

ITU-T 국제표준 중심의 신뢰 서비스 프로비저닝 기술

최환석, 최준균, 이우섭*

ITU-T International Standard based Trust-enabled Service Provisioning Technology

Hoan-Suk Choi, Jun-Kyun Choi, Woo-Seop Rhee*

요약 ICT 기술의 발달로 데이터를 기반으로 하는 다양한 시스템과 서비스가 도입되면서 데이터, 인프라, 서비스에 대한 신뢰 제공 기술의 중요성이 대두되고 있다. 하지만 기존 ICT 서비스 환경은 특정 서비스를 구성하는 다양한 구성요소의 신뢰(콘텐츠, 인프라, 프로세스, 서비스 제공자 등)를 객관적으로 판단하고 관리할 방법이 없으며, 오로지 서비스 제공자의 자체적인 품질 기준에 의지해야만 하는 한계가 있다. 본 논문은 ITU-T 국제표준 관점의 신뢰성 있는 ICT 서비스 제공을 위한 요구사항, 기능구조, 처리절차를 제공한다. 신뢰할 수 있는 서비스 프로비저닝을 통해 기존 ICT 서비스 주체(서비스 자원, 이해관계자, 사용자)에 신뢰 제공을 위한 부가적인 기능을 추가하여, 관련정보를 수집하고, 분석하여 제공함으로써 사용자는 자신의 요구사항을 기반으로 분석된 신뢰를 기반으로 서비스 구성요소의 신뢰를 고려할 수 있다.

Abstract With the development of ICT technologies, various systems and services based on data have been introduced. Also, raising the importance of technologies that provide trust to a data, infrastructure, and services, for ICT services. However, in the existing ICT service environment, there is no way to objectively judge and manage the trust of various components (content, infrastructure, process, service provider, etc) that constitute a specific service, and there is a limitation that we can only rely on the service provider's own quality standards. This paper provides requirements, functional architecture, and procedures for providing reliable ICT services from the perspective of ITU-T international standards. Trust-enabled service provisioning adds additional functions for providing trust to existing ICT service entities (service resources, stakeholders, and users), collecting, analyzing, and providing trust related information. Therefore, a users can consider the trust of various service components based on analyzed trust information based on their trust requirements.

Key Words : Functional Architecture, International Standard, ITU-T, Trust, Trust Enabled Service, Trust Provisioning

1. 서론

인공지능(AI, Artificial intelligence)의 발달은 빅데이터, 로봇공학, 자율주행 시스템 등 신기술의 발전을 가속하여, 스마트 제조, 물류 등 산업계 전반에 걸쳐 상당한 영향을 미치고 있으며[1], AI Index 2023[2]에 따르면, 최근 5년간 패턴인식, 머신러닝, 컴

퓨터 비전, 알고리즘, 데이터 마이닝, 자연어 처리 등 다양한 연구 분야의 연구가 급증하고 있다[3].

지도학습을 기반으로 설계된 기존의 AI는 사람이 학습 규칙을 설정하고 데이터를 구축해야 하는 어려움을 가지고 있어, 번역 및 이미지 분류 등 특정 태스크에 특화된 개별적인 모델을 개발/운영해야 하는 특징

This work was supported by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2020-0-00833, A study on 5G based Intelligent IoT Trust Enabler)
 *Corresponding Author : Department of Intelligent Media Engineering, Hanbat National University (wsrhee@hanbat.ac.kr)
 Received November 27, 2023 Revised December 01, 2023 Accepted December 03, 2023

을 가지고 있다. 서비스에 필요한 지능 일부가 각각의 모델로 운영되어, 인간처럼 다양한 분야를 아우르는 범용성의 한계를 보여왔다[4].

이에 범용적으로 사용 가능한 범용 인공지능의 필요성이 대두되면서, 기존 AI 대비 모델의 파라미터 수와 학습 데이터셋 크기를 대폭 키운 초거대AI 개발 경쟁이 시작되었다. 특히 OpenAI[5]가 발표한 GPT-3는 전세대 대비 116배 커진 파라미터를 기반으로, 성능이 개선됨을 입증하였으며 뛰어난 언어 구사능력과 더불어 SW 코드, 기사 및 메일 작성 등 콘텐츠 생성 능력을 확인하였다. 특히 초거대AI 모델의 개발에는 방대한 학습 데이터와 이를 처리할 컴퓨팅 파워 및 관련 전문인력이 요구되어 막대한 비용을 감당할 수 있는 글로벌 빅테크 기업을 중심으로 개발이 진행되고 있다.

이러한 거대 AI 모델의 개발 특성상 공정성, 편향성, 윤리적 관점의 문제가 대두되고 있으며, AIAIC((AI, Algorithmic, and Automation Incidents and Controversies)는 AI를 기반으로 보고된 사고가 10년전 대비 26배 증가[3]하였음을 지적하고 있다. 또한 AI 모델이 생성한 결과물에 대한 정확성, 투명성, 최신성이 결여의 한계를 가지고 있다. 따라서 생성물에 대한 신뢰성 검증 및 관리(표질, 가짜뉴스, 성적, 인종적 편견 등)뿐만 아니라 훈련에 활용된 데이터의 신뢰성 관리가 시급한 실정이며[6], 우리나라는 이러한 상황을 감안하여, 생성형 AI 시대의 “디지털 국제 규범”을 마련하고, “대한민국 초거대AI 도약회의”에서 자율규제 관련 논의를 진행하고 있다[7].

국제 표준화 기구인 ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)는 일찍이 ICT 환경의 신뢰성 확보, 제어 및 관리의 중요성을 인식하고, 2016년 Trust Provisioning for future ICT infrastructures and services 기술문서 [8] 발행을 시작으로 ICT를 위한 신뢰 프로비저닝의 기본 원칙을 기술한 표준인 Y.3051[9], ICT 인프라 및 서비스 신뢰의 개념을 정의한 Y.3052[10], 신뢰 네트워킹을 위한 프레임워크를 정의한 Y.3053[11]을 포함한 다양한 신뢰 프로비저닝 및 제공 관련 표준안을 지속적으로 개발하고 있다.

본 논문의 2장에서는 신뢰의 개념과 ITU-T에서 개발한 신뢰 관련 표준 내용을 살펴보고, 3장에서는 23년 9월 승인된(Approved) Y.3058[12]을 기반으로 신뢰 제공을 위한 요구사항, 기능구조, 신뢰 제공 프로시저 등을 소개한다. 끝으로 개발 중인 신뢰 기능구조 표준을 비교 분석하며, 신뢰 제공 기술을 적용한 유즈 케이스를 제공하며, 결론을 맺는다.

2. 신뢰 개념 및 관련 표준

본 장에서는 신뢰의 개념과 대표적인 신뢰 관련 표준 내용을 소개한다. 사회학적 관점에서 신뢰란 모호성을 가지고 있는 타인이 장차 그러한 행동을 할 것이라는 주관적이고 확률적인 기대로 정의되고 있다[13]. 따라서 우리는 신뢰를 가진 타인과의 거래는 비 신뢰적인 타인과의 거래에 비해 위험 발생이 낮을 것으로 간주한다. 검색 시스템에서는 다양한 검색 결과 중 특정 대상을 선택하는 기준으로 활용할 수 있으며, 결과적으로 다양한 상호작용에서 판단의 기준으로 활용할 수 있다. 신뢰의 기술적인 활용을 위해서는 신뢰 정보를 수집하여 알맞은 신뢰 모델을 구축하고 이를 기반으로 용도 및 목적에 맞게 처리하는 기술이 요구된다.

표준화 기구인 ITU-T는 ICT 인프라 및 서비스를 위한 신뢰제공 개념을 정의한 Y.3052[10] 표준안을 통해 신뢰를 다음과 같이 정의한다. “Trust is the measurable belief and/or confidence which represents accumulated value from history and the expecting value for future.” 앞서 소개한 사회학적 관점과 유사하게 ICT 관점의 신뢰 개념 역시 ICT를 구성하고 있는 인프라 및 시스템에 의해 지속적으로 축적된 결과로써 그것을 이용하는 구성원 간에 형성되는 믿음, 확신의 개념으로 정의할 수 있다. 또한 신뢰는 양적, 질적으로 계산, 측정되는 특징을 가지고 있으며, 의사결정에 활용될 수 있다.

2.1 ITU-T SG13의 신뢰 관련 표준화 작업

ITU-T의 산하 그룹인 Study Group 13 (SG13)은 ICT 인프라와 미래 네트워크의 중요 키워드로 Trustworthy를 선정하고 지속적인 표준개발 작업을

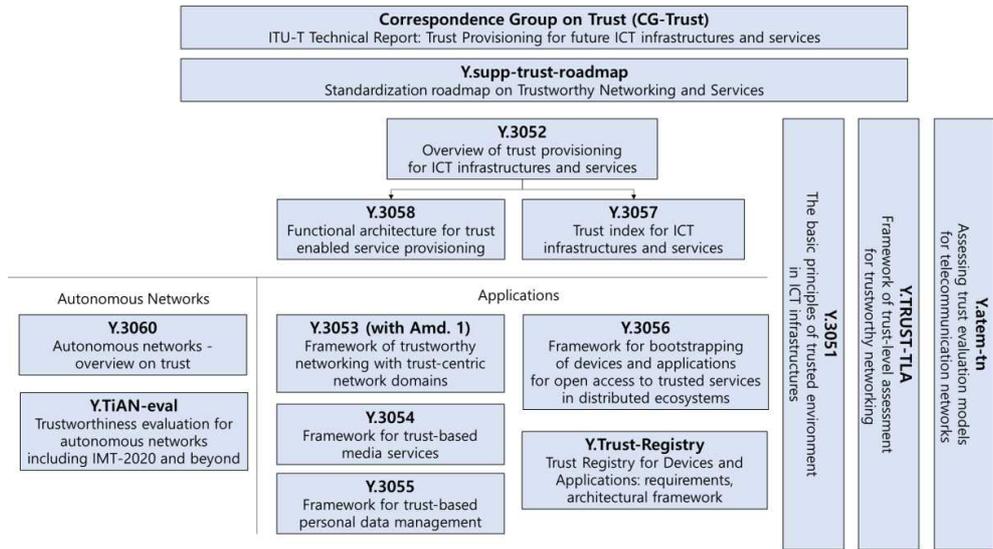


그림 1. ITU-T 신뢰 네트워킹 및 서비스 표준 로드맵
Fig. 1. ITU-T Trustworthy Networking and Services Standardization Roadmap

진행하고 있다. 그림 1은 Y.support.trust-roadmap : “Standardization roadmap on trustworthy networking and services”[14]의 개요로, 해당 문서는 ITU-T 관점의 신뢰 기술을 설명하고, 본 회기에 작업 중인 신뢰 네트워킹과 서비스를 소개하고 있다.

SG13은 Correspondence Group on Trust를 구성하여 미래 ICT 인프라에 대한 신뢰 프로비저닝 개념을 제공하고, ICT 관점의 신뢰의 중요성 및 주요 특징을 정의하였다. 또한 신뢰 제공을 위한 프레임워크를 제안하고, 미래 표준화 전략을 제시하는 기술문서[8]를 발간하였다. 이는 그림 1에서 보이는 바와 같이 모든 신뢰 관련 표준화 아이템의 기초가 되었으며, 이를 기반으로 Y.3052[10]를 개발하고, 기술문서의 내용을 확장하여, 신뢰의 개념, 중요성, 특징을 기술하고 이를 기반으로 신뢰 모델 및 신뢰 평가를 정의하였다. 또한 신뢰 프로비저닝 프로세스를 정의하여 신뢰 제공을 위한 필수적 구성요소를 정리하였다.

Y.3057[15]은 ICT 인프라 및 서비스를 위한 신뢰 지수 (Trust Index)를 개발하였다. 이는 특정 대상의 신뢰를 정량적으로 나타내는 여러 신뢰 지표를 결합한 개념으로, 대상의 신뢰를 수치화 하는 포괄적인

접근 방식을 정의하고 있다.

ITU-T는 이러한 Basis 표준을 기반으로 Y.3053 : 신뢰 네트워킹[11], Y.3054 : 신뢰 미디어 서비스[16], Y.3055 : 신뢰 기반 개인정보 관리[17], Y.3060 : 자율 네트워크[18] 등 다양한 분야에 신뢰 프로비저닝을 적용한 표준안을 지속적으로 개발하고 있다.

3. 신뢰할 수 있는 서비스 프로비저닝을 위한 기능구조

ITU-T Y.3058 “Functional architecture for trust enabled service provisioning” [12] 표준안은 ICT 서비스 인프라를 기반으로 제공되는 기존의 서비스에 신뢰성을 제공하기 위해 요구되는 기능구조를 정의하고 있다. 본 장에서는 신뢰 가능 서비스 프로비저닝의 개념과 요구사항, 기능구조, 주요 프로시저 등을 정의한다.

3.1 신뢰할 수 있는 서비스 프로비저닝 개요

Y.3058은 기존 ICT 서비스 주체(서비스 자원, 이해관계자, 사용자)에 신뢰 제공을 위한 부가적인 기능을 추가하여, 서비스의 품질과 사용자 경험이 향상된 신뢰

적인 서비스를 “Trust Enabled Service (신뢰 가능 서비스)”로 아래와 같이 정의하고 있다:

“Trust enabled service: a reliable service which satisfies service and trust requirements, by applying additional functions for trust provisioning capabilities to conventional ICT service entities (including resources, stakeholders, and users), that is able to develop better quality of services and experience.”

기존의 서비스 환경은 서비스 공급자가 특정 서비스 도메인에 존재하는 다수의 사용자에게 특정 기능이나 가치를 서비스의 형태로 제공한다. 이러한 환경에서 사용자는 자신이 사용하는 서비스가 포함하는 다양한 구성요소의 신뢰(콘텐츠의 신뢰, 서비스를 제공하는 시스템 및 네트워크와 같은 인프라의 신뢰, 서비스 제공 프로세스(로직)에 대한 신뢰, 서비스 제공자의 신뢰, 자원 소유자의 신뢰 등)를 객관적으로 판단하고 관리할 방법이 없으며, 오로지 서비스 제공자의 자체적인 품질 기준에 의해 관리된다.

따라서 신뢰할 수 있는 서비스는 그림 2와 같이 Trust Agent를 통해 신뢰를 제공할 대상의 신뢰 관련 정보를 수집하며, 수집된 정보를 기반으로 대상의 신뢰를 분석한다 (Trust Analysis & Management). 분석된 신뢰 정보는 서비스 제공자가 필요할 때 활용할 수 있도록 제공(Trust Enablement)되며, 서비스 사용자는 주관적, 객관적인 신뢰 요구사항에 따라 분석된 신뢰 정보를 기반으로 다양한 서비스 구성요소의 신뢰를 관리하고, 판단하여, 최종적으로 신뢰할 수 있는 서비스를 구성하고 사용자에게 제공한다.

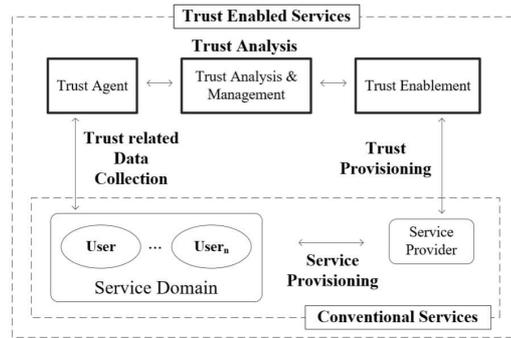


그림 2. 신뢰할 수 있는 서비스 프로비저닝 개념
Fig. 2. Concept of Trust-enabled Service Provisioning

3.2 신뢰할 수 있는 서비스 프로비저닝을 위한 요구사항

일반적으로 신뢰 서비스 제공을 위해서는 신뢰 분석을 위한 데이터 수집이 선행되어야 하며, 수집 데이터의 보안 요구사항, 및 개인정보 보호 관련하여 해당 사항을 규율하는 지역, 및 국가에 따라 적절한 규제가 필요하다. 지역적, 문화적, 특성상 데이터 수집에 대한 인식 및 환경이 매우 다양하여, 글로벌 표준의 도출은 어려운 실정이며, 이에 따라 국가별로 다양한 관점을 담은 규제가 설정되어 있다.

본 장에서는 신뢰할 수 있는 서비스 제공을 위한 기능구조 정의를 위해 3가지 관점(데이터 수집, 신뢰 분석 및 신뢰 프로비저닝)의 요구사항을 정리한다.

3.2.1 신뢰 관련 데이터 수집 요구사항

특정 대상의 신뢰 측정을 위해서는 대상과 직/간접적으로 관련이 있는 다양한 종류의 데이터를 수집할 필요가 있다. 본 절에서는 신뢰 관련 데이터 수집 과정의 요구사항을 정리한다.

- 데이터 수집 범위 : 대상의 신뢰는 특정 영역에 한정되어 형성될 뿐만 아니라, 대상이 활용 및 활동하는 모든 영역에 영향을 받는 속성을 가지고 있다. 따라서 신뢰 평가 대상인 자원 및 서비스 구성원(이해관계자)의 신뢰 관련 데이터 수집 범위는 특정 서비스 영역뿐만 아니라 해당 자원이 활용되고 서비스 이해관계자가 활동하는 모든 서비스 영역에서 신뢰 관련 데이

터를 수집할 필요가 있다.

- 상태 추적 : 서비스 구성요소(자원 및 서비스 이해관계자)의 가용성 관리를 위해서는 대상의 프로필 및 상태를 지속해서 수집해야 한다.

- 개인 식별 정보 수집 : 프라이버시 보호를 위해 PII(Personal Identifiable Information) 정보를 요청하지 않고 저장하지 않아야 한다.

- 수집 데이터 전처리 : 수집된 신뢰 데이터를 정제하기 위해 데이터 필터링 및/또는 전처리가 요구될 수 있다. 또한 서로 다른 서비스 도메인에서 수집된 이기종 데이터의 의미적, 형태적 변환을 제공해야 한다.

3.2.2 신뢰 분석 요구사항

신뢰는 주관적, 객관적인 다양한 요소로 구성되며 활용 목적, 활용 범위, 대상에 따라 다양한 분석 방법이 있을 수 있다[15]. 본 장에서는 신뢰 분석을 위한 요구사항을 정리한다.

- 신뢰 관계 표현 : 신뢰를 형성하는 모든 이해관계자가 신뢰자(trustor)와 피신뢰자(trustee) 역할을 할 수 있으며, 신뢰 모델은 양방향 관계 (Bi- Directional Relationship) 표현을 지원해야 한다.

- 다양한 신뢰 모델 지원 : 대상의 관계를 포함하여 서로 다른 서비스 도메인의 자원 및 이해관계자에 대한 신뢰 관련 데이터 처리가 요구되며, 서비스 도메인이나, 대상 애플리케이션, 이해관계자에 따라 다양한 신뢰 모델이 활용될 수 있어야 한다.

- 신뢰 속성 : [8] 및 [10] 은 신뢰를 구성하는 속성(Trust attribute)의 다양한 특징(주관적 특성, 변동 가능성 등)을 설명하고 있으며, 이러한 특징을 고려하여 처리되어야 한다.

- 멀티 도메인 : 신뢰 분석 및 관리를 위해 다양한 서비스 도메인의 접근성을 확보해야 한다.

- 사용성 고려 : 신뢰 분석을 위해 자원 및 서비스 이해관계자의 사용성 데이터 (예: 활동 및 활용 기록)를 고려해야 한다.

- 신뢰 모델 확장성 : 대상의 신뢰를 표현하는 신뢰 모델은 지속적으로 변경될 가능성이 있으므로, 신뢰 분석에 필요한 추가 정보를 포함할 수 있도록 확장성을 제공할 수 있게 설계되어야 한다.

- 신뢰 평가 방법 : 신뢰를 구성하는 특성(Trust Attribute)이 다양하고, 서비스나 애플리케이션의 목적 및 상황에 따라 특정 신뢰 특성을 평가하는 방법이 다를 수 있으므로, 대상의 신뢰 평가는 다양한 방법 (Metric)을 지원해야 한다.

- 신뢰 측정 단위 : 신뢰 측정 결과의 원활한 활용을 위해 신뢰 측정 결과를 실수로 표현하는 신뢰 양자화 (Quantization)를 지원해야 하며, 지속적인 신뢰 계산 수행을 위해 신뢰 계산 및 신뢰 처리 과정의 데이터를 보관할 필요가 있다.

3.2.3 신뢰 프로비저닝 요구사항

분석/측정된 신뢰는 목적에 따라 적절히 제공되고 활용되어야 한다. 본 장에서는 신뢰 프로비저닝을 위한 요구사항을 정리한다.

- 피드백 적용 : 신뢰 프로비저닝 결과에 대한 대상 (Trustor, Trustee)의 피드백을 수집하여, 추후 신뢰 측정 결과 개선에 활용될 수 있도록 한다.

- 요구사항 분석 : 목적 및 상황에 따른 다양한 신뢰 측정을 수행하기 위해, 신뢰 측정 요구사항을 분석하고, 이를 기반으로 신뢰 속성을 추출해야 한다.

- 신뢰 기반 검색 : 신뢰 요구사항 분석 결과에 따라, 신뢰 조건을 만족하는 리소스 및 서비스 검색 및 추천을 제공해야 한다.

- 신뢰 기반 의사결정 : 신뢰 측정 결과 및 신뢰 기반 검색/추천에 따라 자원 선정, 요청 허용 등 신뢰 기반 의사결정을 제공할 필요가 있다.

- 신뢰 기반 계약관리 : 신뢰 측정 결과를 기반으로 특정 자원, 서비스의 제공을 합의하였다면, 위탁자와 수탁자 사이에 계약조건 및 이용정보를 저장 및 갱신하는 계약관리를 제공해야 한다.

- 사용 및 권한 제어 : 합의된 계약조건에 따라 대상의 인증을 수행하고, 사용성 및 권한을 제어(Usage, Admission and Access Control)해야 한다. 만약, 신뢰 관리 대상이 사용자의 신뢰 요구사항을 충족하지 못하면 자원 제공을 중단해야 한다.

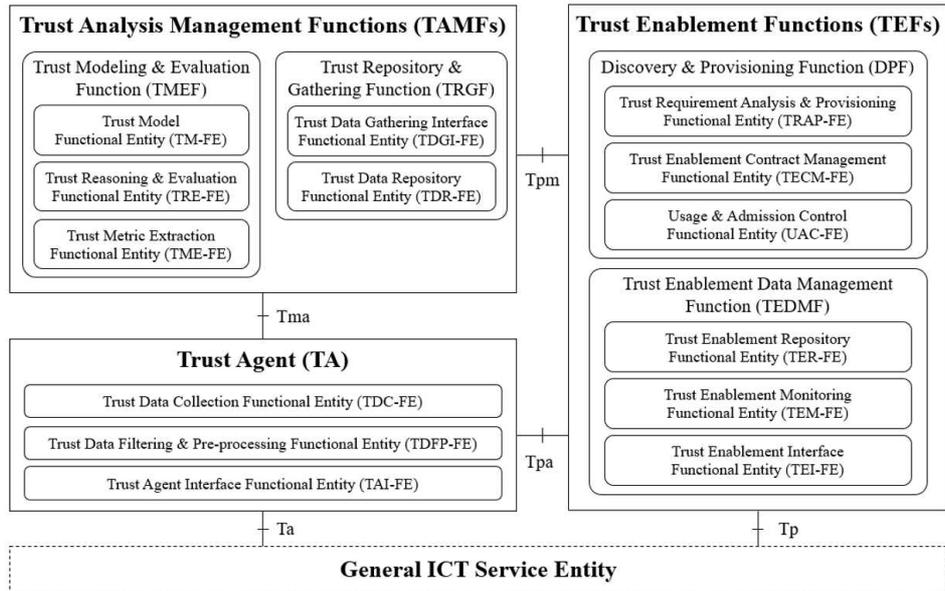


그림 3. 신뢰할 수 있는 서비스 프로비저닝을 위한 기능구조
 Fig. 3. Functional Architecture of Trust-enabled Service Provisioning

3.3 신뢰할 수 있는 서비스 프로비저닝을 위한 기능구조

그림 3은 Y.3058[12]에서 제안하는 신뢰할 수 있는 서비스 프로비저닝을 위한 기능구조이다. 이는 [8, 10, 16]에서 정의된 ICT 신뢰 프로비저닝 개념, 프레임워크 및 요구사항을 기반으로 설계되었으며, 신뢰 데이터 수집을 위한 TA (Trust Agent), 신뢰 측정을 위한 TAMF (Trust Analysis Management Functions) 그리고 신뢰 프로비저닝을 위한 TEF(Trust Enablement Functions)로 구성되고 세부 내용은 아래와 같다.

3.3.1 Trust Agent (TA)

TA는 인터페이스, Trust 데이터 수집, Trust 데이터 필터링 및 전처리를 통해 일반 ICT 서비스 대상의 신뢰 관련 데이터를 효과적으로 수집한다.

- TAI-FE (Trust Agent Interface Functional Entity) : 신뢰 관련 데이터 수집을 위해, 다양한 유형의 대상에 대한 연결을 제공하며, 기존의 플랫폼 및 장치에 연결하여 데이터 추출을 지원한다.

- TDC-FE (Trust Data Collection Functional

Entity) : 대상의 신뢰 수준을 평가하기 위해 요구되는 신뢰 관련 데이터를 수집하는 역할을 하며, 특정 서비스 도메인 관점에서 대상의 신뢰 수준을 평가하기 위해 일반 데이터 및 도메인 관련 데이터를 수집한다.

- TDFP-FE (Trust Data Filtering & Pre-processing Functional Entity) : 신뢰 평가를 위해 활용되지 않거나, 부정적 영향을 미칠 수 있는 데이터(중복, 관련없음, 민감 데이터 등)를 걸러내거나, 수집된 신뢰 데이터를 처리 용이한 형태로 변환한다.

3.3.2 TAMFs (Trust Analysis and Management Functions)

TAMFs는 TA를 통해 수집된 신뢰 데이터를 기반으로 대상의 신뢰도를 도출할 수 있도록 신뢰 모델을 제공하며, 이를 기반으로 추론을 수행한다. 또한 특정 요구사항을 분석하여, 대상의 신뢰를 분석하기 위한 신뢰 지표를 도출한다. TAMFs는 TMEF (Trust Modelling & Evaluation Function)과 TRGF (Trust Repository & Gathering Function)으로 구성된다.

- TMEF (Trust Modelling & Evaluation Function) : 대상의 신뢰 분석을 제공하고, 수집된 신

뢰 관련 정보를 신뢰 모델로 관리하며, 신뢰 평가 및 추론에 적합한 신뢰 지표(Trust Index) 추출 기능을 제공하며, 다음과 같이 3개의 기능 개체를 포함한다.

- TM-FE (The Trust Model Functional Entity) : CPS (Cyber-Physical Space)와 ICT 인프라를 표현하여, 특정 서비스를 위한 신뢰 관점의 환경을 정의할 수 있는 신뢰 모델을 제공한다. 신뢰 모델은 신뢰 데이터의 추론을 위해 대상 간의 신뢰 관계를 표현하며, 신뢰 분석에 필요한 부가적인 정보를 포함한다.

- TRE-FE (Trust Reasoning and Evaluation Functional Entity) : TM-FE가 제공하는 신뢰 모델을 기반으로 대상의 신뢰 수준을 분석 및 평가한다. 서비스 영역에 따라 다양한 유형의 추론 방법을 지원하며 특정 대상에 대한 적절한 추론 방법을 선정하여 대상의 신뢰 수준을 분석/평가한다.

- TME-FE (Trust Metric Extraction Functional Entity) : 3.2.2에서 설명한 바와 같이 신뢰 평가를 위해서는 서비스 요구사항에 맞는 신뢰 속성을 도출하고, 다양한 수치화 방법 중 알맞은 방법을 선택해야 한다. TME-FE는 요구되는 신뢰 특성을 도출하고, 신뢰에 영향을 미치는 요소를 고려하며 대상의 신뢰를 수치화 하고 계산방법(Trust Metric)을 결정한다.

- TRGF (Trust Repository & Gathering Function) : 수집된 데이터를 관리하기 위한 저장소 기능으로 아래 두 가지 기능 개체를 포함한다.

- TDGI-FE (Trust Data Gathering Interface Functional Entity) : 신뢰 분석을 위한 관련 데이터를 수집하기 위해 대상이 포함된 서비스 도메인을 담당하는 적절한 TA 및 TEFs와의 인터페이스를 제공한다.

- TDR-FE (Trust Data Repository Functional Entity) : 대상의 동작, 객체 간의 상호작용 등 이력 정보를 포함하는 신뢰 관련 데이터를 저장/관리한다.

3.3.3 TEFs (Trust Enablement Functions)

다양한 서비스 공급자로부터 수집된 데이터는 앞서 설명한 TAMFs에 의해 분석되며, TEFs는 신뢰 분석 결과를 필요로 하는 여러 서비스 제공자에게 서비스

구성요소 및 각종 자원에 대한 신뢰 분석 결과를 제공한다. 또한 요청받는 신뢰 요구사항을 기반으로 신뢰 자원의 추천, 검색을 수행한다. 특정 자원을 활용하는데 필요한 계약을 지원하며, 사용 제어를 제공하고, 만족도 데이터를 수집하여, 대상의 신뢰를 지속해서 갱신한다.

이렇게 지속적으로 변화하는 신뢰 관련 데이터 저장소를 관리하고 서비스 도메인 간에 도메인별 신뢰 지식을 공유 및 보급하기 위한 중개 기능을 제공한다. TEFs는 DPF(Discovery and Provisioning Function)와 TEDMF(Trust Enablement Data Management Function)로 구성된다.

- DPF (Discovery and Provisioning Functional Entity) : 신뢰 요구사항을 분석하고 적절한 형태로 자원의 정보를 제공하는 TRAP-FE (Trust Requirement Analysis & Provisioning Functional Entity), 선택된 구성요소(자원)를 활용하기 위해 대상 간 신뢰 자원 활용 계약을 제공하는 TECM-FE (Trust Enablement Contract Management Functional Entity (TECM-FE), 대상의 사용성 및 권한 제어를 담당하는 UAC-FE (Usage & Admission Control Functional Entity)의 하위 기능요소로 구성된다.

- TRAP-FE (Trust Requirement Analysis & Provisioning Functional Entity) : TRAP-FE는 서비스 환경 (예: 사용자 및 서비스 제공자)에서 요구되는 신뢰 요구사항을 분석하고 대상의 신뢰 분석을 위해 적합한 신뢰 속성을 추출한다. TA에 의해 수집된 신뢰 관련 데이터를 기반으로 TAMFs에게 대상의 신뢰 계산 결과를 요청하며, 전달받은 신뢰도를 통해, TRAP-FE는 필요한 신뢰 수준을 가진 적합한 자원 또는 서비스 목록을 생성하고, 이를 신뢰 대상을 요청한 신뢰 자원 요청자 및 서비스 제공자에게 제공한다. 또한 이전에 사용된 신뢰 수준과 유사/적합한 대상을 발견하는 경우, 사용자에게 신뢰 자원의 추천을 제공한다.

- TECM-FE (Trust Enablement Contract Management Functional Entity)는 신뢰 기반 서비스 참여자(신뢰 자원 제공자, 사용자) 간의 계약을 생성/관리하며, 이러한 계약 정보는 TEDMF (Trust

Enablement Data Management Functional)에 의해 저장된다.

- UAC-FE (Usage & Admission Control Functional Entity)는 사용 및 접근 제어 기능 수행하는 기능요소로, 신뢰 활성화 서비스 사용자 및 신뢰 자원 연결을 위한 인터페이스인 TEI-FE (Trust Enablement Interface Functional Entity)를 통해 서비스 제공자와 신뢰 자원 사용자의 접근을 제어한다. 또한 특정 자원의 사용성 제어(Usage Control)를 위해 신뢰자원 활용 계약에 명시된 TLA (Trust Level Agreement)에 따라 사용 권한을 부여하며, TLA는 인증된 사용자에 대한 허용 동작(Operation), 활용 범위 및 허용 시간을 정의한다.

- TEDMF (Trust Enablement Data Management Function) : 신뢰 계약 정보, 사용성 정보, 사용 후 만족도 정보 등 신뢰 자원 활용에 대한 관련 정보들을 저장 및 관리하는 기능으로, TER-FE (Trust Enablement Repository Functional Entity), TEM-FE (Trust Enablement Monitoring Functional Entity), TEI-FE (Trust Enablement Interface Functional Entity) 3가지 기능요소를 포함하고 있다.

- TER-FE (Trust Enablement Repository Functional Entity) : 신뢰 계약 정보, 사용성 정보 및 신뢰 자원 활용에 대한 만족도 정보 등 신뢰 자원 활용에 대한 관련 정보를 저장한다. 신뢰 계약 정보(Trust Enabled Contract Information)는 해당 계약의 참여자 정보와 대상 서비스를 구성하는 모든 신뢰 자원의 신뢰 요구사항 즉, TLA를 포함하고 있다. 사용성 정보(Usage Information)는 생성 시간, 접속 시간, 수정 시간, 자원 사용자 및 트랜잭션 유형과 같은 내역 정보를 포함하고 있으며, 만족도 정보는 해당 계약을 기반으로 한 서비스 경험에 대한 자원 제공자(Trustor 역할) 및 사용자(Trustee 역할)의 피드백 데이터이다. 서로 양방에 대한 만족도를 제공함으로써, 추후 신뢰 기반 서비스 품질 향상에 활용된다.

- TEM-FE (Trust Enablement Monitoring Functional Entity) : 신뢰 계약 정보, 사용성, 및 만

족도 정보와 같은 신뢰 자원 관련 정보를 실시간으로 수집하여 TER-FE에 저장한다.

- TEI-FE (Trust Enablement Interface Functional Entity) : TEF와 일반 ICT 서비스 구성요소 간 API(Application Programming Interface)를 제공하여 신뢰 관련 자원의 활용을 지원한다. TEI-FE는 TAMFs에게 신뢰 기반 서비스 참여자와 관련 신뢰 자원의 신뢰 관련 정보를 제공하며, 승인된 신뢰 기반 서비스 참여자(Trustor and Trustee) 간의 신뢰 관계 연결을 생성하도록 한다.

3.3.4 기능 구조간 레퍼런스 포인트

본 장에서는 그림 3에서 정의하고 있는 기능구조의 구성요소 간 연결을 지원하는 기능블록 간의 인터페이스를 정의한다.

- Reference Point Ta : Ta는 TA와 일반 ICT 서비스 구성요소 사이를 연결하며, TA가 일반 ICT 서비스 주체로부터 신뢰 가능 서비스 주체의 일반 및 신뢰 관련 정보를 수집하는 데 활용된다. TA는 Ta로 신뢰 관련 데이터 및 대상의 상태 데이터를 수집하여 대상을 모니터링하고, 새로운 대상이 검출 되었을 때, 해당 자원을 등록한다.

- Reference Point Tp : Tp는 TEF와 일반 ICT 서비스 구성요소를 연결하며, TEF가 사용자로부터 신뢰 가능 서비스 요청을 수신할 수 있으며, 신뢰 가능 서비스 목록 및 신뢰 계약 정보를 전달할 수 있다. 신뢰 가능 서비스 사용자는 Tp를 통해 특정 신뢰 기준을 만족하는 신뢰 서비스 구성요소에 대한 검색 요청을 TEF로 전송하며, TEF는 Tp를 통해 신뢰 가능 서비스 리스트, 신뢰 계약 정보 및 사용정보를 포함하는 응답을 제공할 수 있다. 신뢰 가능 서비스 사용자는 Tp를 통해 신뢰 자원 목록의 선택 결과를 TEF에 전달할 수 있으며, 선택한 서비스 또는 자원의 만족도 데이터가 포함된 작업 완료 메시지를 TEF에 전달하여 사용 및 신뢰 정보를 업데이트할 수 있다.

- Reference Point Tma : TAMFs는 Tma를 통해 TA에서 수집한 데이터를 수신할 수 있다. TA는 신뢰 지원 서비스 구성요소의 상태를 지속적으로 모니터링하고 수집된 정보를 TAMFs에 전송하여 신뢰 모델

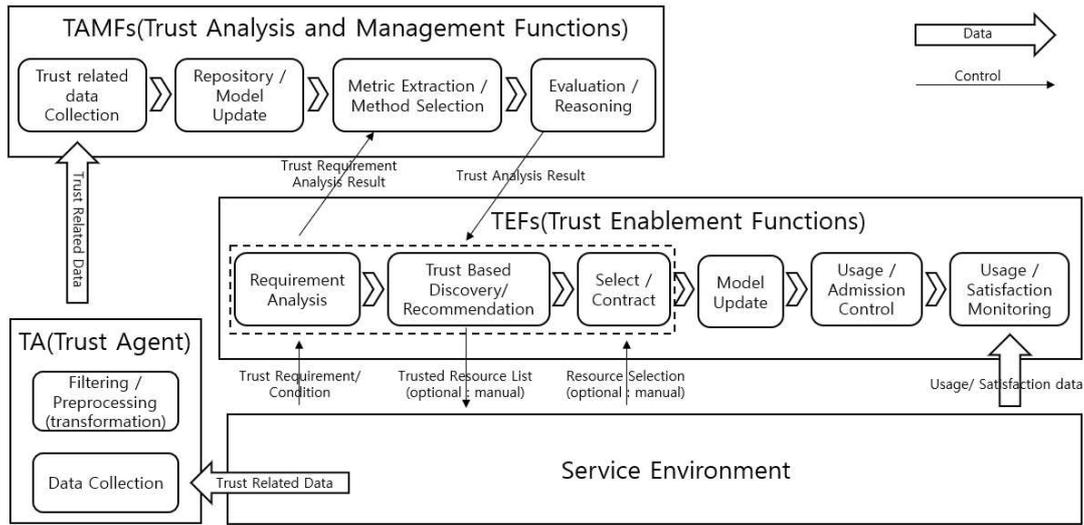


그림 4. 신뢰 프로비저닝 프로세스
Fig. 4. Trust Provisioning Process

을 업데이트하고 대상의 신뢰를 평가할 수 있도록 한다. TA는 특정 대상의 신뢰 평가 결과가 필요할 때 TAMFs로부터 Tma를 통해 평가 결과를 전달받는다.

- Reference Point Tpm : Tpm은 TAMFs와 TEFs 간에 통신을 가능하게 하는 인터페이스이다. TEFs는 Tpm을 통해 TAMFs에게 신규로 생성된 구성요소의 신뢰 관련 데이터를 보내 신뢰 모델에 대상을 등록하고, 신뢰 수준을 평가하도록 한다. TEFs는 해당 인터페이스를 통해 TAMFs로부터 신뢰 자원의 탐색 및 추천을 위한 신뢰 계산 결과를 수집한다. 신뢰 구성요소의 계약 정보, 사용성 정보와 같은 상태 변화에 따라 TEFs는 신뢰 관련 데이터를 Tpm을 통해 TAMFs에 전송하여, 신뢰 모델을 업데이트한다.

- Reference Point Tpa : Tpa는 TA와 TEFs 간 정보전달을 위한 인터페이스로, 새로운 구성요소 등록을 위해 TA로부터 수집된 신뢰 관련 데이터를 전달하며, TEFs의 TECM-FE는 신규 등록된 엔티티에 대한 신뢰 서비스 계약 및 사용모델을 작성한다.

3.4 신뢰할 수 있는 서비스 프로비저닝 프로시저

본 장에서는 그림 3의 기능구조를 바탕으로 구성요소 등록, 구성요소 요청 및 모니터링, 검색 및 추천과

같은 신뢰 서비스에서 요구되는 서비스 프로비저닝 프로시저를 제시한다. 그림 4는 신뢰 서비스 프로비저닝을 위한 전체 프로세스를 나타낸다. TA를 통해서 서비스 환경의 다양한 신뢰 관련 데이터가 수집되면, 신뢰 프로비저닝을 위해 TAMFs로 전송되며, 신뢰 모델에 반영된다. 신뢰 자원의 활용을 원하는 서비스 제공자는, TEFs에 신뢰 요구사항을 전달하며, 이를 분석한 TEFs는 TAMFs에 신뢰 요구사항 분석 결과를 전달한다. 이러한 요구사항을 바탕으로 TAMFs는 신뢰 측정을 위한 신뢰 요소 및 측정 방법을 도출하며 대상의 신뢰를 분석하여, 분석 결과를 TEFs에 제공한다. TEFs는 신뢰 분석 결과를 통해 특정 요구사항을 만족하는 신뢰 자원을 검색하거나, 추천하여 서비스 제공자가 신뢰 자원을 선택/활용하게 한다.

3.4.1 서비스 구성요소 등록 프로시저

신뢰 서비스를 제공하기 위해서는, 서비스를 구성하고 있는 시스템, 인프라, 콘텐츠, 데이터와 같은 자원 뿐만 아니라, 서비스 제공자, 서비스 사용자와 같은 모든 이해관계자의 신뢰 관리가 수행되어야 한다. 이를 위해 그림 5의 구성요소 등록 프로시저를 활용한다.

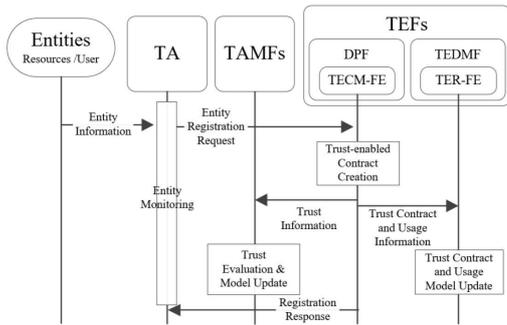


그림 5. 신뢰할 수 있는 서비스 엔티티 등록 절차
Fig. 5. Trust Enabled Entity Registration Procedure

- 1) TA는 자신이 담당하고 있는 범위 내에 신규 개체를 지속적으로 검색하며, 새로운 개체를 발견하면 해당 개체의 일반 정보 및 신뢰 관련 데이터를 포함한 등록 요청 메시지를 TEFs의 TECM-FE에 전송한다.
- 2) TECM-FE는 소유권, 허용기능, 이용 시간, 이용 이력, 대상 등의 권한을 명시한 신뢰 계약을 생성한다.
- 3) TECM-FE는 신규 대상에 대한 신뢰 모델 업데이트 및 신뢰 평가를 위해 신뢰 관련 데이터를 TAMFs에 전달한다.
- 4) TECM-FE는 신규 대상에 대한 신뢰 계약 및 사용성 모델 갱신을 위해 대상의 계약 정보 및 사용성 데이터를 TER-FE로 전송한다.
- 5) 신규 대상에 대한 신뢰 모델, 신뢰 계약 및 사용성 모델의 업데이트가 완료되면, 신뢰 서비스를 위한 등록이 완료된 것으로 TECM-FE는 등록 결과를 TA에 응답한다.

3.4.2 서비스 구성요소 요청 프로시저

신뢰 서비스를 구성하는 특정 자원을 사용하기 위해서는 개체의 상태를 지속적으로 모니터링 하여 대상의 가용 여부 및 신뢰 수준을 파악해야 한다. 그림 6은 이를 위한 프로시저를 제시한다.

- 1) TA는 자신이 담당하는 범위 내의 모든 개체 상태를 지속적으로 모니터링 한다.
- 2) 사용자 A는 특정 대상(자원 1)을 사용하기 위해 TEFs의 UAC-FE에 요청 메시지를 보낸다.
- 3) TEFs의 UAC-FE는 요청된 대상에 대한 권한과

사용성 조건을 확인한다.

4) 사용자 A가 허용되는 경우, UAC-FE는 사용자 A에게 요청된 자원의 액세스 포인트 및 사용 프로파일을 포함한 자원의 상세 정보 및 계약 정보를 전송하고, 허용 메시지를 수신한 사용자 A는 계약 정보를 확인하고, 자원 1을 활용하는 작업(Task)을 수행한다.

5) UAC-FE는 리소스 A에 대한 사용성 정보(허용 대상, 기간, 허용 동작 등)를 TER-FE로 전송하여 사용성 모델을 업데이트 한다.

6) 대상(자원 1)의 상태가 변경되면 TA는 신뢰 평가 및 신뢰 모델 갱신을 위해, 변경된 대상의 상태를 포함한 신뢰 상태 업데이트 메시지를 TAMFs에 전송한다.

7) 자원1을 기반으로 수행하는 작업이 완료되면, 사용자 A는 UAC-FE에 대상(자원 1) 활용에 대한 만족도 데이터를 포함하여 작업 완료를 통보하고, UAC-FE는 변경된 상태를 기반으로 사용성 모델을 갱신한다.

8) UAC-FE는 사용자가 전달한 신뢰 자원 활용 만족도 데이터와 더불어, 신뢰 자원을 활용한 사용자A에 대한 평가를 포함한 만족도 데이터를 TAMFs에 전달하며, 이를 기반으로 신뢰 모델이 갱신된다.

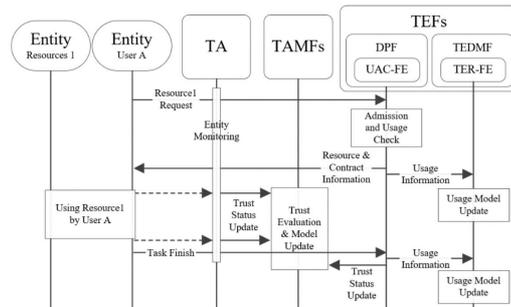


그림 6. 신뢰할 수 있는 서비스 엔티티 요청 절차
Fig. 6. Trust Enabled Entity Request Procedure

3.4.3 서비스 구성요소 검색 프로시저

신뢰 서비스 제공자(신뢰 자원 사용자)는 자신이 원하는 신뢰 요구사항을 충족하는 자원을 활용하여 신뢰 서비스를 구성할 수 있으며, 이때 그림 7과 같은 요구사항 기반의 신뢰 구성요소 검색 프로시저가 수행된다.

1) 사용자 A는 TEFs의 TRAP-FE에게 신뢰 프로파일을 포함한 신뢰 자원 요청 메시지를 전달하여, 신뢰 요구사항을 충족하는 자원을 요청한다. 신뢰 프로파일

은 구성요소의 유형, 신뢰 수준, 사용성 범위 등의 요구 사항을 정의한다.

2) TRAP-FE는 TAMFs가 계산한 대상의 신뢰 평가 정보를 수집하고, TER-FE의 신뢰 계약 정보 및 사용성 정보를 종합하여, 사용자가 요청한 신뢰 프로파일에 부합하는 대상(자원)의 리스트를 생성 및 제공한다.

3) 신뢰 자원 요청자(사용자 A)는 TRAP-FE가 전달한 리스트에서 특정 대상을 선택하고, 3.4.2에서 설명한 신뢰 가능 구성요소 요청 프로시저를 수행한다.

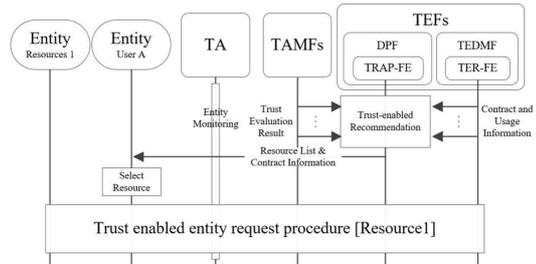


Figure 6 - Trust enabled entity recommendation procedure.

그림 8. 신뢰할 수 있는 서비스 엔티티 추천 절차

Fig. 8. Trust Enabled Entity Recommendation Procedure

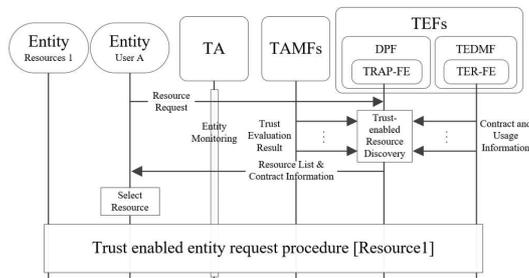


그림 7. 신뢰할 수 있는 서비스 엔티티 검색 절차

Fig. 7. Trust Enabled Entity Discovery Procedure

3.4.4 서비스 구성요소 추천 프로시저

TEFs는 특정 신뢰 요구사항에 부합하는 구성요소(자원 또는 서비스)를 추천할 수 있다. 이를 위해서 TRAP-FE는 신뢰 자원 요청자들의 과거 요구사항 정보(자원 요청자의 요청 메시지, 구성요소 선택 및 활용 후 만족도 데이터 등)를 수집하며, 세부 절차는 그림 8과 같다.

1) TRAP-FE는 신뢰 구성요소 추천을 위해 지속적으로 신뢰 자원 요청정보, 신뢰 계약 정보, 사용성 정보 및 상태정보, 신뢰 측정 정보를 수집함

2) 집계된 신뢰 관련 정보를 바탕으로 TRAP-FE는 1)에서 수집한 정보를 바탕으로 신뢰 요구사항을 만족하는 추천 목록을 작성하며 특정 신뢰 자원을 지속적으로 활용하는 신뢰 자원 요청자에게 전송된다.

3) 추천 목록을 수신한 신뢰 자원 요청자(사용자 A)는 자신이 필요한 대상을 목록 안에서 선택하고, 3.4.2에서 소개한 신뢰 가능 구성요소 요청 프로시저를 통해 적합한 신뢰 자원을 활용할 수 있다.

4. 신뢰 서비스 관련 기능구조 분석

본 장에서는 신뢰 프로비저닝의 기능구조를 다루고 있는 신뢰 프로비저닝 기술문서(TR)[8], 신뢰적 네트워킹 프레임워크 표준 Y.3053[11], 신뢰 기반 미디어 서비스 프레임워크 표준 Y.3054[16], 신뢰 기반 개인 데이터 플랫폼을 위한 Y.3055[17]와 신뢰할 수 있는 서비스 기능구조 표준 Y.3058[12]을 분석하였다.

분석을 위해, Y.3058[18]에서 도출한 기능구조를 기반으로 TA, TAMFs, TEFs의 하위 기능 엔티티와 타 기고서에 정의된 유사 기능을 구분하였다.

표 1은 신뢰 관련 데이터의 수집, 전처리 및 인터페이스를 제공하는 TA의 기능들을 비교한 것으로 대부분 [8]의 기능구조와 대치된다.

표 2는 수집된 신뢰 데이터를 저장하고, 대상의 신뢰를 측정하는 기능을 제공하는 TAMFs의 기능을 분석한 결과로, 신뢰 모델, 신뢰 추론 및 측정, 신뢰 메트릭 추출, 저장소, 인터페이스로 구성된다.

표 1. Trust Agent 기능 비교
Table 1. Functional Comparison of Trust Agent

TR[8]	Y.3053[11]	Y.3054[16]	Y.3055[17]	Y.3058[12]
TA interface		Trust data adapters		TA interface
Trust data collection	Trust verification support FE	Trust relevant media data collector, Trust relevant external data collector		Trust data collection
Trust data filtering and preprocessing		Trust data Filter and preprocessor		Trust data filtering and pre-processing

표 2. TAMFs 기능 비교
Table 2. Functional Comparison of TAMFs

TR[8]	Y.3053[11]	Y.3054[16]	Y.3055[17]	Y.3058[12]
Trust models		Trust models	Trust modelling function	Trust models
Trust reasoner and evaluator	Trust level validation FE	Trust reasoner, Trust attributes evaluator	Trust information analysis function	Trust reasoning and evaluation
Data analytics				
Trust metric extractor		Trust metric extractor, Trust index analysis engine, Trust indicators identification		Trust metric extraction
Trust knowledge gathering Interface		Trust data gathering interface	Trust attributes monitoring function	Trust data gathering interface
Trust data repository		Trust data repository		Trust data repository

표 3은 신뢰 서비스 요청 및 신뢰 프로비저닝을 담당하는 TEFs의 기능 분석 결과로 기술문서[8]의 TSE(Trust Service Enabler)와 TSB(Trust Service Broker)를 포함하며, 신뢰 요소의 ID 관리기능, 신뢰 정보의 생애주기 관리, 신뢰 기반의 추천 및 탐색 기능 등으로 구성된다. 또한 각 권고안의 목적에 따른 추가 기능이 존재한다.

표 3. TEFs 기능 비교
Table 3. Functional Comparison of TEFs

TR[8]	Y.3053[11]	Y.3054[16]	Y.3055[17]	Y.3058[12]
	Trust information lifecycle management FE	Trust information OAM	Trust information lifecycle management function	Usage and Admission control
Trust idM	ID-locator mapping support FE, Trust linker	Trust idM, Trust APIs, Trust linking		Trust enablement interface
Trust based recommendation				Trust requirement analysis & provisioning
	Domain membership management FE, Domain policy management FE		Privacy compliance management functions,	Trust enablement contract management
				Trust enablement repository
				Trust enablement monitoring

5. 신뢰 프로비저닝 적용 시나리오

본 장에서는 신뢰 프로비저닝을 적용한 활용 시나리오를 설명한다. 그림 9는 신뢰 프로비저닝 기반의 전력 보조 시스템 개념을 보여준다. 전력 보조사업자는 전력의 안정적인 공급을 위해 전력 시스템을 관리하는 기업 중 하나로, 전력 소비량에 따라 메인 전력 시스템에서 요구되는 전력을 공급한다.

참여자는 전력 소비자, 일반적으로 사용하는 전력량에 비해 절감 가능한 전력량을 고지하고, 통제가 가능한 전력 자원 정보를 전달하며, 전력 서비스 제공자가 제시한 정보(예: 인센티브, 비용, 감축량 등)를 바탕으로 전력 소비 조절을 결정한다.

시스템 운영자는 전력 계통 전체를 조직하고 관리하는 사람으로 발전기로부터 발전정보를 전달받아 전력 절감량을 결정하고 보조사업자에게 전력의 안정성과 신뢰성을 유지하도록 요청한다.

TA는 신뢰 지수 산출에 활용 가능한 전력 서비스 참여자의 사용량, 감축량 등 실시간 상태정보와 전력

보조 서비스 참여 이력을 수집한다. 신뢰 분석 플랫폼은 수집된 정보를 기반으로 참여자의 신뢰를 산출한다. 전력 보조 사업자는 통제 가능한 전력 자원의 비중, 거래기록, 참여자의 신뢰도를 고려하여 적절한 시장참여자를 선택한다.

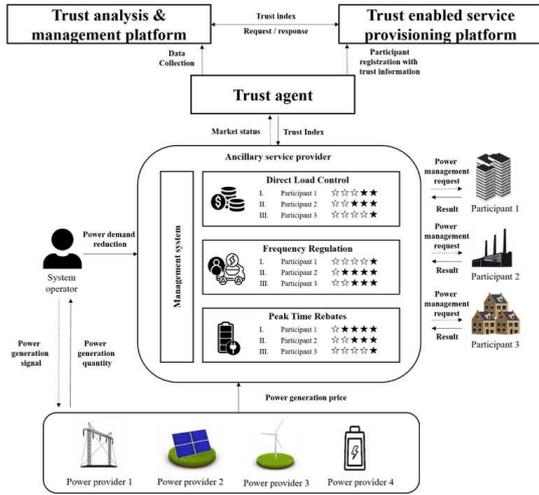


그림 9. 전력시스템 보조 서비스
Fig. 9. Ancillary Service in Power System

6. 결론

사회학적 관점에서 신뢰란 모호성을 가지고 있는 타인이 특정 행동을 할 것이라는 주관적임, 확률적인 기대로 정의된다. 신뢰가 보장되면 교류와 협력, 효율성을 증진하며, 이해충돌 비용이 감소하여 결과적으로 대상의 가치가 상승하는 효과가 나타난다[19].

ICT 기술의 발달로 데이터를 기반으로 하는 다양한 시스템과 서비스가 도입되면서 데이터, 인프라, 서비스에 대한 신뢰 제공 기술의 중요성이 대두되고 있다.

하지만 기존 ICT 서비스 환경은 특정 서비스를 구성하는 다양한 요소의 신뢰(콘텐츠의 신뢰, 서비스를 제공하는 시스템 및 네트워크와 같은 인프라의 신뢰, 서비스 제공 프로세스(로직)에 대한 신뢰, 서비스 제공자의 신뢰, 자원 소유자의 신뢰 등)를 객관적으로 판단하고 관리할 방법이 없으며, 오로지 서비스 제공자의 자체적인 품질 기준에 의지해야만 하는 한계가 있다.

국제 표준화 기구인 ITU-T는 2015년부터 ICT 환경의 신뢰성 확보, 제어 및 관리의 중요성을 인지하고 관련 기술문서 및 표준안을 지속적으로 개발하고 있다.

본 논문은 신뢰의 개념과 ITU-T에서 개발한 신뢰 관련 표준안의 내용을 살펴보고 ITU 관점의 신뢰성 있는 ICT 서비스 제공을 위한 요구사항, 기능구조, 처리 절차를 소개하였다.

제안된 신뢰할 수 있는 서비스 프로비저닝은 기존 ICT 서비스 주체(서비스 자원, 이해관계자, 사용자)에 신뢰 제공을 위한 추가적인 기능을 추가하여, 신뢰정보를 수집하고, 분석하여 제공함으로써 사용자는 자신의 신뢰 요구사항을 기반으로 분석된 신뢰 정보를 기반으로 다양한 서비스 구성요소의 신뢰를 고려할 수 있다. 신뢰 프로비저닝을 위한 기능을 추가로 구성하는 형태로 설계되어, 기존 인프라나 시스템 안정성에 영향을 미치지 않고, 신뢰 기반 서비스가 가능하며, 특히 고품질의 ICT 인프라 보유가 어려운 저개발 국가의 인프라 시스템에 적용시 비용 효율적인 방법으로 신뢰 서비스를 제공할 수 있을 것으로 생각된다.

REFERENCES

- [1] K.W. Kook, "ChatGPT and the Large AI tech trends," *KOSEN REPORT 2023.1069*, April, 2023.
- [2] Institute for Human-Centered AI, "THE AI INDEX REPORT, Measuring trends in Artificial Intelligence," *Stanford University*, [Internet]. Available: <https://aiindex.stanford.edu/report>
- [3] S. W. Ahn, Y. M. Lim, J. H. Yoo, J. M. Kim, M. S. Ahn, J. C. Jang, K. H. Bong, J. W. No, B. R. Oh, "Summary and Implications of 2023 AI Index Report," *SPRI Issue Report IS-159*, May, 2023.
- [4] H. J. Lim, "The evolution of Hyper scale AI and the challenges," *IITP ICT SPOT ISSUE 2022-14*, Dec. 2022.
- [5] OpenAI, [Internet]. Available: <https://openai.com>
- [6] S. W. Ann, J. H. Yoo, W. Y. Jo, J. W. No, H. H. Son, "Rise of Hyper-scale LLM(Large Language Model) and issues," *SPRI Issue*

Report IS-158, Feb. 2023.

[7] S. Y. Lee, "Fake News in the Age of Generative AI..What's the Solutions?," *MTN news*, [Internet]. Available: <https://news.mtn.co.kr/news-detail/2023091910484826429>

[8] ITU-T Technical Report, "Trust provisioning for future ICT infrastructures and services," April 2016.

[9] ITU-T Recommendations, "Y. 3051 : The basic principles of trusted environment in information and communication technology infrastructure," March, 2017.

[10] ITU-T Recommendations, "Y.3052 : Overview of trust provisioning for information and communication technology infrastructures and services," March, 2017.

[11] ITU-T Recommendations, "Y.3053 : Framework of trustworthy networking with trust-centric network domains," Jan. 2018.

[12] ITU-T Recommendations, "Y.3058 : Functional architecture for trust enabled service provisioning," July, 2023.

[13] W. Sherchan, S. Nepal, C. Paris, "A survey of trust in social networks," *ACM Computing Surveys*, vol. 45, Aug. 2013.

[14] ITU-T Draft Recommendation TD410, "Y.supp.trust-roadmap: Standardization roadmap on trustworthy networking and services," July, 2023.

[15] ITU-T Recommendations, "Y.3057 : A trust index model for information and communication technology infrastructures and services," Dec. 2021.

[16] ITU-T Recommendations, "Y.3054 : Framework for trust-based media services," May, 2018.

[17] ITU-T Recommendations, "Y.3055 : Framework for trust-based personal data management," Sep. 2020.

[18] ITU-T Recommendations, "Y.3060 : Autonomous networks - overview on trust," Sep. 2023.

[19] K. J. Kim, "[Expert Column] Trust and the Cost of Crumbling Social Capital," *Ajunews*, [Internet]. Available : <https://www.ajunews.com/view/2023082408424>

6883

저자약력

최 환 석 (Hoan-Suk Choi)

[정회원]



- 2018년 : 국립한밭대학교 멀티미디어공학과 공학박사
- 2015년-현재 : 한국 ITU 연구위원회 국제표준전문가
- 2018년-2020년: 한밭대학교 멀티미디어공학과 박사후연구원
- 2020년-2021년 : 한국과학기술원 전기및전자공학부 위촉연구원
- 2021년: (주)토브데이터 매니저
- 2021년-현재 : KAIST-메가존클라우드 지능형 클라우드 융합기술 연구센터 매니저

〈관심분야〉 IoT, Social IoT, Semantic Processing, Trust management, Trust Chain, 개인정보보호, GDPR, Cloud Computing, AGI, 스마트 제조

최 준 균 (Jun-Kyun Choi)

[정회원]



- 1998년 : 한국과학기술원 전자공학박사
- 1997년 : 한국전자통신연구원 책임연구원
- 2009년-현재: 한국과학기술원전기 및전자공학부 정교수

〈관심분야〉 사물인터넷, 웹, 신뢰네트워크, 에너지

이 우 섭 (Woo-Seop Rhee)

[정회원]



- 2003년 : 충남대학교 공학박사
- 1983년-2005년: 한국전자통신연구원 팀장/책임연구원
- 2005년-현재: 국립한밭대학교 지능미디어공학과 교수
- 2006년-현재: 한국 ITU 연구위원회 국제표준전문가
- 2012년-2013년: Institute TelecomSudParis 방문교수
- 2018년-2019년: Liverpool John Moores University 방문교수

〈관심분야〉 Semantic Processing, Trust Management, Trust chain, IoT, Social IoT