IoT 환경에서의 개인정보보호 프레임워크

A Framework for Personal Information Protection in Internet of Things Study on Contents Technology

이 야 리*, 김 정 숙**
한국보건사회연구원*, 삼육대학교**

Lee Yari*, Kim Jung-sook**
Korea Institute for Health and Social Affairs*, Sahmyook Univ.**

요약

사물인터넷(IoT)은 '개방형 환경에서 인터넷을 기반으로 사람, 사물, 데이터 및 프로세스를 서로 연결하여 정보를 교류하고 상호 소통하는 지능형 인프라'로서 홈·가전, 교통·물류, 건설, 에너지, 헬스케어, 사회안전 등 여러 분야에서 새로운 상품을 개발하고 공급해 창조경제의 핵심동력 가운데 하나가 될 것으로 기대된다. 그러나 네트워크, 서비스, 플랫폼/디바이스 등 기반 환경에서 다양한 개인정보 침해에 대한 위협이 존재하며 개인정보 보호와 기술 활용이라는 이슈에 관한 논의는 아직 초기 단계에 있다. 따라서 본 연구에서는 IoT 환경에서 정보주체의 민감한 개인정보에 대한 안전한 보호 정책 적용과 효율적 정보기술 활용 및 제공이 가능한 개인정보보호 프레임워크를 제안하고자 한다.

1. 서론

IoT(Internet of Things)를 국내에서는 사물인터넷이라고 부르며 그림 1과 같이 '인간, 사물, 서비스라는 3가지 분산된 환경요소에 대하여 인간의 명시적 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보처리 등 지능적 관계를 형성하는 사물 공간 연결망'이라고 정의하고 있다[1].

▶▶ 그림 1. IoT의 3대 주요 구성요소[2]

기존 네트워크, 서비스, 플랫폼/디바이스 등 IoT 기반 환경에서는 다양한 개인정보 침해에 대한 위협이 존재하고 개인정보 보호와 기술 활용이라는 이슈에 관한 논의는 아직 초기 단계[3]의 수준이다. 따라서 인터넷에 연결되는 사물이 많아질수록 해커가 공격할 수 있는 범위 또한 확대되므로 사물인터넷의 확산은 사이버 공격의 측면에서 본다면 개인 데이터 유출 가능성의 증대와 직결된다[4]. 이에 사물인터넷 활성화에 따른 개인정보보호 정책의 필요성이 크게 부각되고 있다.

본 연구에서는 IoT 환경에서 정보주체의 민감한 개인정보에 대한 안전한 보호 정책 적용과 효율적 정보기술 활용 및 제공이 가능한 개인정보보호 프레임워크를 제안하고자 한다.

2. 배경연구

IoT 관련 해외 주요 국가들의 정책 동향을 살펴보면, 미국은 국가정보위원회가 2025년까지 다양한 분야에서 국가경쟁력에 영향을 미칠 수 있는 6대 와해성 기술(disruptive civil technologies, 2008) 분야 중 '사물 인터넷(The Internet of Things)'을 선정하였다. EU에서는 '09년 7월 인터넷 진보를 활용 및 보안(개인정보)과 같은 문제가 발생될 우려가 있는 사항에 적절히 대응할 수 있도록, 14개의 사물인터넷에 관한 액션 플랜을 발표하였다. 중국에서는 IoT에 관한 연구 및 사업지원을 위한 제반환경을 주로 조성하고 있는 것으로 나타났으며, 정책방향에서는 중장기 과학기술 발전계획 수립('06 ~ '20년), M2M 연구센터 구축('10년), 사물네트워크 산업기금('10년)을 조성하였다. 일본에서는 안전한 디지털 안심·안전 사회의 실현을 위한 'i-Japan 전략 2015'를 중심으로, 이용자 관점에 입각한 인간중심(Human Centric)의 디지털사회 구현에 사물지능통신을 포함시키고, '11년 8월 경제산업성에서도 IoT를 중심으로 한 'IT융합에 의한 신산업 창출 전략'을 발표하였다[1].

국제 사물인터넷 표준화 단체인 'oneM2M'은 2013년 4월 분과를 구성하고 사물인터넷 보안 대책 마련에 착수하였다. 그러나, oneM2M의 가이드라인은 '장비 무결성 보장' 정도 수준의 원칙을 제시하였으므로 보다 적극적 사물인터넷 보안 및 정보보호 대책 수립이 요구된다.

사물인터넷 환경에서는 다양한 형태의 수많은 사물 데이터들을 통해 기존에는 알 수 없었던 개인정보의 확인이 가능하다. 이는 곧 개인의 생활패턴, 식습관 등 사물인터넷의 확산으로 인하여 원치 않는 개인정보의 노출을 발생시킬 우려로 귀결되는 상황이다. 이에 시장조사업체 '리사비 리서티(Rysavy Research)'는 사물인터넷이 발생시킨 정보에 대한 접근 권한 및 소유 주체와 보호 방안

에 대한 고민이 필요하다는 결론을 내렸다[4]. 또한 IEEE는 2013년 2월 1,200명 이상의 통신 분야 기술직 종사자들을 대상으로 사물인터넷 확산의 가장 큰 장애요인을 조사한 결과, 전체 46%가 개인정보보호를 지목하였음을 확인할 수 있었다[5].

3. 본론

개인 정보에 기반한 IoT 서비스가 활성화될 수 있는 방안은 개인정보보호 관리체계를 위한 인증 및 제약이 되는 관련 법/제도 사항을 연구 및 개선하는 것이다. 본 연구에서 제안하는 IoT 환경에서의 개인정보보호 프레임워크는 개인정보보호 관리체계 인증 수립 및 관련 법제도 사항 검토 및 개선을 위한 전문가 포럼 운영을 기반으로 구성된다. 그리고 이 전문가 포럼은 관련 부처, 유관기관 및 전문가 등이 참여 및 운영을 통해 IoT 서비스를 제공하는데 제약이 되거나 서비스 제공을 촉진 및 확산하는데 준수해야 할 법/제도를 통합·검토하고 이에 대한 위험 요소 및 보완 사항을 도출하여 개선 계획을 수립하게 된다. 국내 및 국제 인증제도의 인증은 우선 IoT 서비스(플랫폼 관련 및 실 서비스 관련)와 관련한 국내 및 국제 인증제도의 인증 요건을 검토해 볼 수 있다. 국내 인증 제도에는 한국인터넷진흥원(KISA)의 ISMS/PIMS가 있으며, 국제 인증 제도에는 국제 감사인증기준위원회(IAASB)의 SOC 2/3, ISO/IEC 20071 등이 있다. 이에 이러한 인증 요건을 검토하고 획득에 필요한 정보보호 정책, 조직, 교육, 보안/통제 체계, 운영관리 절차, 개인정보 생명주기 관리체계 등 후보 방안들을 수집하고, 국내/해외 사례 자료를 분석한다.

3.1 프레임워크 서비스 분석 및 관련 이슈 도출

IoT 환경에서의 개인정보보호 프레임워크는 IoT 환경 시스템의 서비스들을 분석하고, 개인정보보호 인증제도와 관련되는 이슈들을 도출한다. 서비스는 가변적이기 때문에 본 서비스 분석 및 관련이슈 도출은 상시적으로 수행하며, 개인정보 인증에 주요한 항목에 대한 모니터링 결과는 긴밀히 의사소통하여 단기간에 해결해야 한다.

3.2 시스템 분석 및 관련이슈 도출

시스템 분석을 통해 도출되는 이슈는 서비스 자체의 이슈보다 시스템에서 발생되는 개인정보보호 인증 이슈에 대한 사항을 분석하고 해결 방안을 제시할 것이다. 기본적으로 IoT 환경의 시스템을 바탕으로 사용자의 개인정보는 캡슐화시켜 시스템 관리에 개인정보보호로 수행하고, 시스템 개선을 위한 개인정보 및 활동정보 활용에 대해서는 서비스 사용자에게 사전 동의를 구하여 개인정보보호 인증에 대한 이슈 발생 가능성을 제거하도록 한다.

3.3 서비스 및 플랫폼/시스템 구축방향 분석 및 수정

서비스와 시스템의 이슈를 분석한 결과로 개인정보보호 인증에 중요한 이슈가 발생하였을 경우, 이를 해결하기 위해 서비스 또는 시스템 차원에서의 해결 방안을 제시할 것이다. 또한, 서비스 자체의 변경이 필요한 경우에는 전문가의 의견을 수렴하여 서비스 수정토록 할 것이다. 다음 단계에서는 인증진행 검토 및 확인서비스 및 시스템 변경으로 인한 결과를 확인하고, 초기에 검토한 인증제도에 대한 요건이 갖춰졌을 경우 인증을 진행한다. 인증 결과에 대한 내용을 공유하며 인증에 실패하거나 이슈가 발생했을 경우에는 관련 서비스 및 시스템에 해당하는 부분의 검토를 다시 진행하게 된다.

3.4 개인정보보호 인증이슈 모니터링

개인정보보호 인증에 성공한 경우, 해당 조건에 따라 이슈 발생이 예상되는 서비스 및 시스템 Point를 정리하고 이에 대한 수시 모니터링을 실시. 인증 이슈에 대한 변경은 중요한 사항으로 분류하여 운영진의 의사결정을 신속히 처리하도록 제도를 수립한다.

4. 결론

본 연구에서는 IoT 환경에서 정보주체의 민감한 개인정보에 대한 안전한 보호 정책 적용과 효율적 정보기술 활용 및 제공이 가능한 개인정보보호 프레임워크를 제안하였다. 그러나 개인정보보호 프레임워크 적용 시, 이슈사항이 주로 개인의 일상 데이터를 획득 및 사용하는 과정에서 발생할 것으로 예상되며 다음의 표1과 같은 내용이 될 것이다.

표 1. 제안시스템의 적용 이슈

구분	상세 이슈
1	센서장비를 통한 개인의 생체/심리/행동 정보의 직접 취득
2	SNS/블로그/포털 정보의 Big Data 분석
3	개인 의료기록 및 건강정보 라이프사이클(수집, 이용 및 제공, 저장, 파기)에 따른 개인정보보호 관리체계
4	공공기관(통계청, 건강보험공단 등) 또는 영리기업(금융/통신 /유통 등)이 축적하고 있는 개인의 일상 데이터
5	기업 마케팅 또는 Operation 업무처리 자료 및 프로세스 정보

따라서, 향후 연구에서는 앞에서 살펴본 이슈항목들과 개인의 일상 정보 DB를 구축하는 데 필요한 타 원천 데이터의 정보보호에 관한 법/제도를 분석하여 예상치 못한 기타 이슈사항이 발생하였을 경우를 대비한, 적시의 해당 전문가 의견을 구하는 등 해결 방안을 검토할 수 있도록 최적의 발전 방안을 수립해야할 것이다.

■ 참 고 문 헌 ■

[1] 민경식, “사물 인터넷(Internet of Things)”, 한국인터넷진흥원 인터넷 & 시큐리티 이슈, pp.31-35, 2013.
[2] 김호원, 김동규, “사물인터넷 기술과 보안”, 정보보호 학회지, 제 22권, 1호, 2012.
[3] 김동희, 윤석웅, 이용필, “IoT 서비스를 위한 보안”, 정보와 통신 : 한국통신학회지 = Information & communications magazine, v.30, no.8, pp.53-59, 2013.
[4] 사물인터넷(Internet of Things) 산업의 주요 동향, 해외 ICT R&D 정책동향 06호, 정보통신산업진흥원, 2013.
[5] IEEE, “IEEE Survey Connected Devices and the Internet of Things”, 2013.