TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx 제정일: 2019 년 12 월 31 일

사물 인터넷 환경에서 개인정보 선호도에 기반한 개인정보 처리 보안 프레임워크

Personally identifiable information handling security framework based on privacy preference in the Internet of things environment

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 개인정보보호/ID관리, 블록체인 보안(PG502)

표준안 심의 위원회 정보보호기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	염흥열	순천향대학교	교수	PG502 위원	
표준 초안 작성자	염흥열	순천향대학교	교수	PG502 위원	
	김지혜	한국정보기술단	연구원	PG502 참관위원	
사무국 담당	황예지	TTA		TC 5 간사	

(※ '표준번호'는 제정 또는 개정 시의 표준번호를 기입한다.)

(※ 개정된 표준일 경우, 공헌자를 제정 및 개정 표준별로 구분하여 병기할 수 있다.)

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2019.12

서 문

1 표준의 목적

사물 인터넷 환경에서는 다양한 데이터가 수집되며, 이러한 데이터가 여러 서비스 제공자에게 공유될 수 있다. 사물 인터넷 환경에서 사용자 프라이버시 선호도에 따른 개인정보 처리 시스템의 기술 프레임워크를 제시할 필요가 있다. 본 표준은 사물 인터넷 환경에서 사용자 선택에 따른 개인정보 처리 시스템의 설계와 활용을 가능하게 한다.

2 주요 내용 요약

본 표준은 사물 인터넷 환경에서 개인정보 (PII) 처리 시스템을 위한 기술 프레임워크를 정의한다. 본 표준은 단일 및 다중 서비스 제공자를 위한 사물 인터넷 환경에서 개인정보 처리시스템의 서비스 모델, 개인정보 처리를 위한 주요 규제, 개인정보처리 시스템의 보안 요구사항, 개인정보 처리시스템의 모델과 관련 요구사항을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

본 표준은 다음 2개의 국제표준에 근거해 개발되나, 국내 개인정보보호 법제도의 요구사항을 반영한다.

- ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework
- ITU-T X.iotsec-3, Technical framework for a personally identifiable information handling system in the Internet of things environment

3.2 인용 표준과 본 표준의 비교표

TTAK.xx-xx.xxxx/R1	ITU-T X.iotsec-3	비고
6 개인정보 선호도 기반 사물 인터넷 서비스 모델	7 The Internet of things service model with single or multiple service	동일(번역)

	providers	
7. 개인정보 선호도 기반 개인정보 처리 관련 개인정보 규제	-	추가
8 사물 인터넷 서비스에서 개인정보 데이터를 처리하기 위한 고려 사항	8 Issues concerning PII data on IoT services	번역하여 한국의 상황에 맞게 수정
9 사물 인터넷 서비스에 의한 개인정보 처리를 위한 보안 요구사항	9 Principles for PII data handling by IoT services	동일(번역)
10 사물인터넷 서비스에 의한 개인정보 처리 보안 프레임워크 모델	10 PII data handling in the IoT environment	동일(번역)
11. 사물 인터넷 서비스에 의한 개인정보 처리 기술 프레임워크	11 Technical framework for PII data handling in the IoT environment	동일(번역)

Preface

1 Purpose

In the Internet of things environments, a variety of data including PII (Personally Identifiable Information) is collected, and that data can be shared among various service providers.
The purpose of this standard is to present the technical framework of the PII handling system according to the user privacy preference in the Internet of things environment. This standard allows to design and utilize PII handling system in accordance with user 's privacy preference in the Internet of things environments.

2 Summary

The standard defines the technical framework for the PII handling system based on user's privacy preference in the Internet of things environment. This standard describes service models, major regulations, and security requirements for the PII handling system based on user's privacy preference. It also describes handling models for PII handling systems and their related security requirements.

3 Relationship to Reference Standards

This standard is developed based on the following two international standards, but reflects the requirements of the domestic privacy laws and regulations.

- ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework
- ITU-T X.iotsec-3, Technical framework for a personally identifiable information handling system in the Internet of things environment

목 차

사물 인터넷 환경에서 개인정보 선호도에 기반한 개인정보 처리 보안 프레임워크 (Personally identifiable information handling security framework based on privacy preference in the Internet of things environment)

1 적용 범위

사물 인터넷 환경에서는 다양한 데이터가 수집되며, 이러한 데이터가 여러 서비스 제공자에게 공유될 수 있다. 본 표준은 사물 인터넷 환경에서 사용자 개인정보 선호도에 따른 개인정보 처리 시스템의 기술 프레임워크를 제시할 필요가 있다. 본 표준은 사물 인터넷 환경에서 사용자 개인정보 선호도에 따라서 작동하는 개인정보 처리 시스템의 설계와 활용에 이용 가능하다.

2 인용 표준

ITU-T X.iotsec-3, Technical framework for a personally identifiable information handling system in the Internet of things environment

ISO/IEC 29100:2011, Information technology-Security techniques-Privacy framework

3 용어 정의

3.1 개인정보 (personally identifiable information) [ISO/IEC 29100]

자체로 해당 정보와 관련된 (a) 개인정보 주체를 식별하는 데 사용될 수 있거나, (b) 개인정보 주체와 직접적으로 또는 간접적으로 연결하는데 이용되는 정보.

3.2 개인정보 데이터 (personally identifiable information data)

개인정보를 포함하고 있는 데이터

3.3 개인정보 선호도 (PII preference) [ISO/IEC 29100:2011]

정보주체가 자신의 개인 정보가 특정 목적으로 처리되는 방법에 대한 개인정보 주체에 의해 이뤄진 특정 선택

3.4 개인정보 선호도 관리자 (PII preference manager)

개인정보 주체가 자신의 개인정보 처리 선호도를 설정하게 하고 이에 기반해 자신의 개인정보에 대한 이용 및 제 3 자 제공을 가능하게 만드는 실체

3.5 개인정보파일 [b-개인정보보호법]

개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

3.6 개인정보처리자 [ISO/IEC 29100:2011]

개인 목적으로 데이터를 사용하는 자연인을 제외한 개인 정보 처리 목적과 수단을 결정하는 이해 관계자

3.7 옵트인 [b-ISO / TS 17975: 2015]

정보주체가 특정 유형의 개인정보 처리에 대해 구체적이고, 명시적이며, 사전적 동의를 표시하는 별도의 조치를 취하는 정책 프로세스 또는 유형

3.8 옵트아웃 [b-ISO / TS 17975: 2015]

특정 유형의 개인정보 처리에 대한 동의를 보류하거나 철회하기 위해 정보주체가 별도의 조치를 취해야 하는 정책 또는 프로세스 유형

참조-1: 옵트아웃인 경우, 정보주체가 명시적으로 허가를 거부하거나 철회하지 않으면, 조직이 개인 정보를 처리할 수 있는 묵시적 동의를 간주한다. 옵트아웃은 정보주체가 특정 유형의 개인정보 처리를 수행하는 허가를 거부하거나 취소 할 수 있기 위해 데이터 수집 조직에 의해 제공되는 프로세스이다.

3.9 정보주체 [ISO/IEC 29100:2011]

정보주체가 특정 유형의 개인정보 처리에 대해 구체적이고, 명시적이며, 사전적 동의를 표시하는 별도의 조치를 취하는 정책 프로세스 또는 유형

4 약어

해당 사항 없음

5 개인정보 선호도 기반 개인정보처리 보안 프레임워크 개요

사물 인터넷 환경에서 많은 유형의 사물 인터넷 디바이스가 존재하지만, 그 중 일부는 수집되는 데이터에 개인정보(예, 위치정보)를 포함한다. 데이터에 포함된 개인정보(이후 개인정보 데이터로 칭함)는 다양한 유형의 서비스에 이용할 수 있으므로 서비스 제공자는 정보주체로부터 개인정보가 포함된 다양한 데이터를 수집하려 한다. 이러한 서비스 제공자는 데이터를 수집하는 제공자와 다른 서비스 제공자에서 수집된 데이터를 이용해 서비스를 제공하는 서비스 제공자로 구분된다.

정보주체 관점에서 보면, 개인정보 데이터는 이러한 서비스 제공자에 의해 적절하게 처리되어야 한다. 정보주체가 사물 인터넷 환경에서 개인정보 데이터 처리 방법에 대해 의도를 지정할 수 있어야 한다. 여러 서비스 제공자가 존재하는 사물 인터넷 환경의 개인정보 데이터 이용은 매우 복잡하기 때문에 데이터 사용에 대한 사용자의 의도가 유연하게 제공되어야 한다. 예를 들어, 사물 인터넷 플랫폼에 다음과 같은 기능이 제공된다면 개인정보 데이터는 적절하게 처리되고 있다고 볼 수 있다.

- ·정보주체는 자신의 개인정보 데이터의 처리 선호도를 설정할 수 있어야 한다. 선호도 목록은 정보주체가 수집을 허용하는 개인정보 데이터 목록과 정보주체가 자신의 개인정보 데이터에 대한 접근할 수 있도록 허가하는 서비스 제공자 목록을 포함한다.

- ·수집된 개인정보 데이터에 대한 접근 통제는 개인정보 처리 선호도에 기초해야 한다. 정보주체가 공유를 허용하지 않은 개인정보 데이터는 다른 서비스 제공자에게 공유할 수 없다.

- ·정보주체는 서비스 제공자에게 공유되는 데이터의 접속 로그를 확인할 수 있어야 한다. 사용자는 데이터 이용의 타이밍과 빈도를 알아야 한다.

6 개인정보 선호도 기반 사물 인터넷 서비스 모델

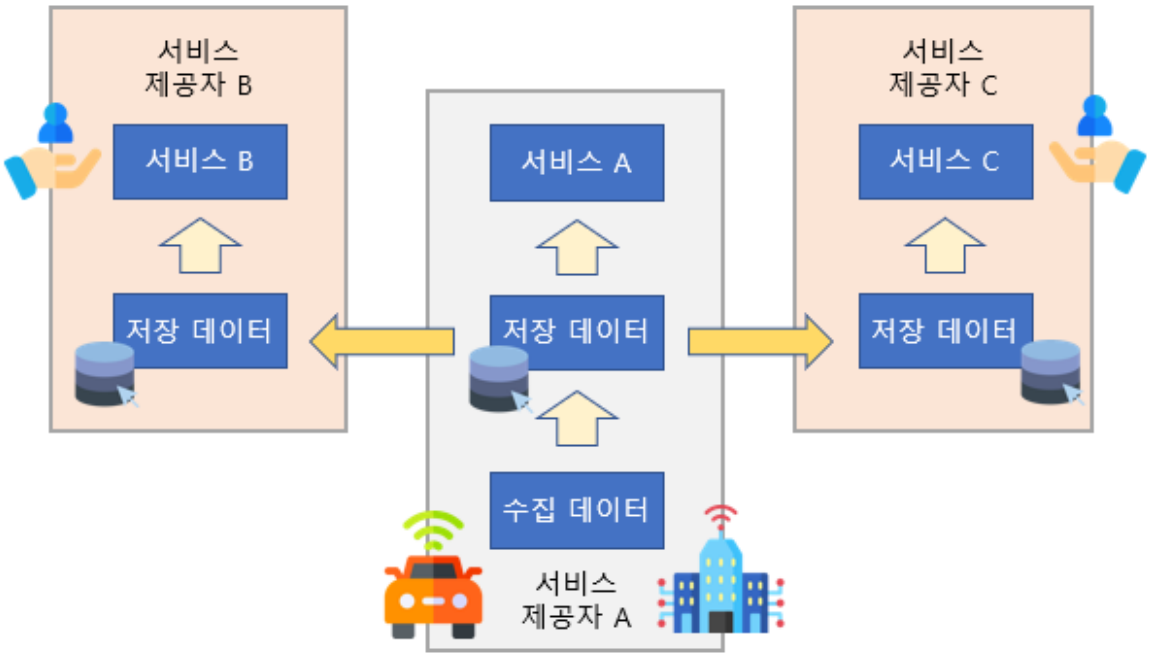
개인정보 선호도 기반한 사물 인터넷 서비스 모델은 크게 2가지로 구분된다. (그림 6-1)은 하나의 서비스 제공자에 의해 제공되는 서비스 모델이다.

(그림 6-1) 단일 사물 인터넷 서비스 제공자 모델

첫 모델은 (그림 6-1)과 같이 하나의 서비스 제공자에 의해 제공되는 단일 사물 인터넷 서비스 모델이다. 이 모델에서는 서비스 제공자가 개인정보를 포함한 여러 종류의 데이터를 수집하고 보유한다. 서비스 제공자는 개인정보 데이터를 보낸 정보주체에게 유익한 서비스를 제공한다.

(그림 6-2)와 같은 다른 사물 인터넷 서비스 모델은 하나의 서비스 제공자가 정보주체로부터 개인정보 데이터를 수집하여 그 데이터를 다른 여러 서비스 제공자에게 공유하는 모델이다. 예를 들어, 서비스 제공자 A가 사물 인터넷 디바이스로부터 개인정보 데이터를 수집하여 다른 서비스 제공자 (예를 들어, 서비스 제공자 B 및 서비스 제공자 C)와 공유한다.

일반적으로 다른 서비스 제공자와 공유되는 개인정보 데이터 목록은 서비스를 위한 약관에 포함되어 있으며 사용자는 서비스를 사용하기 위해서는 이 약관에 동의해야 한다.



(그림 6-2) 다중 사물 인터넷 서비스 제공자 모델

7 개인정보 선호도 기반 개인정보 처리 관련 개인정보 규제

개인정보보호법을 기본으로 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률 등에서 개인정보보호와 관련된 사항을 규정한다.

•· 수집 및 이용 단계

개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

•· 제공 단계

개인정보처리자는 정보주체의 동의를 받은 경우에는 정보주체의 개인정보를 제3자에게 제공(또는 공유)할 수 있다.

•· 수집 및 이용을 위한 동의

개인정보처리자는 정보주체의 수집 및 이용을 위한 동의를 받을 때에는 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의

내용 등의 정보주체에게 알려야 한다.

•· 제3자 제공을 위한 동의

개인정보처리자는 제공을 위한 동의를 받을 때에는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 등의 사항을 정보주체에게 알려야 한다.

8 사물 인터넷 서비스에서 개인정보 데이터를 처리하기 위한 고려 사항

개인정보 데이터가 사물 인터넷 서비스에 의해 처리될 때 다음 사항을 고려해야 한다.

•· 개인정보 데이터 수집 목적 설명

정보주체 관점에서 불필요한 개인정보 데이터 수집을 피하기 위해 정보주체에게 데이터 수집의 목적과 서비스를 위해 수집된 개인정보 데이터의 유형과 성격을 알려야 한다.

•· 개인정보 데이터 수집에 대한 필수 동의

서비스에 가입하고자 하는 정보주체는 여러 유형의 개인정보 데이터의 수집에 동의해야 한다. 일반적으로 이 정보는 약관에 쓰여지며 정보주체는 서비스를 이용하려 할 때 이 약관에 동의해야 한다.

•· 개인정보 데이터 제3자 제공

사물 인터넷 장치로부터 수집된 데이터는 제3자(다른 서비스 제공자)와 공유될 수 있다. 이 경우 서비스 제공자는 개인정보 데이터를 제3자에게 보내기 전에 정보주체의 동의를 얻어야 한다. 일반적으로 정보주체는 개인정보 데이터의 전송을 통제할 수 없다. 다시 말해, 정보주체는 개인정보 데이터 전송을 허용하는 제3자를 선택할 수 없으며 개인정보 데이터의 유형을 설정할 수 없다. 또한 정보주체는 어떤 종류의 개인정보 데이터가 제3자에게 전송되는지 알 수 없다.

•· 개인정보 데이터 수집의 옵트인 및 옵트아웃 동의

서비스가 정보주체 개인정보 데이터를 사용하려면 서비스 제공자는 개인정보 데이터를 수집하기 위한 정보주체의 동의를 얻어야 한다. 동의 획득 시기와 동의 획득 방법(옵트인 또는 옵트아웃)도 고려되어야 한다.

9 사물 인터넷 서비스에 의한 개인정보 처리를 위한 보안 요구사항

9.1 일반 보안 요구사항

개인정보는 특정 개인을 식별하거나, 특정 개인에게 연락하거나, 또는 특정 개인을 찾는데 사용될 수 있다. 개인정보 유출은 신원 도용 또는 기타 사기적 목적으로 이어질 수 있다. 이로 인해 개인에게 심각한 물적 및 정신적 피해, 당혹, 불편을 초래한다. 따라서 사물 인터넷 서비스에서 개인정보 데이터를 처리할 때 다음과 같은 일반적 보안 요구사항을 만족해야 한다.

•· 개인정보 데이터 암호화

민감 데이터가 아닌 한, 사물 인터넷 디바이스 상 또는 개인정보 데이터를 저장하는 서비스 데이터베이스 상에 저장되어 있는 개인정보 데이터는 암호화되어야 한다. 모든 민감 데이터는 시스템의 모든 구성요소 (즉, 장치, 저장 장치, 응용/서비스) 간에 전송되는 동안 암호화되어야 한다.

•· 인증/접근 제어

개인정보 데이터가 사물 인터넷 디바이스 또는 서비스 데이터베이스에 저장되는 경우, 적절한 접근 제어가 적용되어야 한다. 개인정보에 대한 접근 권한은 접근 요구의 이용 목적을 달성을 위해서만 주어져야 한다. 이 이용 목적은 서비스 제공자가 정보주체의 동의를 얻은 목적에 포함되어야 한다. 허용되지 않은 식별 또는 추가적으로 민감 데이터를 추론하게 하는 저장 데이터 세트 간에 연결 가능성이 있을 때 그러한 데이터 세트의 접근은 제어되어야 한다.

•· 로깅

개인정보가 포함된 컴퓨터 판독 가능 데이터 추출물의 생성은 작성자, 일시, 정보 유형, 추출 목적 및 사용자를 포함한 공식 로그에 관리해야 한다. 이러한 로그에 포함된 모든 개인정보 (예, 사용자 이름)는 암호화되어 접근 제어의 대상이 되어야 한다.

•· 통신 암호화

개인정보 데이터가 여러 서비스 제공자 사이에 공유되면 이 데이터는 암호화되거나 마스크되어야 한다.

•· 데이터 훼손 통보

시스템에서 데이터 누설, 유출, 오용 또는 오 처리로 인해 개인정보 데이터가 훼손된 경우 서비스 제공자는 훼손 사실을 발견한 즉시 영향받는 정보주체에게 알려야 한다.

• · 보유를 위한 데이터 최소화 절차

개인정보 데이터의 저장은 서비스 제공자가 수행한 데이터 처리 결과로 생성되거나 수집되는지 여부에 무관하게 서비스 제공자가 명시적 동의를 얻은 목적으로 만으로 제한되어야 한다. 서비스 제공자는 이용 목적, 추가적인 민감한 데이터의 식별 또는 추론을 초래할 수 있는 저장된 데이터 세트 간의 연결 가능성, 적용 가능한 법률 및 규정에 근거해서 개인정보I 데이터의 보존을 위한 최대 기간을 설정해야 한다.

9.2 개인정보 처리를 위한 보안 요구사항

사물 인터넷 디바이스에서 개인정보 데이터를 수집하는 서비스 제공자는 이를 적절하게 처리해야 한다. 특히 데이터가 서비스에 의해서 이용되거나 다른 서비스 제공자에게 공유되는 경우 데이터 처리는 사용자의 의도를 충족해야 한다. 따라서 사물 인터넷 서비스로 개인정보 데이터를 처리할 때 다음 요구 사항을 충족해야 한다.

• · 개인정보 데이터 수집 목적 설명

정보주체로부터 개인정보 데이터를 수집하기 위해 서비스 제공자는 약관에서 개인정보의 수집 목적과 보유 기간을 설명해야 한다.

• · 사용자로부터 개인정보 데이터를 수집하는 명시적 동의

서비스 제공자는 정보주체로부터 개인정보 데이터를 수집하는 서비스를 제공하는 경우 데이터 수집에 대한 명시적 동의를 얻어야 한다. 특히 서비스 제공자는 가능하면 동의를 얻기 위한 옵트인 모델을 구현해야 한다.

• · 개인정보 데이터 이용의 추적 가능성

서비스 제공자가 수행하는 데이터 처리 출력으로 생성된 중요한 데이터를 포함하여 개인정보 데이터를 다른 서비스 제공자와 공유할 경우, 시스템은 정보주체가 개인정보 데이터 이용을 확인할 수 있도록 개인정보 데이터에 대한 추적 메커니즘을 제공해야 한다. 또한 시스템은 데이터 불일치가 발생할 경우 사용자가 사용할 수 있는 수정 도구를 제공해야 한다.

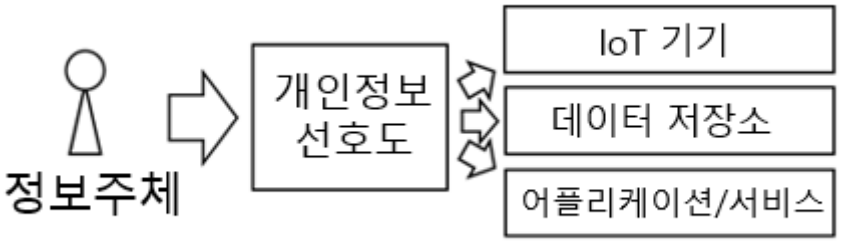
• · 개인정보 선호도 설정

개인정보 데이터는 정보주체가 설정한 개인정보 통제 선호도에 따라 처리해야 한다.

10 사물인터넷 서비스에 의한 개인정보 처리 보안 프레임워크 모델

10.1 개인정보 선호도 기반 프레임워크

사물 인터넷 환경에서 선호도 기반의 개인정보 데이터를 처리하기 위한 기본 프레임워크는 (그림10-1)과 같다. 정보주체는 개인정보 데이터 처리에 대한 개인정보 선호도를 결정하고 이를 개인정보 선호도 매니저에 설정한다. 정보주체의 개인정보 데이터는 개인정보 선호도 관리자에 의해 통제된다.



(그림10-1) 개인정보 데이터 처리를 위한 기본 프레임워크

개인정보 선호도는 다음 항목을 포함한다.

- **사물 인터넷 디바이스가 수집하는 데이터 종류:** 사물 인터넷 디바이스는 사용자가 자신의 개인정보 선호도 설정에서 지정한 개인정보 데이터만을 수집할 수 있다.

- **사물 인터넷 디바이스에 의한 데이터 수집 시기 (예: 평일 9:00에서 17:30 사이):** 정보주체는 언제나 개인정보 데이터가 수집되기를 원하지 않으므로 수집 시기가 개인정보 선호도에 설정되어야 한다.

- **수집된 개인정보 데이터를 공유할 수 있도록 허용된 서비스 제공자:** 정보주체는 자신의 개인정보 데이터에 접근할 수 있는 서비스 제공자를 선택할 수 있다. 또한 정보주체는 서비스 제공자가 접근할 수 있는 모든 개인정보 데이터를 선택할 수 있다. 여기에는 사물 인터넷 디바이스에서 수집된 데이터를 포함해서 일차 서비스 제공자에 의해 수행된 데이터 처리 결과를 포함한다.

10.2 개인정보 선호도 설정을 위한 사용자 인터페이스 요구사항

서비스 제공자는 정보주체가 개인정보 선호도를 설정할 수 있도록 사용자 인터페이스를 제공해야 한다. 이 사용자 인터페이스는 다음 요구사항을 충족해야 한다.

- **정보주체 친화적인 접근**: 모든 정보주체는 사용자 인터페이스에 쉽게 접근할 수

있어야 한다. 예를 들어, 서비스의 첫 화면에 사용자 인터페이스에 대한 접근 링크를 제공해야 한다.

- **사용자 인터페이스에 대한 적절한 접근 제어:** 정보주체는 자신의 개인정보 선호도 설정 환경을 갖는다. 따라서 이 선호도에 접근하기 전에 정보주체는 인증되어야 한다.

- **포괄적 인터페이스:** 개인정보 선호도 설정 인터페이스는 한 곳에서 관리가 가능해야 한다.

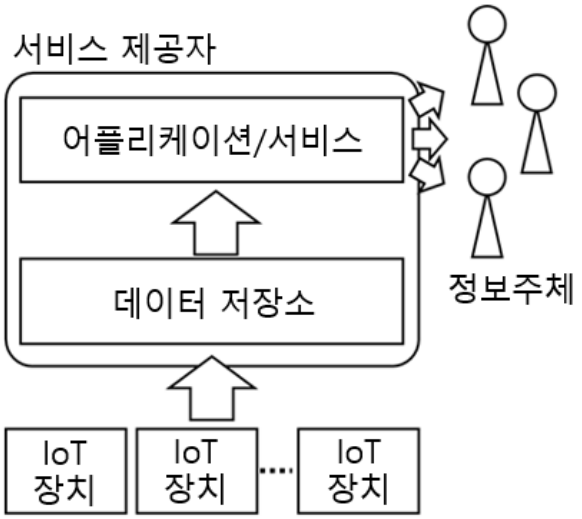
- **사용하기 쉬운 인터페이스:** 사용자 인터페이스는 개인정보 선호도를 설정하기 위해 쉽고 간단해야 한다.

11 사물 인터넷 서비스에 의한 개인정보 처리 기술 프레임워크

11.1 단일 서비스 제공자에 의한 사물 인터넷 서비스

11.1.1 참조 모델

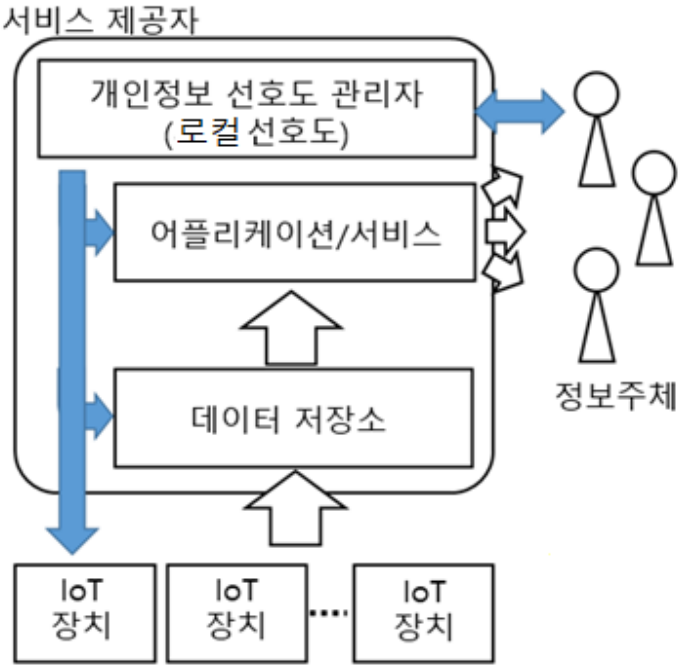
(그림 11-1)는 하나의 사물 인터넷 서비스 공급자가 제공하는 개인정보 선호도에 기반한 사물 인터넷 서비스에 대한 참조 모델을 보여준다. 하나의 서비스 제공자는 서비스의 모든 기능을 제공한다. 서비스 제공자는 사물 인터넷 디바이스로부터 개인정보 데이터를 수집하고 데이터 저장소에 개인정보 데이터를 저장한다. 수집된 데이터를 이용하여 사용자에게 맞춤형 서비스 또는 응용 프로그램을 제공한다.



(그림 11-1) 단일 서비스 제공자에 의한 사물 인터넷 서비스 참조 모델

11.1.2 단일 서비스 제공자에 의한 개인정보 데이터 처리를 위한 기술 프레임워크

(그림 11-2)는 개인정보 선호도 관리자가 하나의 서비스 제공자의 시스템에 위치하여 정보주체로부터 수집된 개인정보 데이터를 처리하기 위한 기술 프레임워크를 나타낸다. 정보주체는 개인정보 선호도 관리자로 개인정보 선호를 설정하며, 사물 인터넷 디바이스, 데이터 저장소, 그리고 응용/서비스와 같은 서비스의 구성 요소는 해당 선호도에 기반하여 개인정보 데이터를 처리한다. 하나의 서비스 제공자에 대한 정보주체의 특정 개인정보 선호도를 로컬 선호도라고 한다. 예를 들어, 사용자가 사물 인터넷 디바이스로부터 수집된 특정 개인정보 데이터를 못하게 하면, 사물 인터넷 디바이스는 정보주체의 개인정보 선호도를 참조해 이러한 개인정보 데이터가 데이터 저장소로 전송되지 않도록 한다.



(그림 11-2) 단일 서비스 제공자에 의한 데이터 처리를 위한 기술 프레임워크

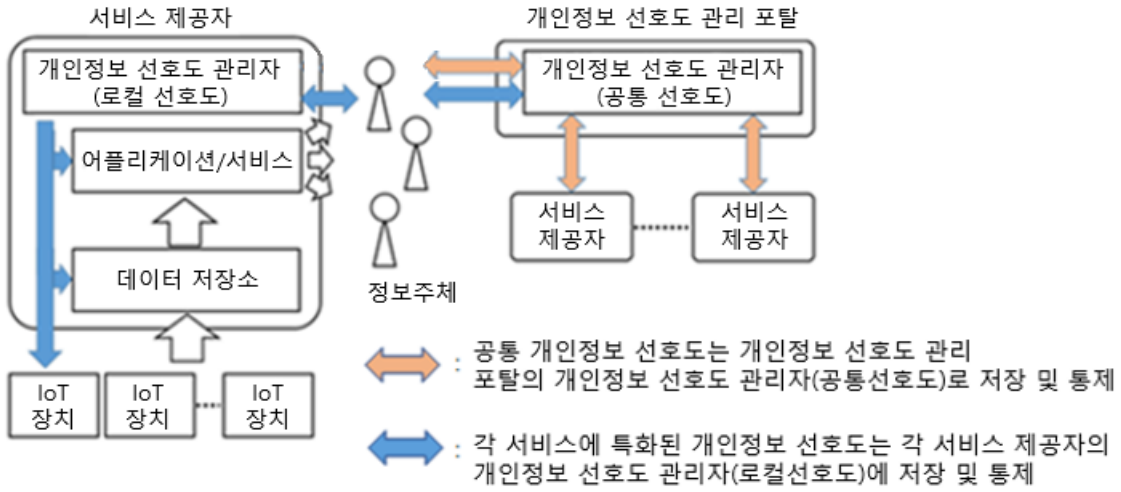
11.1.3 공통 개인정보 선호도 관리 서비스 제공자를 갖는 단일 서비스 제공자에 의한 개인정보 데이터 처리를 위한 기술 프레임워크

사물 인터넷 서비스가 단일 서비스 제공자에 의해 제공되는 경우, 사물 인터넷 장치에 의해 수집된 데이터는 다른 종류의 사물 인터넷 서비스를 제공하는 다른 서비스

제공자와 공유되지 않는다. 그러나 PII 환경 설정의 기본 항목 중 일부는 다른 서비스와 공유할 수 있다. 각 사물 인터넷 서비스에 대해 개인정보 선호도 환경 설정을 구성하는 데 시간이 오래 걸릴 수 있지만 정보 주체가 모든 종류의 사물 인터넷 서비스에 대해 공통 개인정보 선호도 환경 설정을 제공할 수 있으면 각 서비스에 대한 개인정보 선호도 설정을 쉽고 효율적으로 구성할 수 있다. 이 매커니즘을 실현하기 위해 기술 프레임워크에는 두 가지 유형의 개인정보 선호 관리자가 있다.

(그림 11-3)은 두 가지 유형의 개인정보 선호 관리자가 존재하는 기술 프레임워크이다. 여기서 하나는 서비스 제공자의 시스템에 위치하며 다른 하나는 다른 서비스 제공자와의 공통 개인정보 선호도를 관리하는 데 이용되는 개인정보 선호도 관리 포탈에 존재한다.

이 경우 모든 서비스에 대한 공통의 개인정보 선호도는 개인정보 선호도 포탈에 저장되며, 각 서비스에 특화된 개인정보 선호도는 각 서비스 제공자가 관리하는 개인정보 선호도에 저장된다. 정보주체는 서비스를 등록할 때 서비스 제공자 시스템의 개인정보 선호도 관리자는 제3자에 의해 관리되고 정보주체가 미리 사전에 설정해 놓은 개인정보 선호도 관리 포탈에서 공통 개인정보 선호도를 조회한다. 정보주체는 개인정보 선호도 관리자로 개인정보 선호도를 설정하지만, 개인정보 선호도 관리 포탈에 저장된 공통 개인정보 선호도를 반복적으로 설정하지 않는다. 사물 인터넷 디바이스, 데이터 저장소, 그리고 응용/서비스와 같은 서비스의 구성 요소는 개인정보 선호도 관리자 내에 개인정보 선호도에 따라 개인정보 데이터를 통제한다.

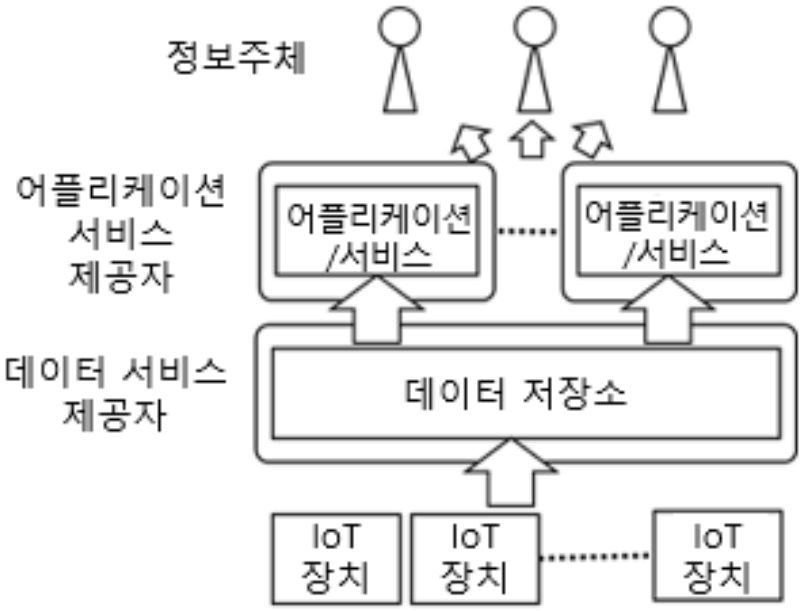


(그림 11-3) 개인정보 선호도 관리 포탈에 의한 개인정보 데이터 처리 기술 프레임워크

11.2 다중 서비스 제공자에 의한 사물 인터넷 서비스

11.2.1 참조 모델

(그림 11-4)은 여러 사물 인터넷 서비스 제공자가 공급하는 사물 인터넷 서비스에 대한 참조 모델을 나타낸다. 이 경우 여러 서비스 제공자는 사물 인터넷 서비스 플랫폼을 구성하고 각 서비스 제공자는 사물 인터넷 장치에서 수집한 데이터를 사용하여 자체 서비스를 사용자에게 제공한다. 따라서 사물 인터넷 디바이스에서 개인정보 데이터를 수집하는 서비스 공급자는 사용자에게 서비스를 제공하는 서비스 제공자와 다를 수 있다. (그림 11-4)에서 볼 수 있듯이 사물 인터넷 디바이스에서 개인정보를 포함한 데이터를 수집하는 '데이터 서비스 제공자'와 수집된 데이터를 사용하여 사용자에게 응용/서비스를 제공하는 '어플리케이션 서비스 제공자'가 존재한다.

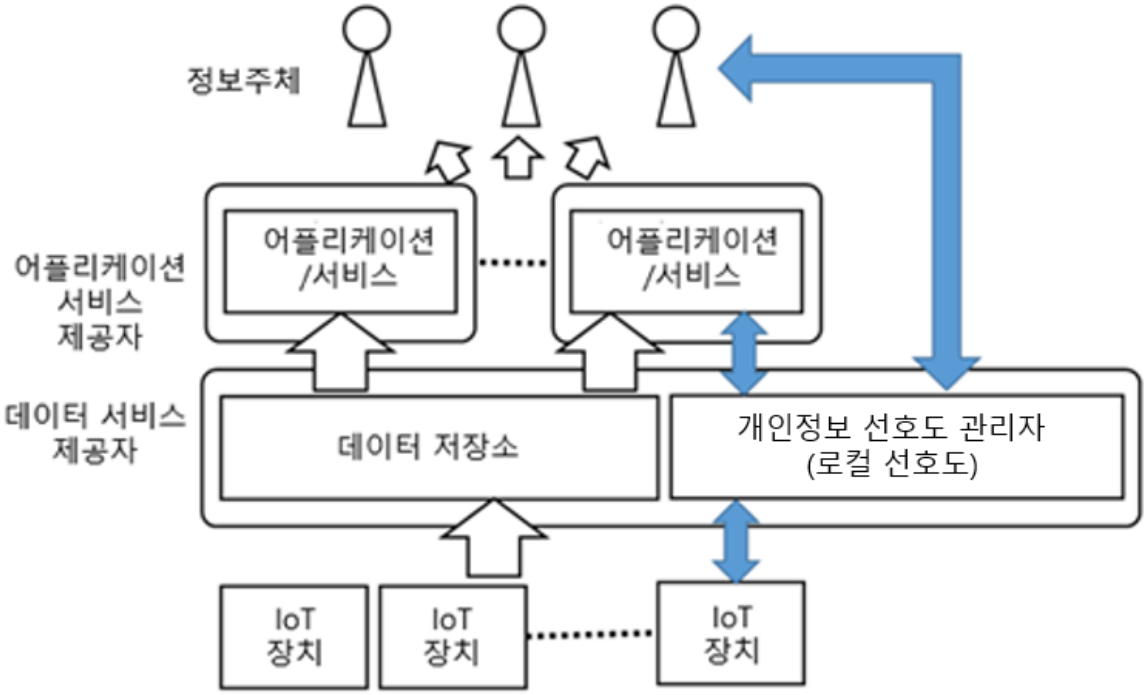


(그림 11-4) 다중 서비스 제공자에 의한 사물 인터넷 서비스 참조 모델

11.2.2 다중 서비스 제공자에 의한 개인정보 데이터 처리를 위한 기술 프레임워크

(그림 11-5)은 개인정보 선호도 관리자가 여러 서비스 제공자로 구성된 플랫폼에 포함되며 개인정보 데이터를 처리하기 위한 모든 사용자 선호도가 이 관리 구성요소에 의해 관리되는 기술 프레임 워크를 나타낸다. 사용자는 개인정보 선호도 관리자로 개인정보 선호도를 설정하고, 사물 인터넷 디바이스, 데이터 저장소, 응용/서비스와 같은 서비스 구성 요소는 개인정보 선호도 관리자의 로컬 개인정보 선호도에 기반해 개인정보

데이터를 처리한다.

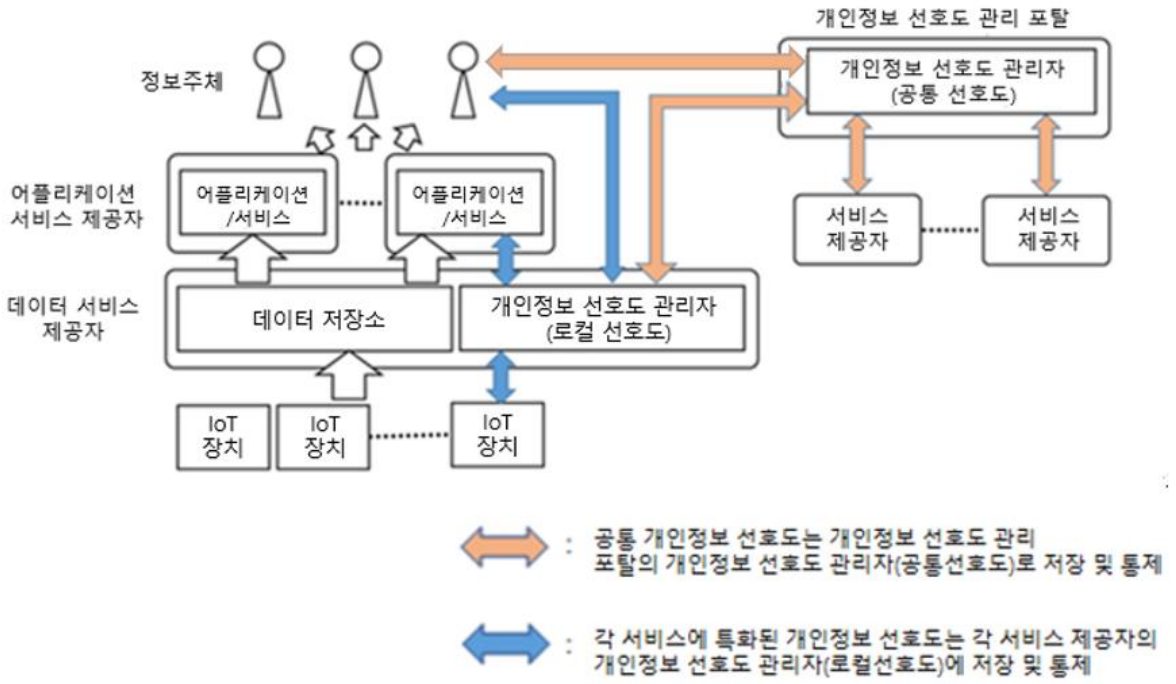


(그림 11-5) 다중 서비스 제공자에 의해 개인정보 데이터 처리 기술 프레임워크

11.2.3 공통 개인정보 선호도 관리 포탈 기반 개인정보 데이터 처리 기술 프레임워크

(그림 11-6)는 여러 서비스 제공자로 구성된 사물 인터넷 서비스 플랫폼이 개인정보 선호도 관리 포탈에 저장된 사용자 개인정보 선호도를 이용하는 기술 프레임 워크를 나타낸다.

이 경우 모든 서비스에 대한 공통 선호도가 개인정보 선호도 관리 포탈에 저장되며 각 서비스에 특화된 개인정보 선호도가 각 서비스 제공자가 관리하는 개인정보 선호도 관리자에 저장된다. 사용자가 서비스에 등록할 때, 서비스 제공자 시스템의 개인정보 선호도 관리자는 개인정보 선호도 관리 포탈에 있는 공통 개인정보 선호도를 조회한다. 사용자는 개인정보 선호도 관리자로 개인정보 선호도를 설정하지만, 개인정보 선호도 관리 포탈에 저장된 공통 개인정보 선호도는 여러 번 설정할 필요가 없다. 사물 인터넷 디바이스, 데이터 저장소, 응용/서비스와 같은 서비스 구성요소는 개인정보 선호도 관리자의 선호도에 근거해 개인정보 데이터를 제어한다.



(그림 11-6) 공통 개인정보 선호도 관리 포탈에 의한 개인정보 데이터 처리 기술 프레임 워크

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ISO/IEC 29151:2017, Information technology -- Security techniques - code of practice for the personally identifiable information protection

[2] ISO/TS 17975:2015, Health informatics -- Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2019.12.30	제정 TTAx.xx-xx.xxxx	-	개인정보보호/ID관리 및 블록체인보안 (PG502)