홍 승 필 교수지도

석사학위 청구논문

# 스마트 기기 환경 내
# 개인정보 프로파일 설계 및 적용 방안

*2013*

성신여자대학교 대학원

컴퓨터학과

이 연 우

# 스마트 기기 환경 내
# 개인정보 프로파일 설계 및 적용 방안

홍 승 필 교수지도

이 논문을 석사학위논문으로 제출함

*2013*년 *5*월

성신여자대학교 대학원

컴퓨터학과

이 연 우

# 인 준 서

이연우의 석사학위 논문으로 인준함.

심사위원 변 혜 원 인

심사위원 김 태 훈 인

심사위원 홍 승 필 인

성신여자대학교 대학원

# 논문개요

다양한 스마트 기기의 등장과 인터넷의 보편화로 언제 어디서나 인터넷에 접속할 수 있는 유비쿼터스 환경이 도래하고 있다. 이러한 환경 속에서 최근 기기 간의 통신을 가능하게 하는 기술이 연구되고 있으며 사용자 개인 맞춤형 서비스에 활용되고 있다. 스마트 기기 환경에서는 다양한 경로를 통해 개인의 정보가 수집될 수 있으며 서비스 제공자는 수집된 정보를 기반으로 사용자 개인정보 프로파일을 생성, 개인 맞춤형 서비스에 활용하고 있다. 그러나 이러한 정보에는 개인의 행동패턴이나 성향을 파악할 수 있는 위치정보, 습관정보, 신체정보 등 민감한 정보가 포함되어 있으며 사용자의 프라이버시(Privacy)를 침해할 수 있는 위협으로 작용할 수 있다. 특히, 사용자가 항시 소지하고 다니는 스마트 기기를 통해 사용자의 정보를 수집/이용하여 서비스를 제공하는 경우 사용자의 다양한 개인정보가 활용될 수 있어 개인정보 보호방안이 반드시 고려되어야 한다.

본 연구에서는 스마트 기기 환경 내 사용자의 개인정보를 수집, 활용하는 경우 사용자의 프라이버시를 보호할 수 있는 개인정보 프로파일 관리방안을 제시한다. 서론에서는 연구의 개략적인 설명 으로 연구 배경과 범위, 목적에 대해 소개한다. 관련연구에서는 스마트 기기 환경과 개인정보 보호에 대한 소개 및 선행연구를 검토하며 스마트 기기 환경 내 발생 가능한 개인정보 침해위협을 도출하여 본 연구의 방향성에 대해 제시한다. 이를 기반으로 스마트 기기 환경 내 안전한 개인 정보 활용방안으로 프라이버시 보호 개인정보 프로파일 관리 시스템을 제안 하고 제안한 시스템의 실 환경에의 적용 가능성을 검증하기 위해 프로토 타이핑을 보여준다. 후반부에서는 제시한 시스템의 분석 및 성능평가를 진행하며 향후 연구방향에 대해 제시한다.

# 목 차

# 그림 목차

# 표 목차

# Ⅰ. 서 론

다양한 스마트 기기의 등장과 인터넷의 보편화, 네트워크 기술의 진화로 언제 어디서나 인터넷에 접속할 수 있는 유비쿼터스 환경이 도래하고 있다. 이러한 환경 속에서 최근 사람과 사람 사이의 통신 뿐 아니라 사람과 기기, 기기와 기기 간의 통신을 가능하게 하는 기술이 활발하게 연구되고 있다. 이러한 기술은 언제 어디서나 어떠한 기기를 통해서도 실생활의 다양한 요구를 만족시키는 미래인터넷 기술[13]로써 개인 스마트 기기의 확대 및 지능형 전자기기의 등장에 힘입어 사용자 개인 맞춤형 서비스로 영역이 확대되고 있다. 스마트 기기간 통신 환경에서는 RFID, 센서, 스마트 기기 등 다양한 경로를 통해 개인의 정보가 수집될 수 있으며, 서비스 제공자는 수집된 정보를 기반으로 사용자 개인정보 프로파일을 생성, 개인 맞춤형 서비스에 활용하고 있다. 그러나 이러한 정보에는 단순히 사용자의 신상정보를 넘어 신체정보, 위치정보 등의 새로운 정보가 포함되어 있으며, 개인의 성향, 행동패턴에 대해 지속적으로 수집, 분석될 가능성이 있는 민감한 정보[7]이므로 사용자의 프라이버시를 침해할 수 있는 위협으로 작용할 수 있다. 특히, 사용자가 항시 소지하고 다니는 스마트 기기를 통해 사용자의 정보를 수집하고 사용자 맞춤형 서비스를 제공하는 스마트홈, u-City, u-헬스케어, 스마트카 등과 같은 서비스에서는 사용자의 다양한 개인정보가 활용될 수 있어 개인정보 보호를 위한 방안이 반드시 고려되어야 한다.

그러나, 스마트 기기간 통신 환경에서는 다양한 경로를 통해 사용자의 개인정보가 수집되어 서비스에 활용될 수 있는데 반해, 사용자는 자신의 개인정보가 언제 어떻게 수집, 사용되었는지 확인하거나 정보 제공을

제어할 수 있는 방안은 미흡하다. 또한 국내의 경우 지난 2011년 개인정보보호법의 시행으로 개인정보보호를 위한 의무사항이 강화되었으며 이에 개인정보를 활용하는 공공, 민간사업자는 목적에 필요한 최소한의 정보만을 수집, 활용해야 하며 민감한 정보를 사용할 경우에는 사용자 알림 및 동의 등의 절차를 거치는 등 필요한 조치를 이행해야 한다[3,4]. 그러나, 스마트 기기를 통해 개인정보를 수집, 활용하는 것과 관련된 연구는 주로 효율적인 사용자 분석방안이나 통신상의 암호화, 보안 프로토콜 등에 초점이 맞추어져 진행되고 있는 반면 관련 법·제도에서 규제하는 사항을 고려하여 개인정보를 보호하기 위한 연구는 상대적으로 미흡한 상황이다.

본 연구에서는 스마트 기기간 통신 시 개인화 서비스를 위해 다양한 기기를 통해 사용자의 개인정보를 수집, 활용하는 경우 관련 법·제도에서 규제하는 사항을 고려하며 사용자의 프라이버시를 보호할 수 있는 개인정보 프로파일 생성, 관리 방안을 제시한다. 1장 서론에서는 연구의 개략적인 설명으로, 연구의 배경과 범위, 목적에대해 간략하게 소개하였다. 2장은 관련연구로써 스마트 기기 환경과 개인정보보호에 대한 소개 및 선행연구를 검토하며, 3장에서는 스마트 기기 환경 내 개인정보를 활용하는 경우 발생 가능한 침해위협을 도출하며 본 연구의 방향에 대해 제시한다. 4장에서는 스마트 기기 환경 내 안전한 개인정보 활용방안으로 프라이버시 보호 개인정보 프로파일 관리 시스템(PPMS)을 소개하고 세부기능에 대해 설명하며, 5장에서는 제시한 시스템의 실 환경에의 적용 가능성을 검증하기 위해 데이터베이스 설계 및 간략한 알고리즘, 프로토타이핑을 보여준다. 6장에서는 제시한 시스템의 분석 및 성능평가를 진행하며 마지막 7장에서는 연구의 내용 및 결과를 요약하고 향후 연구방향에 대해 제시한다.

# Ⅱ. 관련연구

## 1. 스마트 기기 환경

### 1) 사물지능통신(M2M)

스마트 기기는 일상생활과 밀접하게 연결되어 있는 전자 기기들에 이동성, 연결성 및 경량화를 부각시킨 기기로 탑재된 OS를 통해 PC를 이용하는 것과 동일하게 다양한 작업을 수행할 수 있는 지능화된 모바일 기기를 의미한다. 최근 스마트폰으로 대표되는 스마트 기기 사용자의 급증과 지능형 기기의 등장 그리고 이를 통한 다양한 융합서비스의 증가로 컴퓨팅 환경의 패러다임이 변화하고 있다. 이러한 환경 속에서 최근 사람과 사람 사이의 통신 뿐 아니라 사람과 기기, 기기와 기기 간의 통신을 가능하게 하는 기술이 활발하게 연구되고 있다. 이처럼 사물간의 통신 네트워크를 구성하여 정보를 공유하는 개념 및 기술을 지칭하는 용어로 M2M, IoT, 사물지능통신 등이 있다[11]. 이러한 기술은 언제 어디서나 어떠한 기기를 통해서도 실생활의 다양한 요구를 만족시키는 미래인터넷 기술로써 최근 여러 분야에서 활발하게 응용되고 있다[13]. M2M이란 Machine to Machine의 약어로 기기간의 통신을 의미하며, 같은 맥락에서 IoT는 Internet of Things의 약어로 언제 어디서든 누구에게나 연결되던 정보통신기술이 모든 사물과의 연결로 확장되는 기술을 말한다. 미국의 전기전자학회(IEEE) 및 유럽의 통신표준협회(ETSI)에서는 M2M (Machine-to-Machine)을 사람이 개입하지 않는(혹은 최소 개입) 상태에서 기기 및 사물간에 일어나는 통신이라고 정의하고 있다. 국내의 사물지능통신포럼

에서는 사물통신을 사람이나 지능화된 기기가 방송 통신망을 이용하여 사물 정보를 제공하거나, 사물을 제어하기 위한 통신으로 규정하고 있다. 그리고 방송통신위원회에서는 사물통신을 통신, IT 기술이 결합하여 원격지의 기기, 사람, 환경 등의 상태 정보를 확인할 수 있도록 연결하는 제반 솔루션이라고 정의하고 있다[11,12].

[표 1] 기기간 통신에 대한 정의

| 용어 | 기관 | 정의 |
|---|---|---|
| M2M | ETSI | - 인간의 직접적인 개입이 꼭 필요하지 않은 둘 혹은 그 이상의 객체간에 일어나는 통신 |
| | IEEE | - 가입자 장치(subscriber station)와 기지국(base station)을 거쳐 코어-네트워크에 위치하는 서버간의 정보 교환 혹은 가입자 장치간 인간의 개입 없이 발생하는 정보 교환 |
| MTC | 3GPP | - 인간의 개입이 꼭 필요하지 않은 하나 혹은 그 이상의 객체가 관여하는 데이터 통신의 형태 |
| IoT | ITU-T | - 모든 사물에까지 네트워크 연결을 제공하는 네트워크의 네트워크 |
| | CASAGRAS | - 데이터 수집과 통신기능을 통하여 물리적 객체와 가상의 객체를 연결해주는 글로벌 네트워크 기반구조 |
| MOC | ITU-T | - 인간의 직접적인 개입이 최소한으로 요구되거나, 혹은 요구되지 않는 둘 혹은 그 이상의 객체간의 통신 |
| 사물지능통신 | 사물지능통신포럼 | - 사람이나 지능화된 기기가 방송통신망을 이용하여 사물 정보를 제공하거나, 사물을 제어하기 위한 통신 |
| | 방송통신위원회 | - 통신, IT 기술이 결합하여 원격지의 기기, 사람, 환경 등의 상태 정보를 확인할 수 있도록 연결하는 제반 솔루션 |

초기 M2M 시장은 텔레매틱스, 원격검침, POS(Point of Sales) 시스템 등 기업이 주류를 이루어 왔으나, 최근에는 개인 스마트 기기의 확대로 eBook,

스마트 홈 등으로 영역이 확장[12]되고 있다. 가장 보편적으로 제공되는 M2M 서비스는 텔레매틱스, 보안관제, 의료, 물류, 유통 등이 있다.

[표 2] M2M 서비스 분류

| 서비스영역 | 응용서비스 | |
|---|---|---|
| Utilities/Energy /Metering | - Smart Meters<br>- Windmills, Solar Fields<br>- Home Area Network<br>- Power<br>- Gas | - Water<br>- Heating<br>- Grid Control<br>- Industrial Metering |
| Remote Maintenance /Buildings | - Escalators<br>- HVAC<br>- Lighting<br>- Elevators<br>- Safety | - Fire Systems<br>- Conveyor Systems<br>- Access Systems<br>- Smart Home |
| Consumer Electonics | - Home Automation<br>- Stereo/Hi Fi Audio<br>- Kitchen belnder<br>- Home Theater<br>- Digital camera | - DVD<br>- Home appliances : dishwasher, refrigerator<br>- Digital photo frame<br>- eBook |
| Tracking/Tracing /Telematics /Transportation | - Fleet management<br>- Order management<br>- Pay as you drive<br>- Asset tracking<br>- Navigation, GPS | - Traffic management<br>- Road tolling<br>- Emergency Call<br>- Parking Meters<br>- Supply Chain |
| Security/Payment | - Surveillance systems<br>- Backup for landline<br>- Control of physical access<br>- Car/driver security | - Point of sales<br>- Vending machines<br>- Gaming machines |
| U-Healthcare | - Monitoring vital signs<br>- Supporting the aged<br>- Web access telemedicine points<br>- Remote diagnostics<br>- BAN/PAN | - MRI<br>- Implants<br>- Fitness equipment<br>- Clinic<br>- Diagnostics |

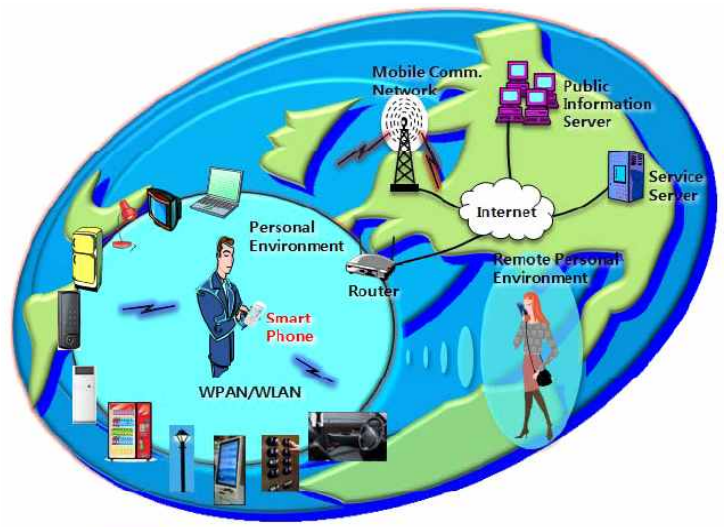
※ 출처 : M2M 기술 및 보안동향, 인터넷정보학회지, 2012

### 2) 개인화 서비스

개인화 서비스는 사용자의 개인 데이터를 수집, 분석하여 사용자에 맞는 서비스를 제공하는 것으로 타켓 마케팅, 추천 서비스에서 사용자 선호도를 기반으로 가전기기들을 제어하는 스마트홈 서비스까지 다양한 분야에서 활용되고 있다. 지금까지의 개인화 서비스는 사용자의 데이터를 서비스 제공자의 서버에 수집하고 분석하는 서버 중심의 개인화 서비스가 주를 이루었던 반면, 최근에는 개인 스마트 기기의 확산으로 인해 개인 스마트 기기를 이용하여 직접 데이터를 수집, 관리하고 개인화 서비스에 필요한 사용자 개인정보 프로파일을 생성해 필요 서비스에 직접 제공하는 사용자 중심의 개인화 서비스[32]로 변모하고 있다. 사용자 중심의 개인화 서비스는 사용자의 스마트 기기에 저장된 사용자 개인정보 프로파일을 기반으로 지능형 기기들이 직접 통신을 하고 정보를 제공하는 개인환경 서비스(PES, Personal Environment Service)라는 개념으로 확대되었다[17,18].

개인환경서비스는 사용자가 스마트 기기를 가지고 가정과 사무실, 차량, 공공장소를 이동하면, 스마트 기기가 주변의 각종 생활 기기들을 자동으로 인식하고 제어하여 사용자 개인에게 최적화된 생활환경을 제공하는 서비스를 의미한다[18]. 개인환경서비스는 사물지능통신가 유사한 개념이나 보다 사용자의 스마트 기기를 활용하여 보다 개인화에 초점이 맞추어진 서비스는 점에서 차이가 있다. 개인환경서비스에서는 사용자의 신상정보 및 선호도 정보를 포함한 사용자 개인정보 프로파일이 미리 사용자가 항시 소지하는 스마트폰과 같은 스마트 기기에 저장된다. 스마트 기기에는 무선랜이나 블루투스와 같은 근거리 무선통신 모듈이 내장되어 있으며, 사용자 주변의 각종 전기, 전자, 기계 장치에도 동일한 방식의 근거리 무선통신 모듈이 내장되어 있어야 한다. 그러면 사용자가 휴대폰을 가지고

움직일 때마다 생활공간에 설치된 각종 생활기기의 서비스 프로파일을 인식해, 휴대폰에 저장된 사용자 개인정보 프로파일에 따라 생활기기들을 최적으로 제어하고 사용자의 생활환경을 개인에게 최적화시키는 것이다[17,18].




(그림 1) 개인환경서비스(PES) 구성도

※ 출처 : 휴대폰과 사용자 개인정보 프로파일 기반의 개인환경서비스(PES), TTA Journal, 2010.07

이러한 개인환경서비스는 최근 스마트폰 등과 같은 개인 스마트 기기의 보편화와 M2M과 같은 기기간 통신 기술의 발전으로 인해 등장하게 된 개념으로 사용자의 개인정보를 활용하여 다양한 서비스 모델로의 발전이 가능하다. 이는 사용자에게 최적화된 다양한 서비스를 제공함으로써 만족도와 편의성을 향상시킬 것으로 기대되고 있으나 표준화 업무를 수행하는 표준화기구가 부재한 상태이며 세부기술별 표준안 마련이 시급한 상황이다. 아울러 사용자의 개인정보가 활용될 수 있다는 점에서 각종 법, 규제를 고려하며 동시에 사용자 프라이버시를 침해하지 않는 방안이 고려되어야 할 것이다.

## 2. 개인정보보호

### 1) 개인정보와 프라이버시의 정의

국내 개인정보보호법에서는 개인정보를 “살아 있는 개인에 관한 정보로서 성명, 주민등록번호, 영상 등을 통하여 개인을 알아볼 수 있는 정보와 그 자체로는 직접 알아보기 힘들더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보”로 규정하고 있으며, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)에서도 개인정보 보호법과 마찬가지로 유사하게 정의하고 있다[2,3].

[표 3] 법률상 개인정보의 정의

| 구 분 | 내 용 |
|---|---|
| 개인정보보호법 | - ‘개인정보’란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함 한다.) |
| 정보통신망 이용촉진 및 정보보호 등에 관한 법률 | - ‘개인정보’란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함 한다.) |

※ 출처 : 개인정보보호 연차보고서, 2012

개인정보에 대한 정의는 국가별, 관련법률에 따라 조금씩 차이가 있으나 독일, 영국, 일본 등 여러 나라에서 개인정보를 공통적으로 “생존하는 개인에 관한 정보”, “식별 가능한 개인에 관한 정보”라고 정의한다는 점에서 그 의미는 거의 유사하다고 할 수 있다[14,15,16]. 이렇듯 개인정보는 개인의 신체, 재산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가 등을

나타내는 일체의 모든 정보를 포함한다. 정보사회를 맞이 하여 사회 각 분야에서는 인터넷과 정보통신기술의 사용이 일상화되면서 개인정보는 과거 단순한 신분정보에서 오늘날에는 전자 상거래, 고객관리, 금융거래 등 사회 구성, 유지, 발전을 위해 필수적인 요소로 기능하고 있다.

[표 4] 해외 입법례에서 개인정보의 정의

| 구 분 | | 내 용 |
|---|---|---|
| OECD가이드라인(제1조) | | - 식별되거나 식별 가능한 개인에 관한 모든 정보 |
| EU 지침(제2조) | | - 정보주체의 신원이 확인되었거나 확인 가능한 정보 |
| 캐나다 | 프라이버시법 (제3조) | - 신원을 확인할 수 있는 개인에 대한 정보 |
| 일본 | 개인정보보호에 관한 법률(제2조) | - 생존하는 개인에 대한 정보로서 특정한 개인을 식별할 수 있는 정보 |
| 호주 | 프라이버시법 (제6조) | - 당해 정보 또는 의견(opinion)으로부터 신원이 명백하거나 확실시 될 수 있는 개인에 관한 정보 또는 의견 |
| 영국 | 개인정보보호법 (제1조) | - 신원확인이 가능한 생존하고 있는 개인과 관련된 데이터 또는 정보관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 데이터나 정보로부터 신원확인이 가능한 생존 개인과 관련된 데이터 |
| 프랑스 | 정보처리 축적 및 자유에 관한 법률(제4조) | - 형식에 관계없이 직접 또는 간접으로 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보 |
| 독일 | 연방개인정보 보호법(제3조) | - 신원이 확실하거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보 |

※ 출처 :미국의 개인정보보호 법·제도 동향, 정보보호학회지, 2012

아울러 최근 개인정보의 개념 및 범위는 사회환경의 변화와 기술 발전에 따라 지속적으로 확대되고 있고, 정보통신기술 발달로 보호되어야 할 개인정보 유형도 다양화되는 추세이다. 구체적인 개인정보 항목은 다음과 같다.

[표 5] 개인정보 유형별 종류(예)

| 유형구분 | 개인정보 항목 |
|---|---|
| 일반정보 | 이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적 |
| 가족정보 | 가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호 |
| 교육 및 훈련정보 | 학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항 |
| 병역정보 | 군번 및 계급, 제대유형, 주특기, 근무부대 |
| 부동산정보 | 소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등 |
| 소득정보 | 현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득 |
| 기타 수익정보 | 보험 (건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가 |
| 신용정보 | 대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록 |
| 고용정보 | 현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과 직무태도 |
| 법적정보 | 전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록 |
| 의료정보 | 가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보 |
| 조직정보 | 노조가입, 종교단체가입, 정당가입, 클럽회원 |
| 통신정보 | 전자우편(E-mail), 전화통화내용, 로그파일(Log file), 쿠키(Cookies) |
| 위치정보 | GPS나 휴대폰에 의한 개인의 위치정보 |
| 신체정보 | 지문, 홍채, DNA, 신장, 가슴둘레 등 |
| 습관 및 취미정보 | 흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향 |

※출처 : 한국인터넷진흥원, 2013

개인정보의 개념이 확대됨에 따라 프라이버시(Privacy)에 대한 개념 또한 변화하고 있다. 최초 프라이버시는 1880년 미국 Thomas Cooley의 저서에서 “홀로 있을 권리(the right to be let alone)” 라는 의미로 제시되었고 1890년도에 Warren과 Brandeis가 “프라이버시는 진보된 문명세계에서 살고있는 개인에게 필수적인 것” 이라 주장한 것에서 유래한다. 전통적 프라이버시 개념은 정보사회에 도래로 새롭게 해석되고 있다. 특히 개인정보가 타인에 의해 전자적 형태로 무한히 수집·처리되기 시작함에 따라 개인정보에 대한 정보주체의 자기결정권을 나타내기 위한 “정보 프라이버시(information privacy)” 라는 개념이 등장 하였으며 이는 국가 차원에서 보호해야 할 중요한 권리로 인정되고 있다. 개인정보는 프라이버시 영역에 속하는 정보 프라이버시의 보호대상이다. 프라이버시가 사생활에 관한 이익을 총칭하는 가장 넓은 개념이라면 개인정보보호는 프라이버시의 한 내용으로 타인에 의한 개인정보의 수집·처리와 관련해서 해당 개인정보의 주체가 가지는 이익, 즉 “개인정보자기결정권” 을 의미한다[38]. 프라이버시와 관련해 개인정보는 크게 두가지로 구분된다. 하나는 프라이버시와 관계된 정보를 포함하고 있는 경우로 본인의 동의없이 공개, 이용 등의 처리를 할 때 프라이버시 침해가 성립된다. 예로 의료정보, 신용정보, 사상, 유전정보 등 유출 시 개인에게 사회적 차별의 우려가 있는 사항들이다. 다른 하나는 자체만으로는 프라이버시와 무관한 개인 정보로 이미 공개되어 있는 이름, 주소, 전화번호 등이다. 그러나 이들 정보가 “불가침 사적영역” 에 속하는 정보와 연결된다면 전체정보가 프라이버시 영역이 된다. 예를들어 주소 정보는 프라이버시는 아니나 의료 정보가 연결되어 공개될 시 프라이버시 침해가 될 수 있다[37]. 따라서 개인정보보호는 개인의 정보 프라이버시를 보호하기 위해 반드시 고려되어야 하는 사항이라 할 수 있다.

## 2) 개인정보 침해동향

정보통신 기술의 발전과 IT분야의 유관 산업과의 접목으로 다양한 융합 서비스 제공 및 이용의 기회로의 무한한 발전 가능성을 보이고 있다. 특히 언제 어디서나 다양한 서비스를 가능케 하는 매체와 통신 기술의 사용이 일상화되면서 개인정보는 과거 단순한 신분정도에서 오늘날에는 기업 및 민간 사업자 측면에서 전자상거래, 고객관리, 금융거래 등 사회의 구성, 유지, 발전을 위한 필수적인 요소로서 가능하고 있다. 그러나 주제자의 어떠한 사전 동의 없는 개인정보의 무단 수집·이용·유통의 보편화는 물론 관리의 부재로 인한 개인정보 내돌리기, 불법거래, 유출 등으로 개인정보 침해문제가 심각해지고 있다.


(그림 2) 국내 개인정보 침해동향

※ 출처 : 한국인터넷진흥원, 2013

위 그림은 '08~' 11년 사이 발생한 개인정보 침해 동향으로, 개인정보 침해 건수는 2010년 5만4천여 건에서 2011년 12만여 건으로 전년대비 2배

이상 증가한 수치를 보이면서 사회적으로 개인정보 처리 및 관리에 대한 심각성이 고조되어 있다. 2012년 개인정보 침해건수는 16만여 건으로 전년대비 약 36.5%의 증가한 수치를 보이고 있으며 주민번호등 타인정보의 도용 위협이 가장 많은 비중을 차지하고 있다[5,6].

[표 6] 개인정보 침해신고 상담 건수 (단위 : 건)

| 침해유형 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|---|
| 개인정보 무단수집 | 1,129 | 1,075 | 1,267 | 1,623 | 3,507 |
| 개인정보 무단이용제공 | 1,037 | 1,171 | 1,202 | 1,499 | 2,196 |
| 주민번호등 타인정보도용 | 10,148 | 6,303 | 10,137 | 67,094 | 139,724 |
| 회원탈퇴 또는 정정 요구 불응 | 949 | 680 | 826 | 662 | 717 |
| 법적용 불가 침해사례 | 24,144 | 23,893 | 38,414 | 38,172 | 12,915 |
| 기타 | 2,404 | 2,045 | 2,986 | 13,165 | 7,742 |
| **합계** | 39,811 | 35,167 | 54,832 | 122,215 | 166,801 |

※ 출처 : 한국인터넷진흥원, 2013

한편, 국내·외 기업 및 국가기관이 관리 및 보유하고 있는 개인(민감)정보 노출사고 발생에 따른 피해규모가 확대되면서, 기업 및 기관의 이미지 실추 및 사회적, 경제적 막대한 손실을 발생시키고 있다. 특히, 2011년 7월 SK컴즈 회사의 경우에는 개인정보 유출사고 사상 역대 최고 규모의 인터넷 개인정보 유출 사건이 발생하면서 개인정보보호법을 기반으로 기술적, 관리적, 서비스 측면의 적용 가능성에 대한 관심이 증폭되어 있는 실정이다.

## 3) 개인정보보호 법·제도

### (1) 국외 개인정보보호 법·제도 및 가이드라인

개인정보보호와 관련하여 세계 각국에서는 다양한 법·제도·정책을 제정,

시행하고 있으며 특히 정보통신기술의 발달로 인한 전자적 형태의 개인정보보호와 관련한 법률이 다수 존재하고 있다[1,14].

[표 7] 국외 개인 및 정보보호 법·제도

| 국가 | 법.제도 | 주요 내역 |
|---|---|---|
| 미국 | 전기통신 프라이버시법 (ECPA) | - 「전기통신 프라이버시법(ECPA : Electronic Communications Privacy Act of 1986)」은 전자통신기록에 불법적으로 접근하거나 보유정보를 허가 없이 공개하는 것을 예방하고자 제정 |
| | 의료보험의 책임에관한법 (HIPPA) | - HIPPA는 전자적 형태의 개인 의료정보보호를 의무화하고 의료기관에 개인 의료정보보호 정책을 작성·시행할 것을 요구 |
| 영국 | 데이터보호법 | - 「1984년 데이터보호법(Data Protection Law)」에서는 데이터 보호 등록소 (Data Protection Register)와 등록관(Registrar)을 두고 등록제 운영<br>- 데이터이용자와 컴퓨터 정보회사에 의한 등록에 관한 규정을 두어 데이터보호 등록부에 등록할 의무 규정 |
| | 프라이버시 및 전자통신규칙 2003 | - 「프라이버시 및 전자통신규칙(Privacy and Electronic Communications (EC Directive) Regulations 2003」은 EU의 전자통신부문프라이버시 지침(2002/58/EC) 을 반영하여 제정 |
| 독일 | 정보통신법 | - 「정보통신법(Telecommunications Act/TeleKommunikationsgesetz-TKG), 2004년 제정, 2005년 3월 14일 개정」은 정보통신 서비스를 제공하는 모든 책임자는 고객정보를 정부에서 접근 가능한 상태로 할 의무가 있으며, 그러한 데이터는 정부의 감시기관이 직접 접근할 수 있도록 해야 한다고 규정 |
| | 연방 데이터보호법 (BDSG) | - 독일의 개인정보를 보호하기 위한 기본법인 「연방데이터 보호법(Federal Data Protection Act(BDSG), 1990년 제정, 2003년 1월 14일 개정)」은 개인정보 정의, 정보주체의 권리와 정보처리자의 각종 의무 등에 대한 내용 포함<br>- 2003년 EU의 개인정보보호지침 반영을 위해 개정 |

| | | |
|---|---|---|
| 일본 | 정보통신 네트워크 사회 형성 기본법 | - 일본의 대표적인 IT법률은「고도 정보통신 네트워크 사회 형성 기본법(IT기본법)(2000년 법률 제 144호)」<br>- 네트워크의 안전성 및 신뢰성, 개인정보보호의 확보를 기본방침 중 하나로 정한 정보보호 법제도의 기본 방침 |
| | 개인정보보호 관련 법률 | - 개인정보의 적정한 관리를 목적으로 하는 일본의「개인정보보호법」은 2005년 4월부터 시행<br>- 정보의 부정취득과 누출을 막기 위한 여러 의무를 기업과 단체에 부과 |

한편, OECD (Organization for Economic Co-operation and Development)를 포함한 여러 국제기구들은 이용자가 쉽게 이해할 수 있는 명확하고 간결한 개인정보보호 정책을 내세우기 위해 개인정보보호 가이드라인을 제시하고 있다.

### o OECD Privacy Protection

개인정보의 국제법적·제도적 측면에서 중요한 연구 방향 중 한 가지는 OECD에서 제시하는 “프라이버시 보호 및 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)”이다. OECD 기준은 주로 정보주체의 동의 절차에 대한 명시가 중요한 내용으로 포함되어 있다. 즉 개인정보에 대한 관리가 정보주체의 동의절차와 수집경로 그리고 이용목적에 대한 고지가 어떻게 이루어지고 있는가 하는 점이 중요한 문제이다. 이에 대한 기준으로는 아래와 같은 8가지(수집 제한, 정확성 확보, 목적명시, 이용제한, 안전성, 공개, 개인 참여, 책임) 원칙이 중요시 되어 지고 있다[8].

[표 8] OECD의 개인정보 보호 8원칙

| 원칙 | 내용 |
|---|---|
| 수집제한 | - 개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 정보도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다. |
| 정확성확보 | - 개인데이터는 그 이용목적에 부합되며, 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다. |
| 목적명시 | - 개인정보는 수집 시 그 수집목적이 명확히 제시하고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다. |
| 이용제한 | - 개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다. |
| 안전성확보 | - 개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다. |
| 공개 | - 개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다. |
| 개인참여 | - 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다. |
| 책임 | - 데이터관리자는 원칙 실시를 위한 조치에 따를 책임이 있다. |

### o APF(APEC Privacy Framework Privacy/Data Protection) 9가지 원칙

아시아태평양경제협력체(APEC, Asia-Pacific Economic Cooperation)은 회원국 간의 전자상거래 촉진을 위해 제반 활동을 하는 고위관료회의 산하 특별그룹인 ECSG(Electronic Commerce Steering Group)에서 APF(APEC

Privacy Framework: Privacy/Data Protection) 개인정보보호 9원칙을 개발하였다. APF 개인정보보호 9원칙은, 피해예방, 사용자 고지, 수집제한, 개인접오 활용, 선택, 무결성, 보안조치, 열람 및 수정, 책임이다. APF 원칙들은 개인정보의 원활한 국제적 이전을 촉구하여 전자상거래를 활성화하는 동시에 개인정보 및 개인정보보호를 도모한다[10].

o ISTPA(International Security, Trust and Privacy Alliance)

보안 및 프라이버시 관련 문제 해결을 위한 구성된 단체로 ISTPA에서 개발한 프라이버시 프레임워크는 개인정보보호를 위한 요구사항으로 8가지 프라이버시 원칙을 정의하였다. ISTPA의 8가지 프라이버시 원칙은 책임, 수집제한, 접근, 개인참여, 적절성, 보안, 사용제한 검증이 있다[1].

o IPC(Information and Privacy Commissioner)

캐나다 Ontario의 IPC는 1998년 1월부터 개인정보보호와 접근 이슈들에 대한 연구를 지휘하고 개인정보보호와 접근 이슈에 대하여 공공 교육을 지원해왔다. IPC는 개인정보보호에 대한 10가지 원칙으로 책임, 목적확인, 동의, 수집제한, 제한된 사용/공개/유지기간, 정확성, 보호책, 개방성, 개인접근, 도전적인 참여의식을 제시하고 있다[1].

### (2) 국내 개인정보보호법

국내 개인정보보호 관련한 법제도는 크게 공공부문과 민간부문으로 구분하였으며, 공공부문은 「공공기관의 개인정보보호에 관한 법률」, 민간부문은 정보통신서비스제공자 등 일부 사업자에 대해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 각 분야별로 개별법이 적용되었으나, 2011년 9월 30일을 기준으로 「개인정보보호법」이 시행되면서 국내 개인정보 보호체계가 변경되었다.

[표 9] 국내 개인정보보호법

| 개인정보보호법 | | |
|---|---|---|
| 개요 | - 정보통신서비스를 이용하는 자의 개인정보를 보호하고, 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활을 향상시키고 공공복리를 증진할 목적으로 제정된 법률 | |
| 주요 사항 | 규율대상 | - 공공민간의 모든 개인정보 처리자(9만개 공공기관, 350만개 사업자) |
| | 보호범위 | - 보호범위 확대 : 컴퓨터 등에 의해 처리되는 개인정보파일 뿐만 아니라 종이문서에 기록된 개인정보도 포함 |
| | 고유식별번호 처리제한 | - 주민등록번호 등 고유식별번호 처리 제한 : 원칙적으로 처리 금지하며 정보주체의 별도 동의, 법령의 근거가 있는 경우 등은 예외 허용 |
| | 유출통지 | - 개인정보 유출통지 의무화 |
| | 개인정보 영향평가 | - 공공기관 개인정보 영향평가 의무화<br>- 민간분야의 개인정보 영향평가 제도 확대 |
| | 집단분쟁조정 | - 집단분쟁제도 도입(재판상 화해 효력 부여) |
| | 단체소송 | - 단체소송(권리침해 중지) 도입 |
| | 위원회 | - 대통령 소속 개인정보보호위원회 |


(그림 3) 개인정보보호법 구성 체계

※ 출처 : 국가정보보호백서, 2013

이는 대규모 개인정보 유출사건이 빈번히 발생하면서 심각한 사회문제로 대두되었으나 기존의 법들이 각 분야별로 분산되어 산재하면서 비영리 기관, 오프라인 사업자 등이 법적용 대상에서 배제되어 발생하는 개인정보보호 사각지대 발생 문제를 해소하고 개인정보 침해사고의 사전 예방과 사후 구제를 위해 공공과 민간에 모두 적용되는 법이다. 새로이 제정된 개인정보보호법은 기존 법체계에서 분절적으로 규정하고 있는 개인정보 처리기준을 표준화하여 개인정보의 단계적 보호조치를 정립하였다[4,5]. 개인정보 생명주기는 수집, 저장, 이용 및 제공, 파기의 단계로 분류된다. 수집은 서비스를 이용하고자 하는 개인정보 소유자의 개인정보를 수집하는 단계로 서비스 이용자의 이용신청과 동시에 자신의 개인정보를 서비스 제공자에게 제공함으로써 이루어진다. 수집한 개인정보는 서비스 제공자의 데이터베이스에 저장되어 적절한 보호조치 아래 추가, 수정, 파기 등이 관리가 이루어지며, 저장된 개인정보는 여러가지 필요에 의해 이용하거나 제3자에 제공할 수 있다. 파기는 개인정보 소유자에 의한 서비스 이용중단(탈퇴), 요청 서비스 종료 등 개인정보의 보유기간이 종료되었을 경우 보유하고 있는 개인정보를 지체없이 파기하는 단계이다. 개인정보보호법의 관련조항을 개인정보 생명주기(수집, 저장, 이용 및 제공, 파기)에 따라 분류해보면 다음과 같다[3].

[표 10] 개인정보 생명주기별 개인정보보호법 관련조항 분류

| 단계 | 개인정보보호법 관련조항 |
|---|---|
| 수집 | • **제15조(개인정보의 수집 · 이용)**<br>- 개인정보를 수집기준 및 수집 목적의 범위 확인<br>- 정보주체의 동의 필요<br>• **제16조(개인정보의 수집 제한)**<br>- 목적에 필요한 최소한의 개인정보를 수집<br>• **제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)**<br>- 정보주체에게 알려야 함 |

| | |
|---|---|
| | • **제22조(동의를 받는 방법)**<br>- 개인정보의 처리에 대하여 정보주체의 동의를 받는 방법 명시 |
| 저장 | • **제4조(정보주체의 권리)**<br>- 정보주체는 자신의 개인정보 처리와 관련 권리<br>• **제29조(안전조치의무)**<br>- 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 요구<br>• **제31조(개인정보 보호책임자의 지정)**<br>- 개인정보의 처리에 관한 업무를 총괄할 개인정보 보호책임자 지정<br>• **제35조(개인정보의 열람)**<br>- 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람 요구<br>• **제36조(개인정보의 정정·삭제)**<br>- 제35조에 따라 정보주체는 개인정보의 정정 또는 삭제 요구<br>• **제37조(개인정보의 처리정지 등)**<br>- 정보주체는 자신의 개인정보 처리의 정지를 요구 |
| 이용 및 제공 | • **제15조(개인정보의 수집·이용)**<br>- 개인정보를 수집 목적의 범위 내에서 이용<br>• **제17조(개인정보의 제공)**<br>- 정보주체의 개인정보를 제3자에게 제공(공유를 포함)<br>- 제공사항을 정보주체에게 알리고 동의를 받아야 함<br>• **제18조(개인정보의 이용·제공 제한)**<br>- 개인정보를 목적 외의 용도로 이용하거나, 이를 제3자에게 제공 방안 명시<br>- 변경의 경우, 이를 알리고 동의를 받아야 함<br>• **제19조(개인정보를 제공받은 자의 이용·제공 제한)**<br>- 개인정보를 목적 범위 내에서 이용 및 제공<br>• **제22조(동의를 받는 방법)**<br>- 개인정보의 처리에 대하여 정보주체의 동의를 받는 방법 명시<br>• **제26조(업무위탁에 따른 개인정보의 처리 제한)**<br>- 제3자에게 개인정보의 처리 업무를 위탁<br>- 위탁하는 업무의 내용과 수탁자 정보를 정보주체에게 알려야 함<br>• **제27조(영업양도 등에 따른 개인정보의 이전 제한)**<br>- 영업의 전부 또는 일부의 양도·합병 등<br>- 이전에 대한 사항을 해당 정보주체에게 알려야 함(통지) |
| 파기 | • **제21조(개인정보의 파기)**<br>- 보유기간의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 파기 |

### 4) 개인정보보호 기술

인터넷의 발전에 따라 개인정보의 활용도가 높아지면서 개인정보보호 법제도적인 측면에서는 개인의 권리를 존중하며 꼭 필요한 최소 정보만을 제공해야한다고 요구하지만, 정보통신기술의 발달로 사이버 범죄 역시 급증하여 보다 정확한 기술적인 보호 방안이 필요해졌다. 이에 꼭 필요한 개인정보보호 기반기술과 개인정보보호 강화기술, 개인정보 정책개발 기술로 구분하여 설명한다. 개인정보보호 기반기술은 정보기술시스템을 형성하기 위해 기반이 되는 기술로써 기술의 적용범위와 적용대상에 따라 영역별로 상세분류를 하고, 개인정보보호 강화기술은 정보 인프라를 바탕으로 개인정보의 안전성을 향상시키기 위해 개인정보 진단, 보호 및 기술로써 개인정보보호 방안을 강화한다[19,20]. 개인정보 정책개발 기술은 개인정보를 처리하는 방식에 관한 정책과 사용자가 미리 설정해 놓은 프라이버시 정책을 비교하여 결과를 처리하는 정책 처리기술, 정책에 의해 접근을 제어하는 기술, 프라이버시 정책을 인지하는 기술로 분류할 수 있다.

[표 11] 개인정보보호 기술

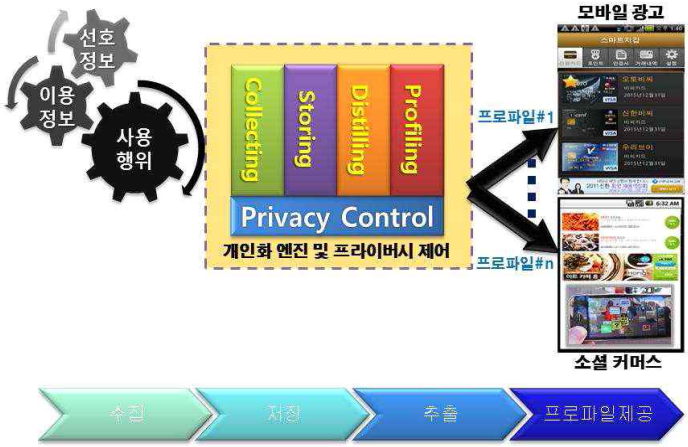
| 분 류 | 소분류 | 개 념 | 개인정보보호 대표기술 |
|---|---|---|---|
| 개인정보 보호기반 기술 | 암호화 | - 암호란 평문을 해독 불가능한 형태로 변형하거나 또는 암호화된 암호문을 해독 가능한 형태로 변형하기 위한 원리, 수단, 방법 등을 취급하는 기술 | - 대칭키 암호시스템<br>- 공개키 기반구조 (PKI) |
| | 네트워크· 인터넷 보안 | - 네트워크는 분산되어 있는 시스템 노드들 사이의 데이터를 전송하기 위한 통신 기반 구조 | - 방화벽<br>- IDS/IPS<br>- VPN |

| | | | |
|---|---|---|---|
| | 접근통제 기술 | - 소유주의 자원(컴퓨팅 자원, 통신 자원 및 정보 자원 등)에 대하여 허가되지 않은 접근을 방어 | - 임의적 접근통제<br>- 강제적 접근통제<br>- 역할기반 접근통제 |
| | 사용자 신분확인 기술 | - 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법 | - ID/패스워드 방식<br>- 인증서 방식<br>- 스마트카드 방식<br>- 생체인식 |
| | 시스템 보안 | - 사용 허가권이 없는 사용자가 파일, 라이브러리 폴더 및 장치 등을 사용하지 못하도록 제한 하여 보호하는 시스템 기능 | - 웹서버 보안<br>- Kerberos<br>- 감사추적/로깅/ 백업 |
| 개인정보 보호강화 기술 | 웹 기반 기술 | - 클라이언트의 익명성 제공 기술<br>- 서버의 익명성 제공 기술 | - Anonymizer<br>- Onion Routing<br>- Janus |
| | 네트워크 기반기술 | - 네트워크에서 정보의 안전성과 신뢰성을 제공 | - 프록시 기술<br>- 방화벽<br>- IDS/IPS |
| | 에이전트 기반기술 | - 인터넷의 정보 유출에 대해 사용자를 대신하여 통제 | - 쿠키매니저<br>- 에드브로커<br>- 스파이웨어 필터 |
| 개인정보 정책개발 기술 | 정책 처리기술 | - 사용자 개인정보 처리 방식에 관한 정책과 사용자가 미리 설정해 놓은 프라이버시 정책에 따라 수준 비교 후 결과 처리 | - P3P |
| | 정책 접근제어 기술 | - 시스템을 사용할 수 있는 자격을 가지고 있는 사용자만 시스템이나 자원에 접근 할 수 있도록 제어 | - RBAC |
| | 법·제도 인지기술 | - 데이터 접근 및 사용자 정보 보호를 위해 프라이버시 정책 인지 및 생성 | - APPEL<br>- XACML |

## 3. 선행연구 동향

본 논문에서는 스마트 기기를 통해 개인화된 서비스를 제공하고자 할 시, 사용자의 프라이버시를 보호할 수 있는 개인정보 프로파일 관리 방안에 대해 제시한다. 따라서 선행연구로는 모바일 환경 내 개인정보보호를 위한 관련 표준과 개인화 서비스 제공을 위한 사용자 개인정보 프로파일링 및 스마트 기기 환경 내 개인정보 보호방안에 대한 연구를 검토하였다.

개인환경서비스처럼 사용자에게 최적화된 서비스를 제공하기 위해서는 필연적으로 사용자의 스마트 기기에 저장된 사용자 정보를 활용해야 한다. 이와 관련하여 한국기술통신진흥협회에서는 모바일 기기에서 사용자 데이터를 수집하고 저장, 관리하여 사용자 개인정보 프로파일을 추출하는 개인화 서비스 프레임워크에 대해 정의하고 있다[32].




(그림 4) 모바일 환경의 개인화 서비스 개념도

※ 출처 : 한국정보통신기술협회, 2012

해당 표준에서는 사용자 개인정보 프로파일을 서비스에 제공할 시 발생할 수 있는 프라이버시 침해 및 개인정보 노출에 대비하기 위한 기능을 포함하고 있다. 표준에서 정의하는 프라이버시 제어는 사용자의 선택과

결정에 따라 설정되는데 수집은 수집에서 제외되는 항목을 설정하고 추출은 프로파일의 범위를 제어하며 제공에서는 제공 여부와 제공 범위를 설정할 수 있다. 또한 서비스에 제공되는 프로파일에는 사용자의 식별정보를 포함하지 않아 사용자가 해당 서비스에 인증하지 않고는 서비스는 각각의 사용자를 식별할 수 없어 기본적인 프라이버시 보호 기능을 제공한다[32].

사용자 개인정보를 기반으로 사용자 맞춤 서비스를 제공하기 위한 연구는 기존 PC환경에서, TV, 스마트 기기 등 다양한 분야에서 진행되고 있다. 이와 관련된 연구는 주로 효율적인 개인 맞춤형 서비스 제공 방안에 초점이 맞춰져 있으나 개인 프라이버시와 관련해서 침해위협과 이에 대한 대응 방안이 필요함을 언급하고 있다. 송창우[22]는 시맨틱 웹 환경에서 개인화 프로파일을 동적으로 갱신하여 반영할 수 있는 콘텐츠 추천 검색 시스템을 제안하였다. 해당연구는 기존 추천 시스템의 제한된 추천기능을 보완하기 위한 것으로 본 논문의 연구 방향과는 거리가 있다. 그러나, 저자는 사용자 개인정보 프로파일을 수집하는 단계에서 프라이버시 문제가 발생할 수 있음을 밝히고, 프로파일 정보의 사용은 반드시 콘텐츠 추천 서비스를 이용하기 위한 서비스 제공자와 함께 교환이 이루어져야 하며, 표준안의 마련 필요성이 있음을 언급하며 프로파일 생성 시 프라이버시를 고려해야 한다는 의견을 제시하였다. 양방향 맞춤형 방송 서비스를 위한 사용자 개인정보 프로파일 시스템에 대한 연구[23]에서는 사용자의 선호도를 기반으로 사용자 개인정보 프로파일을 생성하고 이를 기반으로 사용자 맞춤형 방송 콘텐츠 추천 시스템을 제안하였다. 제시한 시스템 가운데 개인화 엔진은 사용자의 행동기록을 토대로 선호정보를 추출해 사용자 개인정보 프로파일을 만들고 사용자별 선호정보를 기반으로 콘텐츠를 추천한다. 해당연구 역시 사용자 맞춤형 콘텐츠 제공을 위해 사용자의

행동패턴을 수집하고 선호도를 분석하는 과정을 수행하므로 사용자의 프라이버시 보호를 위한 방안이 필요한 것으로 사료된다. 스마트폰 사용자의 프로파일에 기반을 둔 맞춤형 광고 서비스 모델에 대한 연구[24]에서는 스마트폰 내에 저장된 정보를 추출 및 추론하여 사용자 개인정보 프로파일을 구성하며, 광고주가 광고를 등록할 시 사용자 개인정보 프로파일과 비교할 수 있는 광고의 타겟팅 전략을 함께 등록해야 한다. 이후 생성된 사용자 개인정보 프로파일과 광고주가 등록한 광고의 유사도를 계산하여 광고를 추천하도록 한다. 해당 연구는 사용자 개인 기기로부터 개인정보를 추출, 추론할 시 개인 프라이버시를 침해할 수 있는 위협이 존재하므로 이에 대한 대응방안이 필요한 것으로 보인다. N. J. King[27]은 모바일 환경 내 사용자 행위에 기반을 둔 사용자 개인정보 프로파일링 기술에서 발생할 수 있는 사생활 침해와 개인정보보호 문제를 유럽연합과 미국의 관련 법에 근거하여 분석하고 연계 연구에서 기업의 자기규제와 프로파일링 및 개인정보보호 기술의 방향에 대해 제안하였다.

한편, 스마트 기기의 보급과 각종 지능형 기기의 등장으로 기기간 통신 시의 보안위협에 대응하기 위한 연구도 진행되고 있다. 은선기[25]는 안전한 M2M 통신 환경을 구축하기 위해 고려해야 하는 보안 요구사항을 도출하고 이를 구현하기 위해 필요한 보안 기능을 갖는 M2M통신 아키텍처를 제안하였다. 해당 연구는 M2M 통신 환경에서 디바이스간 신뢰성 제공을 위한 상호인증 및 키 교환을 제공하는 프로토콜을 제안하며, 프라이버시 보호를 위해 디바이스 식별자 암호화로 디바이스의 익명성을 보장한다. 스마트 기기간 환경 내 프라이버시 관련 연구로 Gudymenko[28]는 RFID 기술에 초점을 맞추어 M2M환경 내 프라이버시 침해위협을 도출하고 적용 가능한 보안기술 및 대책을 제시하였다. 또한 개인정보보호와 관련하여 법· 제도

준수의 중요성을 언급하며 RFID 기술에서 고려 해야 할 규제사항을 제안하였다. 해당 연구에서 제시한 RFID 기술의 개인정보보호를 위한 법·제도·정책을 고려사항은 서비스의 개인정보 컴플라이언스 측정, RFID 태그의 영구사용 중지, RFID 사용제한 등이 있다. 해당 연구는 개인정보 보호를 위해 관련 법·제도 준수의 중요성을 언급하고 있다는 점에서 본 연구와 유사한 목적을 지닌다. Biswas[29]는 사용자의 프로파일을 공유·제공할 시 프라이버시 보호할 수 있는 암호화 방법에 대해 연구하였다. 해당 연구는 효율적인 암호화 기법을 통해 개인정보를 보호한다는 점에서 본 논문과 차이를 보이나, 서비스 제공자에 의한 사용자의 프로파일 오·남용 및 침해를 방지하고, 안전한 개인화 서비스 제공을 목표로 한다는 점에서 유사하다. 모바일 환경 내 개인환경서비스에 대한 연구[17]에서는 사용자가 항시 소지하고 다니는 기기에 사용자의 위치정보, 선호도 정보 등에 따라 주변 기기들을 제어하여 사용자에게 최적의 서비스를 제공하는 시스템을 제시하였다. 그러나 해당 연구에서는 서비스 제공자가 사용자 동의 등 프라이버시를 고려하여 사용자의 프로파일을 수집, 활용한다고 하였으나 구체적인 방안에 대해서는 논의하지 않고 있다.

본 논문과 유사한 방향성을 지닌 선행연구로 사용자 프라이버시를 보장하는 모바일 RFID 개인정보보호 서비스 시스템[26]은 사용자와 서비스 제공자가 프로파일을 생성, 변경, 삭제 등을 할 수 있으며, 사용자는 자신의 프라이버시 보호등급을 직접 제어할 수 있고, 사업자는 자신이 제공하는 서비스에 필요한 필요 정보를 관리할 수 있다. 이준규[30]는 u-City 환경 내 개인정보보호를 위해 서비스 제공에 활용되는 개인정보를 분류, 등급화하고 사용자 정보와 u-City 서비스간의 연관성을 기반으로 사용자/서비스 프로파일을 정의, 프로파일 매칭을 통해 서비스 제공여부를 결정하는

방안에 대해 제시하였다. 또한, 전달되는 정보간의 안전성 확보를 위해 암호화 및 키 분배 관리방안을 제시함으로써 u-City 환경에서 발생 가능한 프라이버시 위협에 대응하고자 하였다.

대부분의 선행 연구는 개인화 서비스 제공을 위해 사용자의 프로파일을 수집하고 이를 분석하는 방안을 중심으로 이루어지고 있으며, 프라이버시에 대한 문제점을 지적하고 있으나 이에 대해 구체적으로 논의된 연구는 상대적으로 미흡한 것으로 보인다. 개인정보보호를 위한 연구 중 프로파일 매칭기법을 활용한 연구[30]는 본 논문에서 제안하고자 하는 방향성과 가장 유사한 연구이나, 민감정보 이용 시 사용자 동의 등 관련 법·제도·정책에서 규제하는 사항은 다루지 않고 있다. 모바일 RFID 개인정보 보호에 대한 연구[26]의 경우에는 모바일 RFID에 초점을 맞추어 연구를 진행하였고, 활용되는 개인정보의 민감도 분류 및 관련 법·제도·정책에서 규제하는 사항은 다루지 않고 있다.

개인정보보호법의 시행 등으로 개인정보를 다루는 서비스 제공자는 반드시 법·제도·정책에서 요구하는 사항을 준수해야 하며 이는 개인정보 보호가 선택이 아닌 의무임을 의미한다. 따라서 다양한 유형의 개인정보가 여러가지 형태로 수집, 활용될 수 있는 스마트 기기 환경 내 여러 개인화 서비스는 관련 법·제도·정책에서 요구하는 사항을 고려하여 개인정보를 보호하며 안전하게 활용할 수 있어야 한다. 본 연구에서는 선행연구에서 다루지 않은 개인 정보 관련 법·제도·정책을 고려하여 스마트 기기 환경 내 안전하게 개인정보를 활용할 수 있는 프로파일 생성, 관리 시스템을 제안한다.

# Ⅲ. 문제점 분석 및 연구방향

## 1. 문제점 분석

개인 스마트 기기의 보편화와 지능형 기기의 확산으로 인해 기기간 정보를 제공, 공유할 수 있는 사물지능통신 환경이 도래하고 있다. 이러한 환경에서 사용자가 항시 소지하고 다니는 스마트 기기를 통해 다른 지능형 기기 및 센서들이 스마트 기기에 저장된 사용자의 개인정보를 수집, 활용하여 맞춤형 서비스를 제공하는 개인화 서비스가 주목받고 있다.

그러나, 기기간 통신을 통해 개인화 서비스를 제공하는 환경에서는 다양한 경로를 통해 사용자의 개인정보가 수집되어 서비스 제공에 활용될 수 있는데 반해, 사용자는 자신의 개인정보가 언제 어떻게 수집, 사용되었는지 확인하거나 정보 제공을 제어할 수 있는 방안은 미흡[9,31]하다. 또한 국내의 경우 지난 2011년 개인정보보호법의 시행으로 개인정보보호를 위한 의무사항이 강화되었으며, 이에 개인정보를 활용하는 모든 공공 및 민간 사업자는 법에서 명시하는 사항을 준수해야 할 의무[4]가 있다. 따라서 서비스 제공자는 개인 맞춤형 서비스 제공을 위해 다양한 개인정보를 수집할 시 관련 법에 따라 목적에 필요한 최소한의 정보만을 수집, 활용해야 하며 민감한 정보를 사용할 경우에는 사용자 알림 및 등의 절차를 거치는 등 필요한 조치를 이행해야 한다. 그러나 현재 스마트 기기 환경 내 개인정보보호를 위한 연구는 초기단계이며, 주로 통신의 효율성, 암호화, 보안 프로토콜 등에 초점이 맞추어져 진행되고 있어 관련 법·제도·정책을 고려하여 개인정보를 보호하기 위한 연구는 상대적으로 미흡한 상황이다. 따라서 관련 법·제도·정책을 고려한 스마트 기기 환경 내 개인 정보

보호방안에 대한 연구는 필요하다고 사료된다. 스마트 기기 환경 내 개인화 서비스와 관련된 문제점은 다음과 같이 정리할 수 있다.

O 개인정보 수집경로의 다양화로 프라이버시 침해위협 증대

- RFID, 센서 등 다양한 경로를 통해 사용자의 개인정보가 수집, 활용될 수 있으며 수집되는 개인정보의 범위 확대
- 위치정보, 신체정보 등 민감한 정보 수집 시 사용자 동의 및 고지할 수 있는 방안이 미흡하여 정보주체의 프라이버시 침해위협 증대

O 정보주체의 주요 개인정보 제어기술 부재

- 스마트 기기 환경 내에서는 정보주체가 자신의 개인정보 항목 중 어떤 정보가 수집, 이용, 파기 되는지에 대해 알기 어려우며 인지하지 못한 상태에서 개인정보의 수집, 활용이 가능
- 정보주체가 자신의 개인정보 항목에 대한 제공여부를 결정하고 필요 시 알림 등을 받을 수 있는 개인정보 제어기술 부재

O 개인정보 관련 법·제도·정책 고려한 연구 미흡

- 서비스 제공자가 개인정보를 활용할 경우 관련 법·제도·정책을 고려하여 무분별한 수집을 제한하고 민감정보 이용 시 사용자 동의, 고지 등의 절차를 거쳐야 함
- 기존 연구는 개인 맞춤형 서비스 제공을 위한 사용자 개인정보 프로파일 분석 방안에 초점이 맞추어져 있으며 관련 법·제도·정책을 고려하여 개인정보를 보호하기 위한 연구는 미흡함

## 2. 연구방향

앞서 제시한 스마트 기기 환경 내 개인정보 문제점을 해결하기 위해 본 연구에서는 사용자의 스마트 기기를 통해 다른 기기들과 사용자 개인정보를 공유할 시, 사용자가 자신의 개인정보를 제어할 수 있는 방안을 제시하고, 개인정보 관련 법·제도에 기반하여 민감정보 수집, 활용 시 사용자에게 동의, 고지할 수 있도록 하여 무분별한 개인정보의 수집을 방지할 수 있도록 한다. 아울러, 서비스 제공자의 프라이버시 관련 인증 여부 및 보호정책 유무 등을 기반으로 서비스 신뢰성을 검증함으로써 사용자의 개인정보가 안전하게 활용될 수 있도록 한다. 관련 법·제도·정책을 고려한 개인정보보호를 위해 본 연구에서는 관련 연구에서 제시했던 국제기구별 개인정보보호 가이드라인과 국내 개인정보보호법을 비교하여 개인정보 생명주기에 따라 최소한으로 준수해야 할 항목을 도출하였다. 분석결과에서 보듯이 국제기구별 개인정보 가이드라인과 국내 개인정보보호법은 유사한 기준을 보이고 있다. 개인정보를 수집할 시에는 수집목적을 밝혀야 하고 사용자의 동의를 요구하고 있으며, 국내 개인정보보호법에서는 고유식별정보의 처리를 제한하고 있다. 또한 개인정보를 저장할 시에는 정보의 정확성과 무결성, 최신성을 유지해야 하며 적절한 보호대책을 마련해야 함을 알 수 있다. 수집한 정보를 활용할 시에는 이용에 제한을 두어야 하며, 목적 외 활용 시에는 정보주체의 동의가 반드시 필요하다. 아울러 보유기간의 경과, 목적을 달성한 정보는 지체없이 파기해야 함을 명시하고 있다. 이는 본 연구에서 개인정보보호를 위한 근거로 활용된다. 수집과 관련하여 서비스별 기준 프로파일을 정의함으로써 수집목적에 필요한 최소한의 항목만을 수집하도록 하며, 민감정보 활용 시 사용자 동의를 거칠 수 있도록 한다. 이와 동일하게 이용 시에도 경우에 따라 사용자 동의를 거칠

수 있도록 함으로써 무분별한 개인정보의 이용을 방지한다. 저장 및 파기와 관련하여서는 서비스 제공자가 별도로 자신의 개인정보보호 정책을 제시하도록 함으로써 서비스 이용자가 이를 확인할 수 있는 방안을 마련한다.

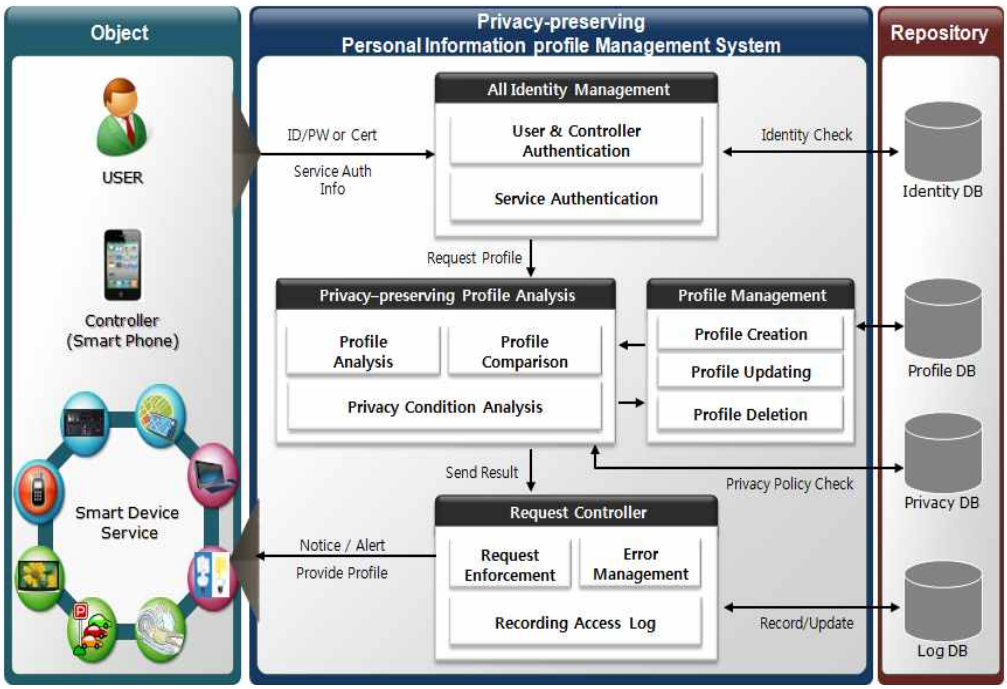
[표 12] 국제기구별 가이드라인 및 개인정보보호법 비교

| 단계 | 항목 | 관련근거 | | | | |
|---|---|---|---|---|---|---|
| | | OECD | APF | ISTPA | IPC | 개인정보보호법 |
| 수집 | 수집목적 | 목적명시 | 고지 | 적절성 | 목적확인 | 목적명확/고지 |
| | 수집항목 | 수집제한 | 수집제한 | 수집제한 | 수집제한 | 수집제한 (고유식별정보 처리제한) |
| | 민감정보 | | | | | |
| | 동의 | 동의 | 동의 | 동의 | 동의 | 동의 |
| 저장 | 보유기간 | - | - | - | 유지기간 | 보유기간 명시 |
| | 정보관리 | 정확성 확보 | 무결성 | 유효성 | 정확성 | 정확성/완전성/ 최신성 |
| | 안전조치 | 안전성 확보 | 피해예방/ 보안조치 | 보안 | 보호책 | 안전조치 |
| | 책임 | 책임 | 책임 | 책임 | 책임 | 보호책임자 지정 |
| 이용 및 제공 | 이용목적 | 이용제한 | 개인정보 활용 | 사용제한 | 제한된 사용 | 이용제한 |
| | 이용항목 | | | | | |
| | 위탁제공 | | | | | |
| 파기 | 파기방법 | - | - | - | - | 보유기간경과/ 목적달성 시 정보파기 |

# Ⅳ. 프라이버시 보호 개인정보 프로파일 관리 시스템

## 1. 전체구성

본 논문은 사용자의 개인정보를 기반으로 프로파일을 생성하여 개인화 서비스에 활용하는 경우, 사용자의 개인정보를 보호할 수 있는 프라이버시 보호 개인정보 프로파일 관리 방안을 제안한다. 제안하는 시스템의 전체 구성은 아래 그림과 같이 나타낼 수 있다.




(그림 5) 프라이버시 보호 개인정보 프로파일 관리 시스템 아키텍처

본 연구에서는 사용자가 항상 소지하고 다니는 스마트폰 혹은 태블릿 PC와 같은 개인 스마트 기기를 컨트롤러라고 정의하며, 컨트롤러는 실제

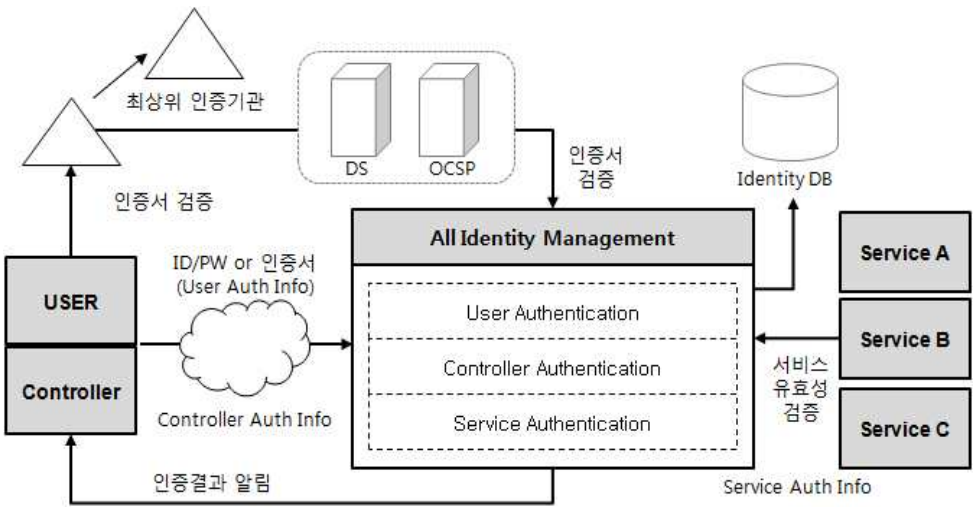
사용자의 개인정보를 저장하고 다른 기기와 통신을 통해 개인정보 프로파일을 제공, 공유하는 역할을 한다. 본 연구에서 제안하는 프라이버시 보호 개인정보 프로파일 관리 시스템은 크게 1) 통합 아이디 관리(All Identity Management)기능, 2) 프로파일 관리(Profile Management)기능, 3) 프라이버시 보호 프로파일 분석(Privacy-preserving Profile Analysis)기능, 4) 요청 제어(Request Controller) 기능으로 구성된다.

통합 아이디 관리 기능은 사용자와 컨트롤러, 그리고 서비스의 인증을 통합적으로 하여 인증된 사용자만이 검증된 서비스를 사용할 수 있도록 접근을 제어함으로써 효율성과 보안성을 강화할 수 있다. 프로파일 관리 기능은 사용자와, 서비스의 정보를 수집하여 이를 기반으로 프로파일을 생성하고, 정보의 최신성 유지를 위한 주기적인 업데이트, 사용자 요청에 의한 편집, 삭제 기능 제공 등 전반적으로 프로파일을 관리하는 기능을 한다. 프라이버시 보호 프로파일 분석 기능은 서비스 요청 시 사용자 개인정보 프로파일과 서비스 프로파일의 분석과 사용자 동의 절차를 통해 정보의 제공 여부를 결정하고 관련 법·제도·정책에서 규정하는 항목을 준수하여 개인정보를 적절하게 수집, 활용하는지를 검증하는 기능이다. 본 기능을 통해 요청을 분석한 후에는 분석 결과를 요청 제어 기능에 전달한다. 요청 제어 기능은 분석 결과를 통해 사용자 개인정보 프로파일을 서비스 제공자에게 제공하거나, 문제가 발생한 경우 사용자에게 알림 메시지를 전달하는 기능이다. 또한 요청 결과를 로그기록으로 남김으로써 추후 문제 발생 시 근거자료로 활용할 수 있도록 한다.

## 2. 세부기능

### 1) 통합 아이디 관리 기능

통합 아이디 관리 기능은 사용자의 신분과 사용자의 컨트롤러, 그리고 서비스를 통합적으로 인증하는 기능이다. 해당 기능은 인증된 사용자가 유효성한 서비스를 이용할 수 있도록 1차적인 보안을 제공하며, 사용자, 컨트롤러, 서비스의 인증을 통합적으로 함으로써 효율성을 강화한다.




(그림 6) 통합 아이디 관리 기능

사용자의 신분확인은 아이디/패스워드 인증방식 혹은 공인인증서를 통해 가능하다. 서비스를 이용하고자 하는 사용자는 사전에 시스템에 저장된 자신의 인증정보를 컨트롤러에 입력하며, 인증서 기반의 인증일 경우에는 인증기관으로부터 인증서 검증을 받아야 한다. 사용자 신분확인과 동시에 사용자가 접속을 시도한 컨트롤러의 인증절차를 거친다. 컨트롤러 인증정보로 활용할 수 있는 정보는 스마트 기기를 식별할 수 있는 고유 정보로써 IMEI번호나, IMSI/USIM번호, MAC 주소가 있다. 최초 사용자가

시스템에 가입할 시, 사용할 컨트롤러의 인증정보 또한 함께 등록해야 한다.

[표 13] 컨트롤러 인증 활용 정보

| 정보유형 | 내 용 |
|---|---|
| IMEI번호 | - 전 지구적 이동통신시스템(GSM) 이동단말기가 서로를 고유하게 식별할 수 있도록 이동단말기에 할당된 식별번호로 형식 승인 코드, 최종 조합 코드 및 일련 번호를 포함하여 15자리로 구성되는 기기고유번호 |
| IMSI/USIM 번호 | - IMSI는 국제 모바일 가입자 식별번호로, 이동통신서비스 가입시 구매하게 되는 USIM(universal subscriber identity module, 범용가입자식별모듈) 카드에 저장되는 정보 |
| MAC주소 | - 구내 정보 통신망(LAN)의 매체 접근 제어 부분층(MACS)에서 사용하는국(局) 또는 접속구를 나타내는 주소 로 각각의 통신장치가 보유하는 고유값 |

서비스 인증정보는 서비스 제공자가 사전에 등록한 서비스를 식별할 수 있는 고유정보로 서비스 등록 시 부여받은 고유번호나 서비스 제공자의 인증정보로 구성할 수 있다.

## 2) 프로파일 관리 기능

프로파일 관리 기능은 사용자, 컨트롤러, 서비스의 프로파일을 생성, 편집, 삭제하는 역할을 한다. 프로파일은 서비스 이용 시 정보제공의 근거로 활용되는 자료로써 항상 최신성을 유지할 수 있어야 하며, 각각의 프로파일은 기기간 상호호환성 및 빠른 처리 효율을 위해 웹 표준언어인 XML을 기반으로 생성한다.

### (1) 사용자 개인정보 프로파일

사용자 개인정보 프로파일은 사용자의 인증정보뿐 아니라 기타 서비스 이용에 필요한 사용자의 개인정보를 기반으로 생성되는 정보이다. 본

연구에서는 선행연구에서 제시했던 다양한 개인정보의 유형 가운데 서비스에 활용될 수 있는 일부 개인정보 항목을 민감도에 따라 레벨을 분류함으로써 레벨에 따른 선택적 보호 및 무분별한 개인정보 수집을 방지하도록 하였다. 개인정보 민감도 레벨은 한국 CPO 포럼에서 제공하는 개인정보 영향도 등급분류와 개인정보보호법 등 유관법률에 근거하여 개인식별정보 및 프라이버시를 침해할 수 있는 민감정보 여부에 따라 다음과 같이 4등급으로 분류한다.

[표 14] 개인정보 민감도 레벨분류 예시

| 레벨 | 정보유형 | 항목 | 레벨설명 |
|---|---|---|---|
| PL1 | 식별정보 | 주민등록번호, 외국인등록번호, 여권번호, 운전면허 번호 | 개인을 식별할 수 있고, 민감한 정보를 포함하고 있어 악용할 경우 위험이 높은 정보 |
| | 신용정보 | 카드번호, 계좌번호 | |
| | 의료정보 | 질병정보, 의료기록 | |
| | 위치정보 | GPS정보 | |
| PL2 | 일반정보 | 휴대폰번호, 전화번호 | 개인을 식별할 수 있으나, 악용할 경우 위험이 다소 낮은 정보 |
| | 통신정보 | 서비스 이용기록 | |
| PL3 | 일반정보 | 아이디, 이름, 이메일 주소 | 개인을 식별할 수 없으나 개인을 식별할 수 있는 정보와 같이 노출 시 위험이 높은 정보 |
| PL4 | 일반정보 | 나이, 성별 | 개인을 식별할 수 없으며 단순 통계조사를 위해 사용되는 정보 |
| | 습관정보 | 서비스리스트, 선호도 | |

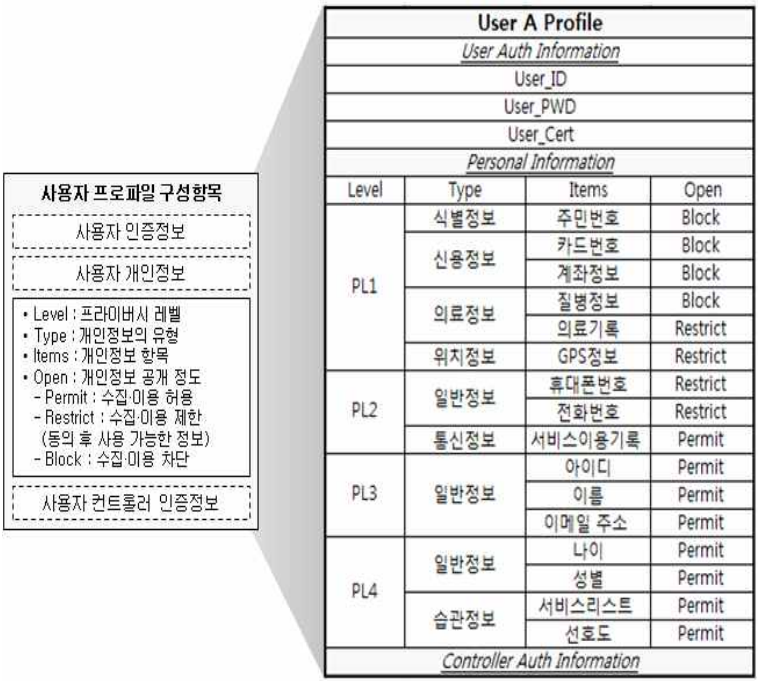
개인정보 레벨은 PL1로 갈수록 개인식별 가능한 정보와 유출 시 개인 프라이버시를 침해할 수 있는 민감한 정보를 포함하게 되며, PL4로 갈수록

개인식별이 불가하며 유출되어도 큰 프라이버시 침해문제를 발생시키지 않는 정보를 포함한다. 예를들어 PL1에는 주민등록번호, 외국인등록번호 등 해당 정보 자체만으로 개인을 식별할 수 있는 정보를 포함하고 있으며, 신용정보, 의료정보, 위치정보 등 유출 시 개인에게 큰 프라이버시 침해위협을 발생시킬 수 있는 정보를 포함하고 있다. 해당 정보들은 각각 「신용정보의 이용 및 보호에 관한 법률」의 신용정보, 「개인정보보호법」에서 정의하는 민감정보, 「위치정보의 보호 및 이용 등에 관한 법률」의 위치정보로 수집, 이용 시 정보주체의 동의를 받아야 하는 정보들이다. 이러한 정보들은 법적으로 사용을 제한하는 정보들로 유출 시 사용자의 프라이버시 침해 문제를 발생시킬 뿐 아니라, 수집, 이용하고자 할 때 반드시 사용자의 동의를 받아야 한다.

기본적으로 사용자의 개인정보 중 민감도 레벨이 높은 PL2이상의 정보는 옵트인(Opt-in)[1]방식에 따라 사용자가 허용하기 전까지는 수집할 수 없도록 설정하며, 민감도 레벨이 낮은 PL3 이하 정보는 공개로 설정한다. 사용자는 서비스 이용을 위해 개인정보 민감도 레벨에 따라 자신의 개인정보 사용여부를 설정할 수 있으며, 개인정보 항목별로 허용(Permit) 혹은 사용금지(Block), 사용시 사용자의 별도 동의를 요구하는 제한(Restrict)으로 설정할 수 있다. 사용자 개인정보 프로파일은 사용자가 소지하고 있는 컨트롤러에 컨트롤러 프로파일과 함께 저장된다. 컨트롤러 프로파일은 사용자가 소지하고 있는 컨트롤러의 정보를 담고 있는 것으로 컨트롤러 인증 시 필요한 식별정보와 모델명, 운영체체 종류, 버전, 제조사, 제조일 등의 기본적인 기기정보와 소유자의 인증정보, 사용자가 이용할 수 있는 서비스 리스트를 포함한다. 현재 상용화되고 있는 스마트 기기는 다양한

1) 옵트인(Opt-in) : 당사자가 개인 데이터 수집을 허용하기 전 까지 당사자의 데이터 수집을 금지하는 제도이다

운영체제를 탑재하고 있으며, 각 운영체제 및 버전 등에 따라 서로 다른 정책 및 표준을 따르고 있다. 따라서 서비스 제공 시 컨트롤러의 특성을 고려할 필요가 있다. 컨트롤러 프로파일의 이러한 정보는 추후 서비스 제공 시 활용할 수 있는 자료이나, 본 연구에서의 컨트롤러 프로파일은 단순히 컨트롤러의 인증을 위해서만 사용한다.




**User A Profile**

*User Auth Information*

User_ID

User_PWD

User_Cert

*Personal Information*

| Level | Type | Items | Open |
|---|---|---|---|
| PL1 | 식별정보 | 주민번호 | Block |
| | 신용정보 | 카드번호 | Block |
| | | 계좌정보 | Block |
| | 의료정보 | 질병정보 | Block |
| | | 의료기록 | Restrict |
| | 위치정보 | GPS정보 | Restrict |
| PL2 | 일반정보 | 휴대폰번호 | Restrict |
| | | 전화번호 | Restrict |
| | 통신정보 | 서비스이용기록 | Permit |
| PL3 | 일반정보 | 아이디 | Permit |
| | | 이름 | Permit |
| | | 이메일 주소 | Permit |
| PL4 | 일반정보 | 나이 | Permit |
| | | 성별 | Permit |
| | 습관정보 | 서비스리스트 | Permit |
| | | 선호도 | Permit |

*Controller Auth Information*

(그림 7) 사용자 개인정보 프로파일 예시

### (2) 서비스 프로파일

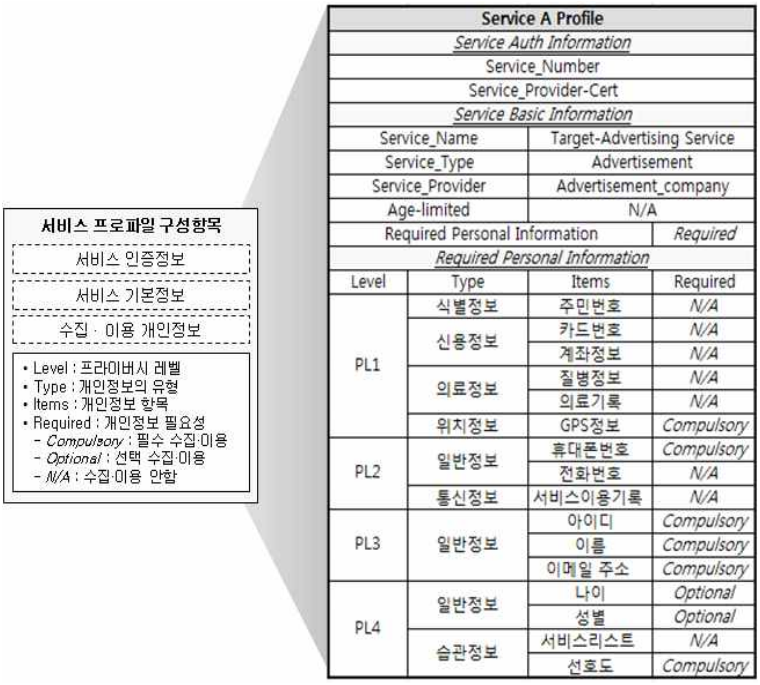
서비스 프로파일은 서비스 제공자가 제공하고자 하는 서비스에 대한 정보를 담고 있는 정보이다. 본 연구에서는 서비스 유형별로 필요로 하는 개인정보 항목을 사전에 정의함으로써 서비스 제공자에 의한 과도한 개인정보 수집을 방지할 수 있도록 서비스 기준 프로파일을 정의한다. 예를들어, 멀티미디어/엔터테인먼트 서비스의 경우에는 일반적으로 서비스

이용자의 인증정보가 요구되며, 유료 콘텐츠 결제 시 신용정보가 활용될 수 있고 미성년자의 성인 콘텐츠 이용의 제한을 위해 주민등록번호와 같이 나이를 확인할 수 있는 정보가 필요하다. 또한 사용자가 선호하는 콘텐츠 정보를 수집해 맞춤형 콘텐츠 제공에 활용할 수 있다. 마찬가지로 U-헬스케어 서비스의 경우에는 사용자의 인증정보 뿐 아니라 의료정보, 위치정보를 활용할 수 있다.

[표 15] 서비스 유형별 기준 프로파일 예시

| 레벨 | 유형 | 항목 | 서비스 | | | |
|---|---|---|---|---|---|---|
| | | | 멀티미디어/ 엔터테인먼트 | 헬스케어 | Smart TV | 기타 |
| PL1 | 식별정보 | 주민번호 | *Optional* | *Compulsory* | *Optional* | *N/A* |
| | 신용정보 | 카드번호 | *Optional* | *Optional* | *Optional* | *Optional* |
| | | 계좌정보 | *Optional* | *Optional* | *Optional* | *Optional* |
| | 의료정보 | 질병정보 | *N/A* | *Compulsory* | *Optional* | *N/A* |
| | | 의료기록 | *N/A* | *Compulsory* | *N/A* | *N/A* |
| | 위치정보 | GPS정보 | *N/A* | *Optional* | *N/A* | *Compulsory* |
| PL2 | 일반정보 | 휴대폰번호 | *Optional* | *Compulsory* | *Compulsory* | *Optional* |
| | | 전화번호 | *Optional* | *Optional* | *Optional* | *Optional* |
| | 통신정보 | 서비스 이용기록 | *Compulsory* | *N/A* | *Compulsory* | *Optional* |
| PL3 | 일반정보 | 아이디 | *Compulsory* | *Compulsory* | *Compulsory* | *Compulsory* |
| | | 이름 | *Compulsory* | *Compulsory* | *Compulsory* | *Compulsory* |
| | | 이메일주소 | *Optional* | *Optional* | *Optional* | *Optional* |
| PL4 | 일반정보 | 나이 | *Compulsory* | *Compulsory* | *Compulsory* | *Optional* |
| | | 성별 | *N/A* | *Compulsory* | *N/A* | *N/A* |
| | 습관정보 | 서비스 리스트 | *Compulsory* | *N/A* | *Compulsory* | *N/A* |
| | | 선호도 | *Optional* | *N/A* | *Optional* | *N/A* |

서비스 제공자는 제공하는 서비스에서 추가적으로 필요한 사용자의 개인정보를 수집, 활용하고자 할 경우에는 사용자에게 별도의 동의를 구해야 한다. 서비스 제공자는 서비스 제공을 위해 반드시 필요한 정보를 필수(Compulsory), 경우에 따라 수집할 필요가 있는 정보는 선택(Optional), 수집하지 않는 정보는 해당없음(N/A)로 설정한다. 서비스 프로파일은 서비스 인증정보, 서비스의 기본정보, 서비스 이용에 필요한 개인정보로 구성된다.



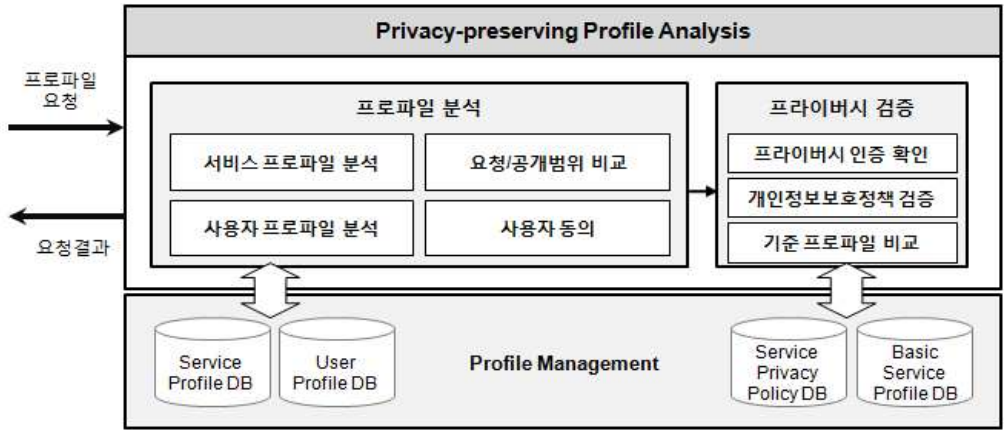

| Service A Profile | | | |
|---|---|---|---|
| *Service Auth Information* | | | |
| Service_Number | | | |
| Service_Provider-Cert | | | |
| *Service Basic Information* | | | |
| Service_Name | | Target-Advertising Service | |
| Service_Type | | Advertisement | |
| Service_Provider | | Advertisement_company | |
| Age-limited | | N/A | |
| Required Personal Information | | | *Required* |
| *Required Personal Information* | | | |
| Level | Type | Items | Required |
| PL1 | 식별정보 | 주민번호 | *N/A* |
| | 신용정보 | 카드번호 | *N/A* |
| | | 계좌정보 | *N/A* |
| | 의료정보 | 질병정보 | *N/A* |
| | | 의료기록 | *N/A* |
| | 위치정보 | GPS정보 | *Compulsory* |
| PL2 | 일반정보 | 휴대폰번호 | *Compulsory* |
| | | 전화번호 | *N/A* |
| | 통신정보 | 서비스이용기록 | *N/A* |
| PL3 | 일반정보 | 아이디 | *Compulsory* |
| | | 이름 | *Compulsory* |
| | | 이메일 주소 | *Compulsory* |
| PL4 | 일반정보 | 나이 | *Optional* |
| | | 성별 | *Optional* |
| | 습관정보 | 서비스리스트 | *N/A* |
| | | 선호도 | *Compulsory* |

(그림 8) 서비스 프로파일 예시

### 3) 프라이버시 보호 프로파일 분석 기능

프라이버시 보호 프로파일 분석 기능은 사용자 개인정보 프로파일과 서비스 프로파일을 기반으로 정보의 제공 여부를 결정하고 서비스 제공자의 개인정보보호를 위한 관련 법·제도·정책의 준수 여부를 확인하여 신뢰성을

검증하는 기능이다. 사용자가 서비스를 직접 요청하는 경우와 서비스 제공자가 서비스 제공을 위해 사용자의 정보를 요청하는 경우에 서비스에서 필요로 하는 개인정보 항목과 사용자가 공개를 허용한 개인정보 범위를 비교하여 1차적으로 개인정보의 제공 가능 여부를 결정한다. 사용자가 공개하지 않은 정보에는 접근이 불가하며 제한된 정보에는 사용자 동의를 거쳐 제공이 가능할 수 있다. 정보의 제공 여부가 결정된 후에는 프라이버시 검증 과정을 통해 서비스의 개인정보보호에 대한 신뢰성을 확인할 수 있도록 한다. 프라이버시 검증기능은 크게 3가지 과정을 거치며, 첫 번째는 국내외 인증기관으로부터 부여받은 프라이버시 관련 인증제도의 유무, 본 연구에서 제시한 최소 준수항목 기준 개인정보 정책 제시 여부, 마지막으로 서비스 유형별 기준 프로파일 대비 민감도 레벨이 높은 정보의 수집 여부를 확인한다.

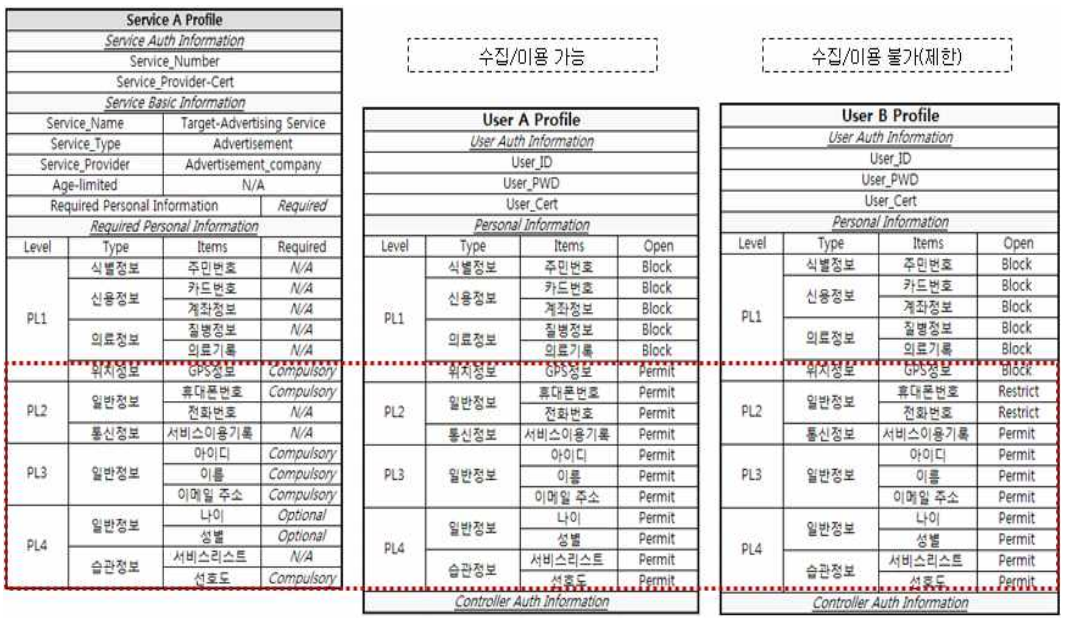



(그림 9) 프라이버시 보호 프로파일 분석 기능

### (1) 프로파일 분석

서비스 제공자에게 사용자의 개인정보 프로파일을 제공하기 위해서는 1차적으로 서비스에서 요구하는 개인정보 항목을 사용자로부터 제공받을 수

있는지 확인이 필요하다. 정보 제공 요청이 발생하면, 사용자 개인정보 프로파일과 서비스 프로파일을 분석하여 서비스에서 요구하는 개인정보 항목과 접근 가능한 사용자의 개인정보 항목을 비교한다. 서비스에서 요구하는 개인정보의 민감도 레벨이 낮고, 사용자가 접근을 허용한 정보일 경우에는 별도의 사용자 동의절차 없이 정보 제공이 가능하다. 그러나, 서비스에서 요구하는 개인정보를 사용자가 접근을 불허했거나 제한한 경우, 민감도 레벨이 높은 경우에는 서비스 이용을 차단하거나 사용자에게 별도로 동의를 받아야 한다. 본 연구에서는 PL2 이상의 정보 이용 시 사용자에게 알림메시지를 전달하며, PL1 정보에 접근시에는 사용자의 공개도에 관계없이 추가적으로 동의과정을 거친다. 사용자가 정보이용에 동의했을 경우에는 개인정보의 수집과 서비스 이용이 가능하나, 동의하지 않았을 경우에는 서비스 이용에 제한을 받으며, 서비스 제공자는 정보 수집이 불가하다. 다음의 그림은 프로파일 분석, 비교 방법의 예시이다.




(그림 10) 프로파일 분석, 비교 방법 예시

서비스 A는 사용자의 위치정보를 활용하여 맞춤형 광고를 제공하는 서비스로 개인의 이름, 아이디, 이메일주소와 같이 신원을 확인할 수 있는 정보와 서비스 제공에 필요한 선호도정보, 휴대폰 번호와 위치정보 등 부가적인 정보가 필요하다. 이때, 나이, 성별정보는 사용자의 정보 공개도에 따라 선택적으로 수집될 수 있다. 서비스 제공을 위해 서비스 제공자가 사용자 A와 B의 개인정보를 수집/이용하고자 할 시, 사용자 A의 경우에는 요구되는 개인정보 항목을 모두 접근을 허용해 두었기 때문에 별다른 사용자의 동의절차 없이 사용자의 정보가 서비스 제공자에게 수집되어 이용될 수 있다. 단, 상대적으로 민감도가 높은 PL2이상의 정보를 활용하기 때문에 사용자에게 해당 사항을 알림메시지로 전달해야 한다.

반면, 사용자 B의 경우에는 서비스 제공에 반드시 요구되는 GPS 정보에 접근을 차단한 상태이므로 서비스를 이용하기 위해서는 해당 정보를 공개해야 한다. 또한 PL2에 해당하는 휴대폰 번호 역시 사용자가 이용을 제한한 정보이므로, 사용자에게 동의를 받아야만 수집할 수 있다.

### (2) 프라이버시 검증

프라이버시 검증 기능은 서비스 제공자가 개인정보를 보호하기 위한 의무를 이행하고 있는지를 확인하여 신뢰할 수 있는 서비스인지를 판단하는 과정이다. 서비스 제공자는 개인정보 보호를 위해 개인정보 생명주기 전 단계에 걸쳐 기술적, 관리적 보호 책임을 다해야 하며, 관련 법·제도·정책을 준수해야할 의무를 지닌다. 프라이버시 검증은 기관에서 부여하는 각종 인증제도의 유무 혹은 본 연구에서 제시하는 검증항목을 준수하여 정책을 제공하고 있는지 여부, 서비스 유형별 기중 프로파일 대비 민감도 레벨이 높은 정보의 수집 여부를 기준으로 판단한다.

O 관련 인증제도 보유여부

검증된 기관으로부터 프라이버시 관련 인증을 받은 서비스의 경우에는 신뢰할 수 있다고 판단한다. 프라이버시 관련 인증에는 다음과 같이 인증제도가 있다[33,34,35,36]. 검증된 기관으로부터 프라이버시 인증을 받은 서비스는 관련 법·제도· 정책을 준수하며 개인정보 보호를 위한 기술적, 관리적 책임 의무를 하고 있는 것이므로 신뢰할 수 있는 서비스로 판단할 수 있다.

[표 16] 국내·외 주요 프라이버시 인증제도

| 구분 | 인증기관 | 인증 | 내용 |
|---|---|---|---|
| 국외 | ISO/IEC | ISO/IEC 27001 | - 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 정보보호 관리체계 국제규격 인증 |
| | 국제감사인증기준위원회(IAASB) | SOC(Service Organization Control)인증 | - 국제인증업무기준(IASE)에 따라라 서비스의 안전성 및 관련 모든 내부통제 수준을 평가하는 제도 |
| 국내 | 방송통신위원회 | 개인정보보호 관리체계(PIMS) | - 기업이 개인정보보호 활동을 체계적이고 지속적으로 수행하고 있는지를 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도 |
| | 개인정보보호협회(OPA) | ePrivacy마크 | - 개인정보보호 수준을 종합적으로 평가하여 일정수준 이상의 웹사이트에 대해 개인정보보호 우수사이트로 선정하고 마크를 부여하는 제도 |

반면, 인증제도를 보유하고 있지 않을 시에는, 다음과 같은 2가지 사항을 추가적으로 비교하여 서비스의 신뢰도를 확인할 수 있도록 한다.

O 검증항목별 개인정보 보호정책 확인

서비스 제공자는 이용자의 개인정보보호를 위해 정책을 마련하고 이를 기반으로 개인정보를 안전하게 관리하며, 개인정보 생명주기 전반에 걸쳐

프라이버시를 침해하지 않도록 기술적, 관리적 조치를 취해야 한다. 서비스의 신뢰성을 검증하기 위한 방안으로 서비스 제공자가 개인정보 보호를 위해 지켜야 할 최소한의 준수 항목을 기반으로 적절한 개인정보 보호정책을 마련했는지를 확인한다. 서비스 제공자의 개인정보 보호정책이 존재하지 않거나 미흡하다고 판단되면 사용자에게 경고메시지를 보내 위험성을 고지할 수 있도록 한다. 개인정보 보호를 위해 최소한으로 준수해야 하는 사항은 관련연구에서 살펴본 국제기구별 가이드라인과 국내 개인정보보호법을 기반으로 다음과 같이 정의할 수 있다.

[표 17] 서비스 별 프라이버시 정책 구성항목

| 단계 | 항목 | 세부내용 |
|---|---|---|
| 수집 | 수집목적 | ▪ 개인정보를 수집하는 목적을 명확하게 제시 |
| | 수집항목 | ▪ 개인정보 수집은 수집목적에 맞추어 최소한으로 해야 함 |
| | 민감정보 | ▪ 민감정보를 수집할 경우 정보주체의 동의를 받아야 함 |
| | 동의 | ▪ 사용자 동의 방법, 절차 |
| 저장 | 보유기간 | ▪ 개인정보를 보유하는 기간 |
| | 정보관리 | ▪ 개인정보의 정확성, 무결성, 가용성을 위해 취해야 할 조치 |
| | 안전조치 | ▪ 개인정보보호를 위해 취해야 할 기술적, 관리적 방안 |
| | 책임 | ▪ 개인정보 관리 책임자 |
| 이용 및 제공 | 이용목적 | ▪ 수집한 개인정보의 이용목적 |
| | 이용항목 | ▪ 이용하는 개인정보의 항목 |
| | 위탁제공 | ▪ 제3자에 제공 및 공유, 위탁여부 |
| 파기 | 파기방법 | ▪ 개인정보의 파기방법 및 절차 |

본 연구에서는 위에서 제시한 항목 가운데 수집, 이용 및 제공에 관련된 사항을 해결하기 위해 민감도가 높은 정보에 접근할 경우 사용자 알림 및

동의절차를 거치도록 하였으며, 서비스 유형별 기본적으로 수집 가능한 항목을 정의해 둠으로써 서비스 제공에 필요한 최소한의 정보만을 수집할 수 있도록 제한하였고 이를 통해 수집, 이용 목적을 명확하게 할 수 있도록 하였다. 이외에 개인정보의 보유기간, 안전조치, 책임, 위탁제공, 파기 등 개인정보의 저장 및 파기 관련사항은 서비스 제공자가 서비스 정보와 함께 등록해야 한다. 본 논문에서 제안하는 시스템은 서비스 제공자가 서비스 프로파일을 등록할 시 개인정보 보호정책을 제시하도록 하며 각 항목별로 관련 법·제도 및 가이드라인, 처벌 기준 등의 정보를 제공하여 올바른 정책을 제시할 수 있도록 한다. 개인정보 보호정책은 사용자 측면에서 자신의 개인정보를 안전하게 관리하고 있음을 확인할 수 있는 근거가 되며, 서비스 제공자 측면에서는 정책에 준한 개인정보보호 방안을 마련할 수 있고 관련 법·제도·정책에서 요구하는 사항을 준수할 수 있다.

O 서비스 유형별 기준 프로파일과의 비교

본 연구에서는 서비스 유형별 일반적으로 활용되는 개인정보 유형을 사전에 정의해두고, 서비스 제공자가 서비스를 등록할 시 기준 프로파일의 범위 내에서 개인정보를 수집할 수 있도록 제한함으로써 최소한의 정보만을 수집할 수 있도록 하였다. 서비스에 따라 기준 프로파일과는 다른 정보를 필요로 할 수 있으나, 기준 프로파일 대비 민감도가 높은 개인정보 항목을 요구하는 경우에는 사용자에게 알림 메시지를 보내 동의를 거친 후 정보를 제공할 수 있도록 한다.

### 4) 요청 제어 및 사용자 알림 기능

요청 제어 및 사용자 알림 기능은 서비스 요청 결과를 처리하고, 필요 시 사용자에게 메시지를 전달하는 기능을 한다. 프로파일 분석 결과 정보

제공이 가능하다고 판단될 시 컨트롤러에게 서비스에 개인정보 제공 가능 신호를 보내고, 컨트롤러는 센서나 다른 스마트 기기 등에 개인정보 프로파일을 전달하여 이를 바탕으로 사용자가 적절한 서비스를 제공받을 수 있도록 하는 한다. 그러나, 정보 제공 요청 과정에서 오류가 발생했거나 사용자의 동의, 고지가 필요한 경우에는 사용자에게 알림 메시지를 전달하여 적절한 조치를 취할 수 있도록 한다. 모든 요청은 로그기록으로 남겨 추후 발생가능한 사고에 대응할 수 있는 책임추적성을 제공하며, 법적인 근거 자료로 활용할 수 있다. 사용자 알림 메시지는 다음과 같이 크게 4가지 단계로 구분되며 각각 알림에 해당하는 설명과 발생상황은 다음표와 같다.

[표 18] 사용자 알림 메시지 예시

| 알림구분 | 메시지 설명 |
|---|---|
| Violation | ▪ 프라이버시 침해위협이 존재하는 경우<br>- 민감한 정보를 요청하나, 프라이버시 검증 과정을 수행할 수 없는 경우(예 : 개인정보 보호정책 확인 불가 등) |
| Warning | ▪ 프라이버시를 침해할 위협은 낮으나, 서비스 이용에 필요한 정보가 부족한 경우<br>- 서비스 제공 정보가 부족한 경우<br>▪ 민감도가 높은 정보에 접근하는 경우<br>- PL2 이상의 정보에 접근하는 경우<br>▪ 인증에 실패한 경우<br>- 사용자 인증정보, 컨트롤러정보 서비스정보의 통합인증 실패 시 |
| Agreement | ▪ 사용자의 별도 동의가 필요한 경우<br>- 사용자가 제한한 정보에 접근하는 경우<br>- PL1에 해당하는 정보에 접근하는 경우 |
| Deny | ▪ 서비스 제공이 불가한 경우<br>- 서비스에 반드시 필요한 필수정보 접근을 차단한 경우<br>- 미성년자가 성인 콘텐츠 서비스에 접근을 시도한 경우 |

# Ⅴ. 설계 및 구현

## 1. 알고리즘

제안한 프라이버시 보호 개인정보 프로파일 관리 시스템(PPMS)의 주요 기능인 프로파일 분석 및 프라이버시 검증 기능을 중심으로 알고리즘으로 제시하였다.

먼저 통합인증 과정에서는 사용자의 인증정보, 사용자 소유 컨트롤러의 인증정보, 서비스의 인증정보를 통합하여 인증함으로써 요청의 유효성을 판단한다. 이후 사용자, 혹은 서비스에 의해 사용자 개인정보 요청이 발생하면 프로파일 분석을 위해 서비스에서 요구하는 개인정보 항목과 사용자의 개인정보 공개레벨을 비교한다. 본 알고리즘에서는 사용자 개인정보 프로파일과 서비스 프로파일은 이미 정의되어 있다고 가정하여 작성하였다. 비교결과, 서비스에서 요구하는 사용자 개인정보가 공개되어 있을경우에는 접근이 허용되며, 제한된 정보가 있을 경우에는 접근제한, 사용이 금지된 정보가 포함될 경우에는 접근이 차단된다. 접근이 허용되었을 시, 서비스에서 요구하는 개인정보의 민감도가 PL2이상으로 민감한 정보일 경우에는 사용자에게 동의를 받을 수 있도록 한다. 이후에는 프라이버시 검증 기능을 통해 서비스의 신뢰성을 확인하는 절차를 거치며, 신뢰성을 확인할 수 없는 경우에는 사용자에게 경고 메시지를 보내 위험성을 고지시킨다. 사용이 제한된 정보에 접근했을 경우에는 반드시 사용자의 동의를 받아야 하며, 동의를 받은 후에는 접근 허용시와 마찬가지로 프라이버시 검증 과정을 통해 서비스의 신뢰성을 확인할 수 있도록 한다. 사용이 금지된 정보에 접근하는 경우에는 알림메시지를 통해

정보를 사용할 수 없음을 알린다. 각각의 모든 경우는 로그기록을 남김으로써 책임추적성을 제공할 수 있도록 한다.

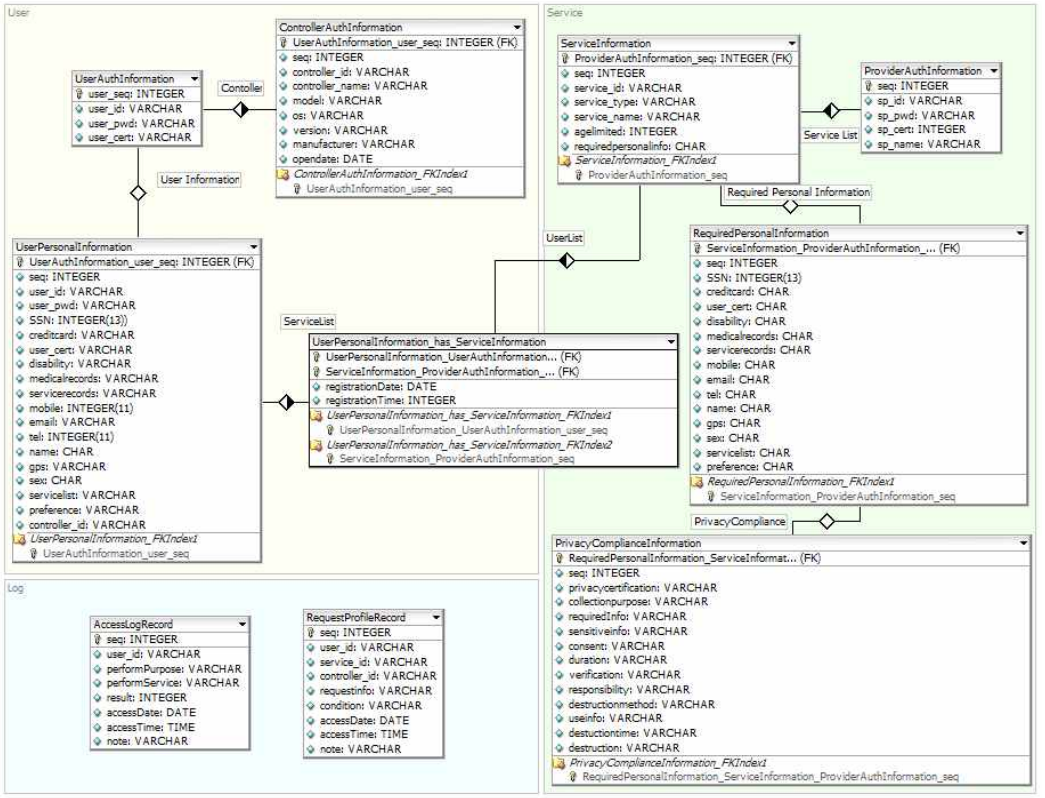
**Algorithm**

```
1: user.auth ← 사용자 인증정보
2: controller.auth ← 컨트롤러 인증정보
3: service.auth ← 서비스 인증정보
4:
5: if AllIdentityMng(user.auth, controller.auth, service.auth) = true then
6:    AllAuthResult ← true
7: else
8:    AllAuthResult ← false
9:    LogRecord(WARNING, AuthenticationFailMsg)
10: end if
11:
12: if AllAuthResult = true ∧ PersonalInfoRequired = true then
13:    user.profile ← RequestUserProfile(user.auth)
14:    service.profile ← RequestServiceProfile(service.auth)
15:    service_requiredinfo ← checkRequiredInfo(service.profile)
16:    user_openlevel ← checkUserOpenLevel(user.profile)
17:    accessResult ← ProfileComparison(service_requiredinfo, user_openlevel)
18:    switch accessResult
19:       case Permit:
20:          if service_requiredinfo ≥ PL2 then
21:             UserMsg(WARNING, AGREEMENT)
22:             if AGREEMENT = false then
23:                return false
24:             end if
25:          if checkPrivacyCompliance(service.auth) = true then
26:             provided_profile ← ProvideUserProfile(user.profile)
27:             LogRecord(user.auth, service.auth, provided_profile, timestamp)
28:          else
29:             UserMsg(VIOLATION, AGREEMENT)
30:             if AGREEMENT = true then
31:                provided_profile ← ProvideUserProfile(user.profile)
32:             end if
33:             LogRecord(user.auth, service.auth, accessResult, note, timestamp)
34:          end if
35:       case Restrict:
36:          UserMsg(WARNING, AGREEMENT)
```

```
37:           if AGREEMENT = true then
38:             if checkPrivacyCompliance(service.auth) = true then
39:                 provided_profile ← ProvideUserProfile(user.profile)
40:             end if
41:           else
42:             LogRecord(user.auth, service.auth, accessResult, note, timestamp)
43:       case Disable:
44:           UserMsg(DENY)
45:           LogRecord(user.auth, service.auth, accessResult, note, timestamp)
46:     end switch
47: else
48:     UserMsg(WARNING)
49:     return false
50: end if
51:
52: Function checkPrivacyCompliance(service.auth){
53:     privacyPolicy ← requestPrivcayPolicy(service.auth)
54:     if privacyPolicy has PrivacyCertification then
55:       return true
56:     else
57:       i ← 0
58:       while i ≤ privacyPolicyItems[].length do
59:         if privacyPolicyItems[i] is invalid then
60:           return false
61:         end if
62:         i++
63:       end while
64:       service.profile ← RequestServiceProfile(service.auth)
65:       serviceType ← RequestServiceType(service.profile)
66:       service_requiredinfo ← checkRequiredInfo(service.profile)
67:       defaultServiceProfile ← RequestDefaultServiceProfile(serviceType)
68:       if service_requiredinfo ≥ defaultServiceProfile then
69:         return false
70:       end if
71:     end if
72: }
```

## 2. 데이터베이스 설계

본 논문에서 제시한 프라이버시 보호 개인정보 프로파일 관리 시스템(PPMS)의 데이터 베이스는 크게 사용자, 서비스 부분, 로그 부분으로 구분될 수 있다.




(그림 11) PPMS 데이터베이스 설계

사용자 부분은 사용자의 인증정보, 개인정보 및 공개도, 소유하고 있는 컨트롤러의 정보, 이용하는 서비스 정보 테이블로 구성되며, 서비스 부분은 서비스 제공자의 인증정보와 서비스 제공자가 등록한 서비스 정보 테이블로 구성된다. 서비스에는 서비스에 대한 기본적인 정보 뿐 아니라 해당

서비스에서 요구하는 개인정보의 항목을 포함하며 서비스 제공자의 개인정보보호 관련 법·제도, 가이드라인을 준수여부를 확인할 수 있는 프라이버시 컴플라이언스 테이블로 구성된다. 로그 부분은 사용자와 서비스 제공자의 시스템 접근기록을 남기기 위한 테이블과 사용자에 의한 서비스 요청 시와 서비스 제공을 위해 사용자의 개인정보를 요청할 시 프로파일 분석 결과를 기록하는 테이블로 구성한다.

## 3. 프로토타이핑

본 논문에서 제안하는 프라이버시 보호 개인정보 프로파일 관리 시스템(PPMS)의 실 환경에서의 적용 가능성을 검증하기 위해 테스트 환경을 구축하고 간략한 프로토타이핑을 구현하였다.

테스트 환경은 크게 PPMS 서버, 사용자, 서비스 제공자로 구분되며, 서비스 제공자와 사용자는 PPMS 시스템의 클라이언트가 된다. PPMS 서버는 Window7 환경에서 구현 하였으며, Apache Tomcat 5.5버전을 지원한다. 개발언어는 JSP, JAVA 언어를 사용하였으며, DBMS는 MySQL 5.5버전을, 개발 도구로는 서버와 클라이언트 모두 Eclipse를 사용하였다. 사용자는 웹페이지 혹은 스마트 기기를 통해 서비스를 이용할 수 있으며 스마트 기기의 경우 기기의 종류에 관계없이 실제 스마트 기기에서 사용이 가능하도록 하기 위해 HTML5를 활용하여 구현하였다. 실제 적용시에는 사용자의 컨트롤러에 탑재되어 사용자 개인정보 프로파일을 직접 타 기기 및 센서 등에 전달하고 기타 필요한 기능을 수행할 수 있는 별도의 모듈이 필요하나, 본 프로토타이핑 에서는 서버에서 해당 역할을 대신할 수 있도록 구현하였다. 서비스 제공자의 경우에는 사용자 개인정보 프로파일을 수집하는 서버 혹은 다른 스마트 기기 등이 될 수 있으며, 프로토타이핑에서는 서비스 제공자가 PPMS를 이용해 서비스 정보를 등록 하고, 필요 시 사용자의 프로파일을 제공받을 수 있는지 여부를 확인할 수 있도록 하였다. 서비스 제공자는 이를 통해 실제 적용시 사용자의 개인정보 프로파일을 전달받아 서비스 이용에 활용할 수 있다. 프로토타이핑은 사용자, 서비스 제공자, PPMS 시스템 관리자로 나누어 다음과 같은 기능을 포함할 수 있도록 하였다.

□ 사용자화면 - 사용자 등록, 프로파일 생성, 프로파일 분석결과 확인

□ 서비스 제공자 화면 - 서비스 등록, 사용자 개인정보 프로파일 확인

□ 관리자 화면 - 사용자/서비스 관리, 시스템 로그 확인

## 1) 사용자 화면

서비스를 이용하는 사용자는 자신의 개인정보를 시스템에 등록하고, 개인정보 항목별로 공개레벨을 설정한다. 공개레벨은 개인정보 민감도에 따라 초기 설정값이 지정되어 있으며, 사용자에 의해 변경이 가능하다. 최초 등록 이후에도 공개레벨은 수정이 가능하며, 등록화면과 수정화면에서는 개인정보 민감도 및 공개레벨 설정에 대한 설명을 보여줌으로써 사용자가 적절하게 레벨을 설정할 수 있도록 한다. 사용자 등록이 완료되면 PPMS 시스템은 이를 기반으로 XML형태의 사용자 개인정보 프로파일을 생성하며, 생성된 사용자 프로파일은 시스템 서버와 사용자의 컨트롤러에 저장된다.


(그림 12) 사용자 등록 화면

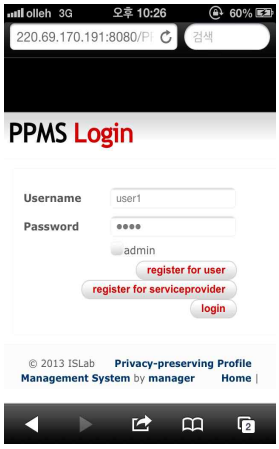

(그림 13) XML형태로 생성된 사용자 개인정보 프로파일

시스템에 등록된 사용자는 PPMS을 통해 서비스를 직접 요청할 수 있으며, PPMS는 사용자의 요청에 따라 서비스 프로파일과 사용자 개인정보 프로파일을 분석하고 제공 여부가 결정되면 서비스 제공자에게 사용자 개인정보 프로파일을 전달하여 사용자에게 적절한 서비스를 제공할 수 있도록 한다. 프로토타이핑에서는 사용자가 자신이 소지하고 있는 컨트롤러와 웹을 통해 서비스를 요청할 수 있도록 하였다. 사용자가 서비스 요청을 하면, PPMS는 프로파일 분석을 통해 사용자의 동의가 필요한 경우 알림 메시지를 전달하며, 서비스 이용에 필요한 개인정보 항목을 고지한다. 프로파일 분석결과 개인정보를 제공할 수 있다고 판단이 되면, PPMS는 서비스의 신뢰성을 확인하기 위해 프라이버시 검증 기능을 수행한다. 프라이버시 검증은 PPMS 상세기능 설명에서 제시했던 것과 같이 관련 인증제도의 보유여부, PPMS 검증항목별 개인정보 보호정책, 서비스 유형별 기준 프로파일과의 비교를 통해 판단한다. 다음의 화면은 사용자가 웹상에서 서비스를 요청했을 시 프로파일의 분석결과를 보여주는 화면과 프라이버시 정책 검증 결과를 보여주는 화면이다.


(그림 14) 분석결과 및 사용자 동의 화면


(그림 15) 프라이버시 검증 결과 화면

프로파일 분석결과 사용자 동의가 필요한 경우에는 동의 메시지를 통해 사용자의 동의를 거쳐야 하며, 서비스의 신뢰성을 확인할 수 없는 경우에는 경고 메시지를 통해 위험성을 사용자에게 고지시킨다. 최종적으로 서비스 제공자에게 프로파일을 제공할 경우에는 수집되는 개인정보 항목을 확인할 수 있도록 한다. 다음은 사용자의 컨트롤러를 통해 PPMS을 이용할 경우 화면으로, 컨트롤러를 통해 서비스를 요청할 수 있고, 서비스 제공자에 의해 정보요청을 받았을 경우 알림 메시지를 확인할 수 있다.



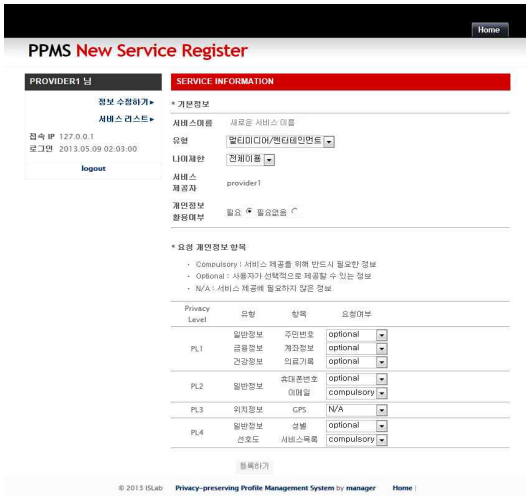

(그림 16) 스마트 기기 시스템 접속 화면


(그림 17) 스마트 기기 알림 메시지 화면

## 2) 서비스 제공자 화면

서비스 제공자는 PPMS에 제공하고자 하는 서비스를 등록해야 한다. 서비스에서 요구하는 개인정보 항목은 시스템에서 제공하는 서비스 유형별 서비스 기준 프로파일을 바탕으로 작성하며, 수정이 가능하다. 또한 프라이버시 정책을 PPMS에서 제공하는 항목에 맞추어 함께 등록해야 하며 이때 각 항목별 관련법령, 가이드라인, 벌칙 정보를 제공하여 적절한 개인정보 보호정책을 제시할 수 있도록 한다.

서비스 제공자는 서비스 제공을 위해 사용자의 개인정보 프로파일을 직접 요청할 수 있다. 이때 PPMS는 사용자가 서비스를 직접 요청했을 시와 마찬가지로 서비스 프로파일과 사용자 개인정보 프로파일을 비교, 분석하여 정보 제공 여부를 결정하고 경우에 따라 사용자에게 알림 메시지를 보낸다. 서비스 제공자가 제공받는 사용자 개인정보 프로파일은 XML형태이며, 이는 XML이 웹 표준으로써 스마트 기기간 정보를 공유할 시 상호호환성 및 빠른 처리 효율을 가져올 수 있다. 다음은 서비스 제공자가 서비스를 등록하는 화면과 개인정보 보호정책을 입력하는 화면이다.



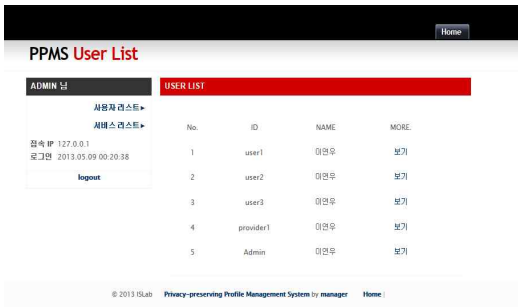

(그림 18) 서비스 등록 화면


(그림 19) 프라이버시 정책 입력 화면

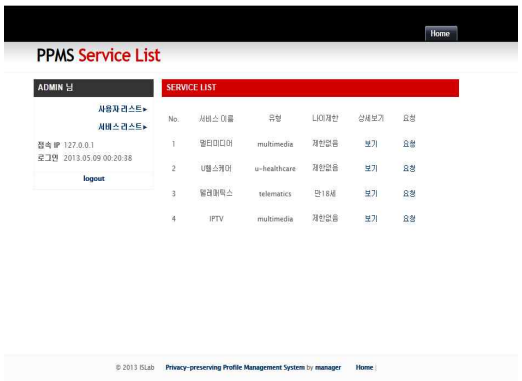
### 3) 관리자 화면

PPMS 관리자는 사용자와 서비스 제공자, 서비스를 관리하며 시스템 접근 로그를 확인할 수 있다. 사용자 리스트는 PPMS에 등록된 회원들의 정보를 볼 수 있는 화면으로 관리자는 사용자의 요청에 의해 시스템에서 회원 정보를 수정, 삭제할 수 있다. 만일 PPMS 서버에서 사용자의 개인정보가

삭제되었을 경우에는 서비스 제공자에게 해당 개인정보 프로파일을 파기할 수 있도록 고지하고 이를 확인할 수 있어야 한다. 본 프로토타이핑에서는 해당 기능은 포함하지 않고 있으며 단순히 사용자와 서비스의 리스트를 확인하고 수정, 삭제할 수 있도록 하였다.



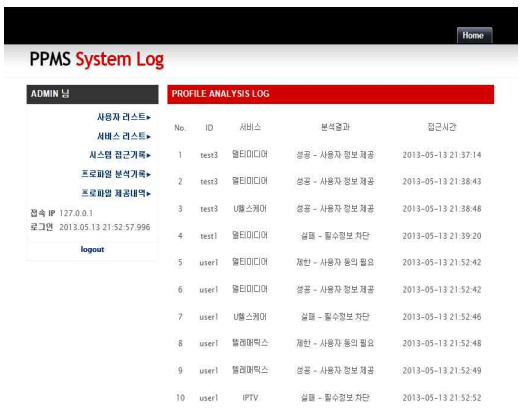

(그림 20) 사용자 리스트 화면




(그림 21) 서비스 리스트 화면

다음의 화면은 PPMS 접근 내역과 프로파일 분석결과를 기록한 로그이다. 관리자는 로그를 바탕으로 사고 발생 시 책임추적성을 확보할 수 있으며 비정상적인 접근시도를 탐지하여 개인정보 침해위협을 최소화 할 수 있다.


(그림 22) 시스템 접근기록 화면



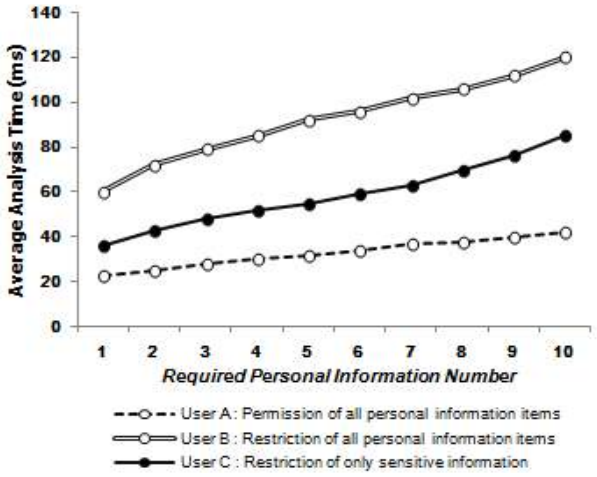

(그림 23) 프로파일 분석기록 화면

# Ⅵ. 분석 및 평가

본 논문에서는 스마트 기기 환경 내 개인화 서비스를 위해 사용자의 개인정보를 활용하는 경우 사용자의 개인정보를 보호할 수 있는 프라이버시 보호 개인정보 프로파일 관리 시스템을 제안하였다. 제안한 시스템은 사용자가 자신의 개인정보의 공개도를 정보의 민감도 레벨에 따라 다르게 설정함으로써 무분별한 정보 제공을 방지하며, 서비스에서 요구하는 정보 프로파일과의 비교, 분석을 통해 서비스의 이용 가능여부를 파악한다. 또한 서비스 제공자의 개인정보 관련 정책을 확인하여 서비스의 신뢰성을 검증할 수 있도록 하였다. 본 연구의 실환경에의 적용을 위해 개발한 시스템을 기반으로 개인정보보호와 관련된 성능을 평가하고자 시뮬레이션을 수행하였다. 서버 프로그램은 Intel Core i5 2.67GHz, 4.00GB RAM 환경의 컴퓨터 상에서 구현되었으며 개발도구는 Eclipse, 개발에 사용된 운영체제는 Windows7이며 Java JDK 1.70 버전을 사용한다. 웹서버를 활용하여 서버 프로그램을 실행하게 되면, 사용자는 시스템에 접속해 원하는 기능을 수행할 수 있다.

성능평가는 크게 프로파일 분석과 프라이버시 검증을 위해 2단계로 나누어 진행하였다. 첫 번째는 프로파일 분석 기능의 성능평가로, 서로 다른 공개레벨을 갖는 사용자가 요구되는 개인정보 항목 수가 다른 서비스를 이용할 시 프로파일 분석에 소요되는 평균 시간을 측정한다. 요구 개인정보 항목은 1개부터 10개까지 변화시켰으며 요청하는 항목수가 증가할수록 민감도가 높은 정보를 포함하게 된다. 사용자 A는 모든 정보를 공개한 사용자로 개인정보 항목 수가 증가할수록 소요되는 시간의 증감이 미비하며 이는 별도의 동의절차를 거치지 않기 때문에 소요시간이 적기 때문이다.

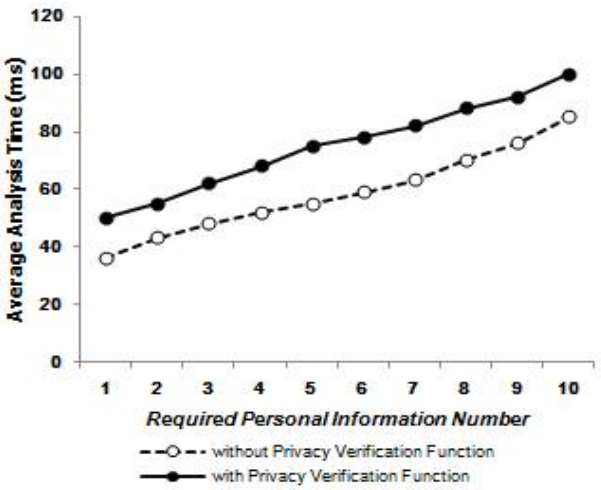
사용자 B는 모든 개인정보의 이용을 제한하여 해당 정보를 이용할 때마다 사용자의 동의를 요구한다. 따라서 이용하는 개인정보 항목수가 증가함께 따라 분석에 소요되는 시간 역시 크게 증가함을 알 수 있다. 사용자 C는 민감한 정보일 경우에만 사용자 동의를 받도록 설정하였다. 따라서 요청하는 개인정보 항목수가 증가할수록 민감한 정보를 포함할 경우가 많아져 프로파일 분석에 소요되는 시간이 증가함을 알 수 있다. 그러나, 사용자 B가 모든 정보에 동의를 요구한것과 달리 일부 민감정보를 요청할 경우에만 동의를 요구하도록 함으로써 사용자 B보다는 적은 분석시간을 보인다. 이는 모든 정보를 허용으로 했을 시보다는 분석에 더 많은 시간이 소요되나, 민감한 정보 이용 시 사용자 동의를 요구함으로써 사용자의 개인정보를 보호하면서도 이용에 큰 불편을 주지 않는 정도의 차이로 보인다.




(그림 24) 프로파일 분석 성능 평가

두 번째는 프라이버시 검증기능의 성능을 검증하기 위한 것으로 첫 번째에 진행했던 실험에 덧붙여 서비스 제공자의 프라이버시 정책을 검증하는 기능을 추가하여 진행하였다. 해당평가는 민감정보만을 제한한 사용자 C를 기준으로 프라이버시 검증을 수행했을 경우와 그러지 않았을 경우의

성능을 비교함으로써 프라이버시 검증에 소요되는 시간을 확인한다. 아래 그래프에서 보듯이 프라이버시 검증을 수행했을 경우에는 수행하지 않았을 때 비에 시간이 더 소요되나 그 차이는 평균 20.3 밀리초로 이는 실제 사용자가 서비스를 이용하는데 큰 불편함을 느끼지 않는 차이로 보인다.




(그림 25) 프라이버시 검증 성능 평가

위 두가지 실험결과에서 보듯이 사용자의 개인정보 보호를 위해 민감정보 이용을 제한하고, 프라이버시 검증절차를 거칠 경우 시간이 더 소요됨을 알 수 있다. 그러나 이는 사용자 입장에서 개인정보를 보호하며 서비스 이용에 큰 불편함을 주지 않는 정도인 것으로 사료되며, 실 환경에 적용할 시 개인정보를 안전하게 보호하며 성능면에서도 큰 문제가 되지 않을 것으로 보인다. 하지만 해당 성능평가 결과는 상대적으로 고성능인 PC환경에서, 즉 서버 단에서의 프로파일 분석, 검증시간을 측정한 것이므로 상대적으로 저성능인 스마트 기기에 탑재되어 해당 기능을 수행할 시에는 소요시간이 더 걸릴 것으로 예상된다. 따라서 실제 스마트 기기에 탑재될 경우에는 스마트 기기의 성능을 고려해야 할 것이다.

# Ⅶ. 결론 및 향후연구

개인 스마트 기기의 보편화와 지능형 가전기기, 센서기술, 네트워크 기술 등의 발전으로 보다 편리하고 자동화된 생활이 가능해지고 있다. 특히, 개인 스마트 기기가 주변의 각종 가전기기나 센서 등을 인식하고 제어하여 사용자 개인에게 최적화된 서비스를 제공하는 개인환경서비스에 대한 연구가 활발하게 진행되고 있다. 그러나 개인환경서비스에서는 필연적으로 사용자의 개인정보가 수집되어 서비스에 활용될 수 있는데 반해, 사용자는 자신의 개인정보가 언제 어떻게 수집, 사용되었는지 확인하거나 정보 제공을 제어할 수 있는 방안은 미흡하다. 또한 관련 법·제도에서는 서비스 목적에 필요한 최소한의 정보수집, 민감정보 활용 시 사용자 동의 등 사용자 프라이버시를 보호하기 위한 사항을 명시하고 있으나 이와 관련된 연구는 미흡한 실정이다. 이에 본 논문에서는 스마트 기기간 통신 시 개인화 서비스를 위해 다양한 기기를 통해 사용자의 개인정보를 수집, 활용하는 경우 관련 법·제도· 정책에서 규제하는 사항을 고려하며 사용자의 프라이버시를 보호할 수 있는 개인정보 프로파일 관리 방안을 제시하였다. 이를 위해 본 연구에서는 스마트 기기 환경의 특징과 개인정보보호 동향, 선행연구를 검토하여 발생 가능한 개인정보 침해위협을 도출하고 개인정보 보호와 관련된 국내·외 관련 가이드라인 등을 기반으로 최소한으로 준수해야 하는 항목을 개인정보 생명 주기 단계별로 분류하였다. 본 연구에서 제안한 시스템은 사용자가 직접 자신의 개인정보 공개범위를 설정하며 민감정보 요청 시 동의를 받을 수 있도록 함으로써 자신의 정보를 제어할 수 있는 기능을 제공한다. 또한 개인정보를 활용하는 서비스 제공자는 서비스 제공 목적에 필요한 정보만을 수집하도록 하며, 민감정보 활용 시

사용자 동의, 개인정보 보호정책 마련 등을 하게 함으로써 관련 법·제도·정책에서 명시하는 최소한의 요구사항을 충족 시킬 수 있도록 하였다. 이는 사용자 측면에서 무분별한 개인정보의 수집을 방지함으로써 프라이버시 침해위협을 최소화할 수 있으며 서비스 제공자 입장에서는 관련 법·제도·정책을 준수하여 개인정보를 활용함으로써 컴플라이언스 측면의 강화 및 개인정보 유·노출 사고로 인한 피해를 최소화 할 수 있을 것으로 보인다.

향후연구로는 본 연구에서 제시했던 서비스 유형별 기준 프로파일을 정의하기 위한 명확한 표준이나 기준이 존재하지 않으므로 이에 대한 연구를 지속할 예정이다. 또한 본 연구에서 제시했던 최소한의 법·제도·정책 준수 항목 가운데 저장 및 파기 관련 사항은 단순히 서비스 제공자가 제시한 정책만을 근거로 신뢰성을 판단하며, 실제 서비스 제공자의 이행여부 및 검증방안에 대한 사항은 미흡하다. 따라서 개인정보 저장 및 파기와 관련된 사항을 해결할 수 있는 연구가 필요할 것으로 보인다. 아울러 본 논문에서 제안한 시스템을 실 환경에 적용하기 위해서는 사용자 스마트 기기에 탑재되어 사용자의 프로파일을 관리하고 타 기기 및 센서 등에 사용자 개인정보 프로파일을 제공하는 별도의 모듈이 필요하다. 이때 반드시 스마트 기기의 성능을 고려하여 빠른 처리속도를 보장하는 방안 또한 지속적으로 연구되어야 할 것이다. 향후 개인 스마트 기기를 활용한 다양한 개인화 서비스가 등장할 것으로 예상되는 가운데 본 연구는 스마트 기기 환경 내 개인정보 관련 법·제도· 정책을 고려하여 개인정보를 보호하는 방안으로 활용 가능할 것으로 기대된다.

# 참고 문헌


[1] 홍승필, “개인정보보호 개론“, 한티미디어, 2009.

[2] 개인정보보호위원회, “2012 개인정보보호 연차보고서”, 2012.

[3] 대한민국국회, “개인정보보호법”, 법률 제10465호, 2011.03.

[4] 안전행정부, “개인정보보호법 주요 내용 및 향후 추진과제”, 2011.

[5] 한국인터넷진흥원, “2013 국가정보보호백서”, 2013, pp.124-143.

[6] 인터넷침해대응지원센터, “개인정보침해신고 상담건수”, 2013.

[7] 한국인터넷진흥원, “유비쿼터스 프라이버시보호 종합대책 수립”, 2007.

[8] OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, Available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 1980.

[9] OECD, “Machine-to-Machine Communications: Connecting Billions of Devices”, OECD Digital Economy Papers, No. 192, 2012.

[10] APEC, “APEC Privacy Framework”, Available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, 2005.

[11] 유상근, 홍용근, 김형준, “스마트모바일 서비스 - M2M 기술 및 표준 동향”, 전자통신동향분석 Vol.26 No.2, 2011.04, pp.50-60

[12] 이근호, “M2M 기술 및 보안 동향”, 인터넷정보학회지 Vol.13 No.1, 2012.03, pp.21-29.

[13] 백은경, 이성춘, “미래인터넷 생태계에서의 M2M 서비스”, Digieco Focus, kt경제경영연구소, 2010.05.

[14] 임종인, “주요국가의 개인정보보호 동향조사, 한국인터넷진흥원, 2009.

[15] 전은정, 김학범, 염홍열, “미국의 개인정보보호 법·제도 동향”, 정보보호학회지 Vol.22 No.1, 2012.02, pp.47-57.

[16] 전은정, 김학범, 염홍열, “유럽의 개인정보보호 법·제도 동향”, 정보보호학회지 Vol.22 No.2, 2012.04 , pp.58-72.

[17] Jongtaek Oh, Zygmunt J. Haas, “Personal Environment Service based on the Integration of Mobile Communications and Wireless Personal Area Networks”, IEEE Communications Magazine, Vol.48 No.6, 2010.06, pp.66-72.

[18] 오종택, “휴대폰과 사용자 개인정보 프로파일 기반의 개인환경서비스(PES)”, TTA Journal No.130, 2010.07, pp.67-74.

[19] 노종혁, 진승헌, “웹 환경에서 정책 기반 개인정보보호 기술”, 전자통신동향분석 Vol.22 No.4, 2007.08.

[20] 장현미, 김경진, 김혜리, 정지희, 홍승필, 강성민, “인터넷 환경 내 개인정보보호 아키텍처 설계 방안”, Entrue Journal of Information Technology Vol.8 No.1, 2009.01, pp.117-131.

[21] 김경식, 이재동, “효율적인 프로파일 운영을 위한 웹 서비스 기반의 프로파일 프레임워크”, 정보과학회논문지 Vol.13 No.1, 2007.11, pp.11-23.

[22] 송창우, 김종훈, 정경용, 류중경, 이정현, “시맨틱 웹에서 개인화 프로파일을 이용한 콘텐츠 추천 검색 시스템”, 한국콘텐츠학회논문지 Vol.8 No.1, 2008.01, pp.318-327.

[23] 신사임, 이종설, 장세진, 이석필, “사용자 개인정보 프로파일 기반의 맞춤형 광고 서비스 및 양방향 개인 맞춤형 방송 시스템 구축”, 방송공학회논문지 Vol.15 No.5, 2010.09, pp.632-641.

[24] 박민영, 권혁철, “스마트폰 사용자를 위한 사용자 맞춤형 광고 서비스 모델”, 한국정보과학회논문지 Vol.39 No.8, 2012.08.

[25] 은선기, 전서관, 안재영, 오수현, “안전한 M2M 통신 구축을 위한 상호인증 및 키 교환 프로토콜”, 정보보호학회논문지 Vol.20 No.1, 2010.02.

[26] 박남제, “사용자 프라이버시를 보장하는 모바일 RFID 개인 정보보호 서비스 시스템”, 정보기술학회논문지 Vol.8 No.10, 2010.10, pp.87-96

[27] Nancy J. King, Pernille Wegener Jessen, “Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones – Part I”, Computer Law and Security Review(CLSR) Vol.26 No.5, 2010.09, pp.455-478.

[28] Gudymenko, I, Katrin B., and Katja T., “Privacy Implications of the Internet of Things.“, Constructing Ambient Intelligence. Springer Berlin Heidelberg, 2012, pp.280-286.

[29] Biswas D., Haller S., Kerschbaum F., “Privacy-Preserving Outsourced Profiling”, Proceedings of 2010 IEEE 12th Conference on Commerce and Enterprise Computing (CEC), 2010.11, pp.136-143

[30] 이준규, 김지호, 송오영, “u-City환경에서 맞춤형 서비스 제공을 위한 프로파일기반 개인 정보보호 관리”, 정보처리학회논문지 Vol.17 No.2, 2010.04, pp.135-144

[31] Weber, Rolf H., “Internet of Things-New security and privacy challenges.“ Computer Law & Security Review(CLSR) Vol.26 No.1, 2010.01, pp.23-30.

[32] 한국정보통신기술협회, “모바일 환경의 사용자 중심 개인화 서비스를 위한 사용자 데이터 처리 구조”, 정보통신단체표준 TTAK.KO-12.0196, 2012.12.

[33] ISO/IEC, ISO/IEC27001, Available at http://www.bsigroup.co.kr/ko-kr/Assessment-and-certification-services/Management-systems/Standards-and-schemes/ISO-IEC-27001/

[34] 국제감사인증기준위원회(IAASB), SOC(Service Organization Control)인증, Available at http://www.aicpa.org/interestareas/frc/assuranceadvisory services/pages/sorhome.aspx

[35] 방송통신위원회 개인정보보호관리체계(PIMS), Available at http://isms.kisa.or.kr/kor/intro/pimsIntro01.jsp

[36] 개인정보보호협회(OPA), ePrivacy마크(정보보호인증마크제도), Available at http://www.eprivacy.or.kr/Info-introduction.do

[37] 이홍섭, “개인정보와 프라이버시”, NHN 개인정보보호 칼럼, Available at http://privacyblog.naver.com/80131529831, 2011.06.

[38] 한국CPO포럼, “CPPG가이드북”, 2012.

[39] Seng-phil Hong, Joon Young Kim, Yeonwoo Lee, “Detecting Privacy-Related Threats via Dynamic Risk Assessing Model in Cloud Computing Environments”, INFORMATION Vol.16 No.2(B), 2013.02.

[40] 이연우, 장현미, 홍승필, “빅데이터 환경 내 개인정보보호를 위한 대용량 개인정보 관리 모델 설계방안”, 한국인터넷정보학회 추계학술발표대회 논문집 Vol.13, No.2, 2012.11.

[41] 김지영, 이연우, 장현미, 김경진, 홍승필, “스마트 환경 내 개인정보 보호를 위한 프로파일링 방안 연구”, 한국인터넷정보학회 춘계학술 발표대회 논문집 Vol.14 No.1, 2013.05.

[42] Senghwan Choi, Sungju Lee, Yeonwoo Lee, Changsun Kim, Taikyeong Jeong, “Secure Video Transmission on Smart Phones for Mobile Intelligent Network”, International Journal of Secuirty and Its Applications(IJSIA) Vol.7, No.1, 2013.01.

# ABSTRACT

## A Study on Design and Application of Privacy Information Profile in Smart Device Environment

Yeonwoo Lee
Dept. of Computer Science
The Graduate School
Sungshin Women's University

With the advent of smart devices and popularization of the internet, the ubiquitous computing environment is on its way which can make us connect to the Internet anytime and anywhere. Recently, there are many studies on smart device communication and they has applied a variety of user-oriented services. In smart device environment, personal data can be collected via different channel such as RFID tags, sensors and smart devices. Service providers can make user's profile based on a mass of collected personal data and use it to provide user-oriented services. However, the collected personal data includes new types of information such as location information, habit, and healthy information which are sensitive information that has possibilities to analyze about user's tendency and pattern of behavior and it can violate user's privacy. Especially, privacy protection must be considered in case of collecting personal data

from user's smart devices, which have become necessity, and using it in order to provide user-oriented services to the user.

In this paper, I propose the Privacy-preserving Personal Information profile Management System(PPMS) to protect user's privacy considering related laws, guidelines and policies in case of collecting and using personal data to provide user-oriented services in smart device environment. At first, I examine theoretical background of both smart device environment and privacy information protection, after briefly introducing the purpose, background and scope of this research. And then I formulate possible privacy threats in smart device environment and suggest the necessity of this research by reviewing precedent studies and analyzing smart device environment threats. To solve formulated privacy threats, I propose the PPMS to protect user's privacy in smart device environment and build a prototype for verifying possibility of the application in real environment. After that, I analyze proposed system by evaluating time performance. Finally, I conclude this research and suggest future research work.