받는 메시지 부인방지와 ISO 국제 표준화에 따라 자료 백업이나 저장, 아카이빙, 그리고 폐기 관련하여 해당 병원이나 업체에서는 빠른 시일 내에 개발이나 구현이 되어야 할 것이다.

위와 같이 기술적인 내용 외에 법제도와 관련하여 의료정보보호 활동이 활발히 진행되고 있다. 미국(HIPPA)은 건강보험이전 가능성 및 책임에 대한 법률이 제정, 의료정보 프라이버시와 보안에 대해서 언급하고 있다. 또한 미국의 3대 HIT 산업협회는 자발 민간조직으로 CCHIT를 설립하고 외래 환자용 진료정보처리제품에 대한 인증기준을 발표하는 등 의료정보를 취급하는 제품/시스템에 대한 보안성평가인증을 하고 있다. 국내에서도 개인의료정보보호, 원격의료시설, 전자의무기록과 관련하여 현행 의료법 조항을 규정하고 있으나 향후 의료보안 분야의 국내외 특히 국내에서 주요 이슈로 자리 잡기 위해서는 기술적인 문제는 물론 원격의료와 관련된 의료법 또한 개선이 선행되어야 할 것이다.

Ⅴ. 결 론

사물인터넷이 우리에게 주는 편리함, 즉 소비자 의료비 절감과 품질 향상, 한편으로 경제성장의 기회를 잡

기 위해서는 반드시 보안이 담보되어야 한다. 지금은 안심하고 사물인터넷 제품과 서비스를 이용할 수 있는 보안이 곧 경쟁력이 되는 시대이기 때문이다. 특히 가전·의료기기 및 자동차 등 사물인터넷의 활용 분야가 우리 실생활의 모든 사물에 접목될 수 있기 때문에 사물인터넷 보안위협은 사람의 생명도 위협할 만큼 큰 피해를 가져올 수 있다.

따라서 본 연구에서는 사물인터넷을 위한 보안 관련 국내외 동향과 기술, 개인의료정보 유출사례, 의료정보의 생명주기에 따른 침해위협요소들과 보호 방안 그리고 표준화기구들의 의료정보보호표준기술을 분석하였다.

REFERENCES

[1] David Niewolny, “How the Internet of Things Is Revolutionizing”, freescale.com/healthcare

[2] Information Security Grand Conference, 2015.

[3] Security Threats and Leakages field to be concerned of Private Information, Poll of Security News, 2015.

[4] Analysis of social costs in the value of personal information and privacy, Privacy Association, 2013.

[5] Security News, Oct. 15. 2014.

[6] LG CNS Security Consulting.

[7] ISO TC215, http://isotc.iso.org/livelink/livelink/open/tc215

[8] HIPAA, http://www.hhs.gov/ocr/privacy

[9] HL7, http://www.hl7.org

[10] S.H.Kim, J.E.Song, M.A.Chung, K.I.Chung, “Technical Standards Trend of Health Informatics and Its Security”, *ETRI, Electronics and Telecommunications Trends,* vol. 21, no 6, pp. 190-201, Dec. 2006.

우성희(Sung-Hee Woo)

1993: 충북대학교 전자계산학과 이학석사.
1999: 충북대학교 전자계산학과 이학박사
현 재: 한국교통대학교 의료IT공학과 교수
※관심분야: 침입차단 및 방지, 의료정보보호, 정보보안, 컴퓨터네트워크
Email : shwoo@ut.ac.kr