KISTI
ISSUE BRIEF

ISSN 2635-5728

과학기술인프라, **데이터로 세상을 바꾸다**

https://doi.org/10.22810/2022KIB050

2022. 12. 12. **제50호**

신뢰 및 신원 관리 기술의 동향: 연구·교육 분야를 중심으로

조진용 · 김승해 · 조부승

2010년대 초반부터 세계 각국 정부는 안전한 사이버 인프라 구축을 위한 국가 전략을 수립해 실천하고 있다. 신뢰 및 신원(Trust and Identity) 인프라는 전략 실현을 위한 핵심 정책프레임워크로써 행정기관은 물론 학·연 분야까지 광범위하게 구축되고 있으며 국가연구망, 데이터 플랫폼, 고성능 컴퓨팅과 함께 핵심 국가 연구 인프라로 인식되고 있다. 특히 개인정보보호에 대한 규제강화, 데이터의 개방성 확대 요구 증가, 과학적 난제해결을 위한 e-인프라의 융합활용 환경 조성, 클라우드 산업 육성을 위한 각국 정부의 의지 반영 등의 이유로 신뢰 및 신원관리 인프라의 중요성이 더욱 증가하고 있다.

이에 본고에서는 신뢰 및 신원관리 체계의 필요성과 학·연 분야에서 활용 중인 신원 모델의 종류 및 기술의 진화 방향에 대해 논하고 적용 사례 등 국제 동향을 살펴보고자 한다. 또한, 산·학·연·관 간 상호 협력과 거버넌스 체계 구성이 필수적으로 요구되는 신뢰 및 신원 인프라의 기술 및 체계 확보 방안과 활용확산 전략에 대해 제언하고자 한다.

CONTENTS

1. 신원 관리의 체계화 필요성

데이터 보호 강화

- **(보안 위협의 대응) 데이터 유출 사고의 81%가 신원증빙 수단의 불법적·탈법적 사용으로 인해 발생(Verizon, 2021)하는 등 사이버 공간의 보안사고 방지와 사생활보호를 위해 신뢰 및 신원(Trust and Identity, 이하 신뢰관리) 인프라의 구축 필요**

  - 미국 정부는 사이버공간의 신뢰관리를 위한 국가전략을 수립(The White House, 2011)하고 신뢰관리 인프라의 구축과 신원증명을 위한 기준을 제시

  - 미국 국립표준기술연구소(NIST)의 신뢰기반 신원연구그룹은 디지털 신원관리 지침 등 안전한 사이버공간 구현을 위한 정책프레임워크를 개발해 가이드라인(NIST 800-63C)으로 제공

  - 미국은 국립과학재단(NFS)의 Campus Cyberinfrastructure 및 Cybersecurity와 Advanced Cyberinfrastructure 사업을 통해 TIPPSS(Trust, Identity, Privacy, Protection, Safety, Security)를 포함하는 자국 내 사이버 인프라 고도화에 지속적 투자

  - 유럽연합은 유럽 단일 시장 내에서 전자거래에 대한 신뢰관리를 위해 eIDAS (eIDAS, 2014)를 제정했으며 개정안(M. Negreiro, 2022)에서는 '유럽 디지털 신원 프레임워크' 구축을 계획하는 등 유럽연합 내 통합 디지털 신원관리 체계 구축을 위해 노력

  - 유럽연합이 EU 공동연구개발프로그램(FP)과 Horizon 연구혁신프로그램을 통해 REFEDS, FIDAS, PRIME, AARC 등 다수의 신뢰관리 관련 연구개발 사업들을 지원한 결과, 유럽연합 내 학·연 분야에서 신뢰관리 체계가 확고히 정착

  - 우리나라는 신뢰관리 체계의 일부가 행정 분야에서 제한적으로 보급(행안부규격, 2017)되었으나 정책 프레임워크의 구성이 미비하거나 파편적으로 적용되고 있어 국가적 차원의 프레임워크 표준화와 활성화 노력 필요

온라인 소프트웨어 산업 지원

- **(산업체의 플레이그라운드) 복합 연평균 성장률이 24.7%로 예측(Verified, 2022)되는 학·연 분야 클라우드 컴퓨팅 시장의 활성화를 위해 신뢰관리 인프라를 육성함으로써 온라인 소프트웨어 산업체의 시장진입을 위한 플레이그라운드로 활용 필요**

  - 인증과 권한부여의 분리, 비밀번호 데이터베이스의 복제활용 금지, 표준 준수, 신뢰 관리 인프라의 활용, 신원 사일로(Silo)[1]의 방지 등은 클라우드 환경의 보안강화를 위한 모범적인 관행으로 인식(N. Sargent, 2012)

1) 특정 디지털 서비스에 로그인하기 위해 설계된 폐쇄형 신원 저장소

- 미국 사이버보안 및 인프라 보안국(CISA)은 클라우드 보안강화을 위한 행정분야 보안 참조 아키텍처로 SAML/OIDC[2] 표준 기반의 신뢰관리 인프라를 적시(CISA, 2022)
- 미국의 신원연합(Identity federation)[3]인 InCommon은 200여 클라우드 산업체와 파트너십 체결을 통해 4,000여 상용 서비스제공자(Service Provider, SP)를 자국 내 학·연 기관에 공급, 클라우드 산업체의 시장 진입과 활성화를 위한 플레이그라운드로 작동
- 국내 클라우드 컴퓨팅 발전법은 클라우드 서비스 간에 상호 운용성 확보를 권고하고 있으며 한국정보통신기술협회(TTA)도 상호 운용성 확보를 위해 표준기반의 신뢰관리 기술 이용을 권장(TTA, 2017)
- 우리나라는 선행국에 비해 신뢰관리 인프라의 조성시기가 10년 이상 늦어 관련 산업생태계가 열악한 상황으로 국내 클라우드 서비스의 대다수는 사일로 방식의 신원관리 모델을 채택하고 있어 클라우드 서비스 간 상호 운용성이 매우 낮음
- 국내 클라우드 서비스가 사일로 방식에서 벗어나 국제적 경쟁력을 확보하고 새로운 서비스 시장을 창출하기 위해 국내 학·연 분야 신뢰관리 인프라의 육성 필요

데이터 및 e-인프라 접속성 확대

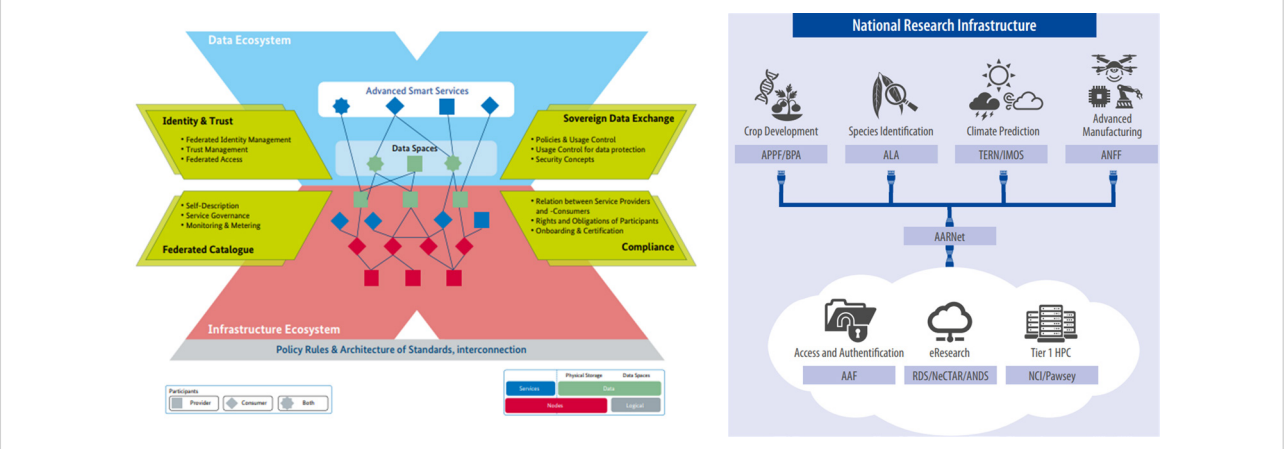
- **(연구분야 핵심 사이버인프라) 4차 산업혁명의 기반인 데이터·인공지능·네트워크의 성장과 혁신을 위해 데이터의 개방성을 확보하고 연구분야 e-인프라를 기관 간 융합 활용하기 위한 촉매제로 신뢰관리 인프라의 역할 증가**
  - 데이터의 탐색(Findable), 접근(Accessible), 상호운용(Inter-operable)과 재사용(Reusable)을 강조하는 FAIR는 유럽연합 집행위원회를 포함한 다수의 조직에서 데이터 원칙으로 인정(DTL, 2021)
  - 유네스코는 데이터 개방을 원칙으로 하되 필요한 경우에 한해 표준규약을 사용한 사용자 인증과 접근통제를 권고

    ※ 데이터 활용 주체의 동의획득과 이력추적 등 데이터 관리를 위해 신뢰관리 체계 필요

2) SAML(Security Assertion Markup Language)은 OASIS에서 정의한 개방형 표준으로 엔터프라이즈 응용의 통합인증을 목적으로 개발, OIDC(OpenID Connect)는 OpenID Foundation에서 정의한 개방형 표준임. 학·연 분야는 SAML을 기반으로 신뢰관리 인프라를 구축하고 있으나 거버넌스의 복잡성, 모바일 응용의 비지원 등 문제가 있어 OIDC로 전환을 시도 중

3) 동일한 정책프레임워크를 공유하는 기관과 서비스제공자의 연합, 우리나라의 신원연합은 KAFE(Korean Access FEderation)으로 국가과학기술연구망에서 운영

<그림 1> 유럽 GAIA-X 및 호주 NRI의 신뢰관리 인프라 활용



출처) BMWi (2020), Australia (2016)

- 범유럽 데이터 인프라 프로젝트 GAIA-X는 가용성과 상호 운용성 및 이식 가능성 확보 등의 주요 목표 달성을 위해 신뢰관리 체계를 데이터 생태계의 핵심 요소에 포함(BMWi, 2020)
- 유럽의 데이터인프라 개발 사업인 '유럽 오픈 사이언스 클라우드(EOSC, European Open Science Cloud)'는 FAIR 원칙의 실현을 위해 신뢰관리 체계를 EOSC 아키텍처에 포함(M. Linden, 2022)
- 호주 정부는 신뢰관리(Access and Authentication), 초고속 연구망, 데이터 및 스토리지 플랫폼, 고성능 컴퓨팅이 핵심 국가 연구 인프라(Australia, 2016)로 작동하는 데이터 기반 디지털 연구 생태계를 구축(M. Barker, 2019)
  ※ 자국 내 학·연 분야 신원연합인 AAF(Australian Access Federation)의 구성을 위해 약 480만 달러의 정부 예산을 투입(Tate, 2008)
- 우리나라 정부도 데이터 산업의 육성을 위해 데이터 3법의 개정 등 법제도를 정비하고 산업 기반을 마련하고자 노력하고 있으나 통합적인 체계 확보의 어려움 예상(한국데이터산업진흥원, 2021)
- 우리나라 학·연 분야 데이터 플랫폼들은 파편화되어 사일로 형태로 운영
  ※ 데이터의 가시성 및 생산성 저하를 초래하므로 개방성과 접근성의 확보 등 FAIR 원칙 실현을 위해 신뢰관리를 통한 플랫폼 간 연계체계 확보 시급

2. 신원모델의 구분 및 연합 신원모델

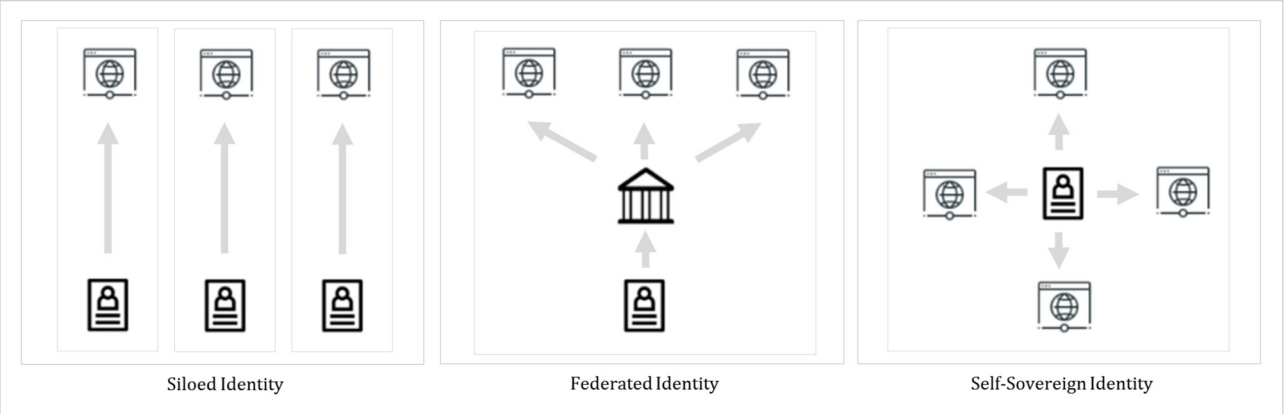
신원 모델의 구분

- **(디지털 신원정보)** 디지털 신원은 온라인에서 개인이나 디바이스를 식별할 수 있는 정보로써 식별자(Identifier)와 식별정보(Identification)으로 구성되며 식별자/비밀번호와 같은 자격증명(Credential)을 통해 확인 가능

- **(신원모델의 유형)** 신원모델은 신원정보의 관리 형태에 따라 개별(Siloed), 연합(Federated), 자기주권(Self-sovereignty)으로 구분, 학·연 분야는 연합 모델에 특화되어 있고 산·관 분야는 개별 모델에서 자기주권 모델로 진화 중

※ 연합 신원모델은 신뢰관리 체계 하에서 작동하나 자기주권 신원모델은 무신뢰(Zero trust [4])를 지향

<그림 2> 디지털 신원모델의 구분



<표 1> 신원모델의 구분

구분	데이터산업법	산업디지털전환법
개별 신원모델	· 개별 서비스에 등록된 신원정보를 활용 · 모델의 구현은 용이하나 비밀번호 피로도가 높고 개인정보보호에 취약	
연합 신원모델	· 기관에서 발급한 신원정보 · 사용자 편의성이 높고 보안 사고의 격리가 가능하나 거버넌스 비용이 높음 · SAML/OIDC 등 표준규약의 활용으로 기술 호환성 높음	
자기주권 신원모델	· 사용자가 신원정보를 직접 관리하는 방식 · 분산원장 및 블록체인 등 기술을 활용해 자격증명 · 웹 표준기구인 W3C 등의 주도로 표준화 진행	

4) 'never trust, always verify'를 지향하는 IT 시스템의 설계 방법론

- **(개별 신원모델의 문제)** 개별 신원모델은 신원관리의 중앙화로 인해 신원정보의 제어권 상실, 취약한 계정 보안, 낮은 사용자 편의성, 규정준수 여부의 비가시성, 사용자 계정의 서비스 종속, 클라우드 간 접속방식의 비일관성 (Okta, 2021) 등 다수의 문제 존재

학·연 분야 신원모델

- **(편의성과 보안성의 강화)** 연합 신원모델은 신원정보의 이동성을 높이기 위해 기술과 표준 및 사례의 일원화된 거버넌스 즉, 신뢰관리 체계를 통해 구현되며 사용자 소속기관이 발급한 신원정보를 이용해 다수의 온라인 서비스들에 통합인증 가능

  - 연합 신원모델의 요소기술은 통합인증, 다중요소인증, 적응형인증, 접근제어, 권한관리 등을 포함

  - 2021년도 리서치 앤 마켓의 조사에 의하면 연합 신원모델의 요소기술을 활용한 글로벌 신원관리 시장의 연평균 복합성장률이 14.8%로써 2026년에는 시장규모가 310억 달러에 달할 것으로 전망

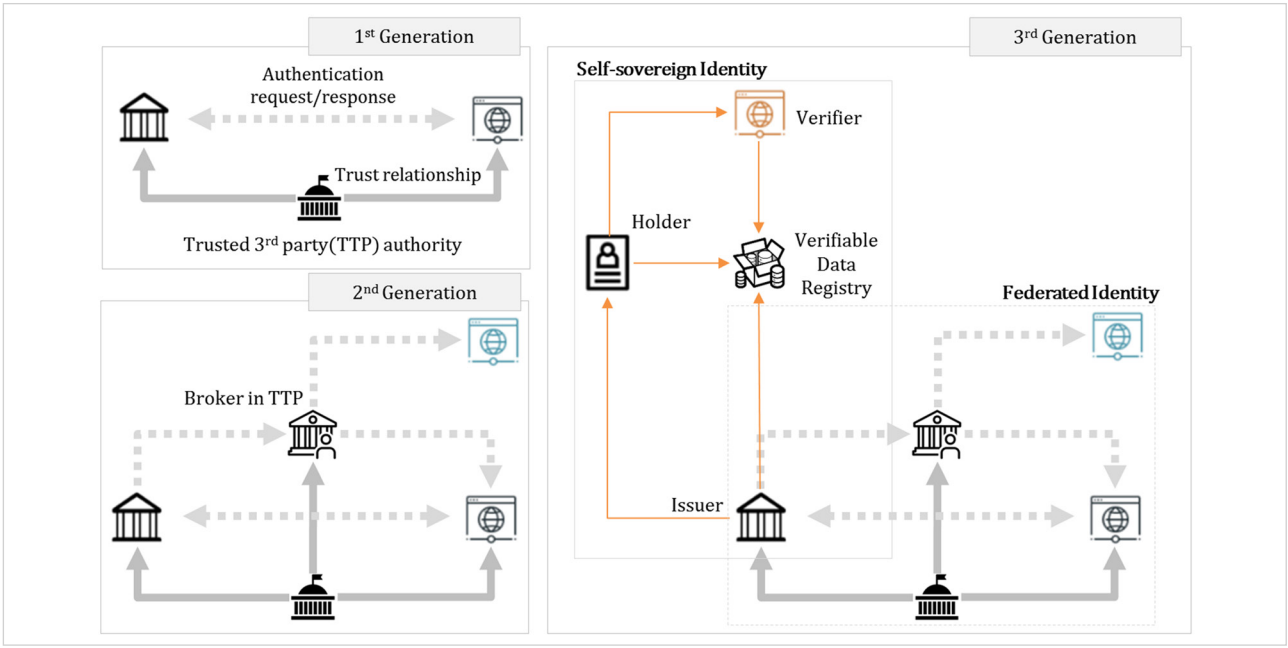
    ※ 2020년도 기준 공공 및 교육 분야의 글로벌 신원관리 시장 점유율은 약 10%로써 학·연 분야 신뢰관리 인프라의 육성을 통해 국내 신원관리 산업체의 글로벌 경쟁력 확보 지원

  - 연합 신원모델은 거버넌스 지점의 단일화, 인증과 권한의 분리, 개인정보 리스크 감소, 클라우드 산업체의 시장 진입 시간 단축, 사용자 정보의 신뢰도, 선제적 보안 집행, 개인정보 보호, 사용자 경험 향상, 관리운영 비용 절감, 거버넌스 효율성 등 장점(G. Hannah, 2014)

    ※ 국제 학·연 분야의 표준 신원모델로 정착되어 국외에서는 신원관리나 클라우드 산업체의 시장 확대를 위한 플레이그라운드 역할 수행 중

    ※ 우리나라도 연합 신원모델기반의 신뢰관리 인프라를 육성하기 위한 정책적 배려 필요

<그림 3> 연합 신원모델 기반 신뢰관리 인프라의 진화



- **(기술적 대비 필요) 연합 신원모델이 적용된 국제 학·연 분야의 신뢰관리 인프라는 메시지 브로커 형태의 2세대 구조를 기반으로 발전하는 가운데 최근에는 자기주권 신원 모델을 접목하려는 시도가 등장(SURF, 2021)함에 따라 2, 3세대 발전방향 각각에 대한 기술적 대비 필요**

  - 단일 인증규약을 사용하는 1세대 신뢰관리 인프라에서 학·연 기관과 서비스제공자는 신원연합 운영자(제3신뢰기관)가 제공하는 정책프레임워크와 공용 소프트웨어를 활용해 사용자인증 메시지를 직접 교환

    ※ 2세대 신뢰관리 인프라는 인증 메시지의 제어강도와 이종 인증규약 간의 호환성향상을 위해 메시지 브로커(Broker)를 도입, 학·연 기관과 서비스제공자는 메시지 브로커를 통해 메시지를 교환

  - 3세대 신뢰관리 인프라에서 발행자(Issuer)에 의해 검증된 신원증빙 정보는 스마트폰 등 사용자 장치에 저장되고 서비스제공자(또는 Verifier)는 사용자가 제출한 신원증빙 정보와 분산원장에 기록된 정보를 비교해 사용자를 인증

    ※ 신원정보 관리의 탈중앙화로 개인정보 보호 강화

  - EU H2020 연구혁신 프로그램의 일환으로 2014부터 6년 간 진행된 AARC(Authentication and Authorisation for Research and Collaboration) 프로젝트는 2세대 신뢰관리 인프라의 준 표준 구조를 제시(AARC, 2022)

    ※ CILogon(NCSA, 미) 등 연합 신원모델이 적용된 다수의 신뢰관리 인프라에서 메시지 브로커의 구현을 위해 AARC BPA(Blueprint Architecture)를 준용

  - 북미 및 유럽의 학·연 분야에서는 사용자 비 친화적인 X.509 인증을 토큰인증 방식으로 전환 시도(Bockelman, 2020),(Gao, 2020)

    ※ 2세대 연합 신원모델이 적용된 국내 신뢰관리 인프라도 토큰인증 기술과 브로커 통합기술의 확보가 요구 됨

  - 네덜란드 연구망 SURFnet은 신원정보의 자기주권 강화를 위해 2021년부터 자기주권 신원모델을 신뢰관리 인프라(3세대)에 적용 시도

    ※ 국내 학·연 분야도 자기주권 신원모델의 도입·활용을 위한 인프라와 기술 확보 필요

신원모델의 패러다임 전환

- **(데이터에 대한 자기주권 강화) 유럽 일반데이터 보호규칙(GDPR) 등의 주요 쟁점인 「자신의 데이터에 대한 통제권 확보」는 블록체인이나 분산원장(Distributed Ledger) 기술을 활용한 탈중앙화 신원관리 모델(자기주권 신원모델)의 도입과 확산을 촉진**

  - 유럽연합은 2014년도 전자신분증 관련법안(eIDAS Regulation)에서 연합 신원모델 기반의 신뢰관리 프레임워크를 채택했고 2021년 개정된 eIDAS 2.0에서는 EU 디지털 신원지갑(Digital Identity Wallet)의 구현을 위해 자기주권 신원모델을 도입(ENISA, 2022),(이강효, 2022)

  - 유럽연합은 2018년부터 블록체인 서비스 인프라(EBSI, EU Blockchain Service Infrastructure)를 구축하고 있으며 2021년에는 자격증, 학생증, 졸업증 등 13개 신원증빙 시나리오를 검증하기 위해 자기주권 신원모델을 적용

    ※ 2023년 말까지 EU 디지털 신원지갑의 대규모 파일럿 계획(Braekeleer, 2022)

- 스위스 연구망 SWITCH는 IBM 등 10여 산업체와 협력으로 개방형 블록체인 인프라인 Dragonfly와 Mantis를 구축하는 등 유럽은 학·연 분야에서도 블록체인 인프라의 확보와 자기주권 신원모델의 도입을 위해 노력

- 학·연 분야의 자기주권 신원모델 도입에 다수의 기술적, 정책적 장벽이 존재하지만 기술 패러다임의 변화에 선제적 대응위해 국내 산·학·연·관의 블록체인 인프라 및 자기주권 신원관리 기술 확보 노력 필요

※ 중앙 관리기관(Central authority)의 필요성[5]이 자기주권 신원모델의 탈중앙화 철학과 대치, 금융실명법이나 개인정보 보호법 등 현행법과 충돌(BLOCKO, 2020),(이강효, 2022), 글로벌 거버넌스의 부재와 Sovrin/Hyperledger 등 자기주권 신원 커뮤니티 간 호환성, 관리주체가 파편화된 응용서비스의 자기주권 신원모델 적용 등 다수 장벽 존재

3. 학·연 분야 신뢰관리 인프라의 활용

국제 동향

- **(72개 국가에서 활용) 연구교육 연합그룹(REFEDS, EU)과 국제 신원연합(eduGAIN, EU)에 의하면 82개 국가에서 86개의 신원연합을 운영 중이며 유럽연구망 GEANT의 거버넌스를 통해 80개 신원연합이 상호 연동**

※ 세계 5,165개 학·연 기관과 3,618개 서비스제공자가 국제 신원연합을 통해 연결, 국가 간 경계 없는 데이터 및 e-인프라 활용환경이 구축 됨

<표 2> 주요 국가의 신원연합

신원연합명	국가	기관	SP	특징	주요 서비스
InCommon	미국	5,179	7,505	클라우드	LIGO, Globus, XSEDE
SURFConext	네덜란드	162	27	클라우드	EOSC, eduRoam, OCRE
AAF	호주	55	253	데이터	NeCTAR, MWA, RDS
GakuNin	일본	281	197	전자저널	NII, JAIRO, KOSEN
SWITCHaai	스위스	70	1,601	연구인프라	CERN, SWITCH Cloud
KAFE	한국	28	61	연구인프라	KiCloud, DataOn, ScienceOn

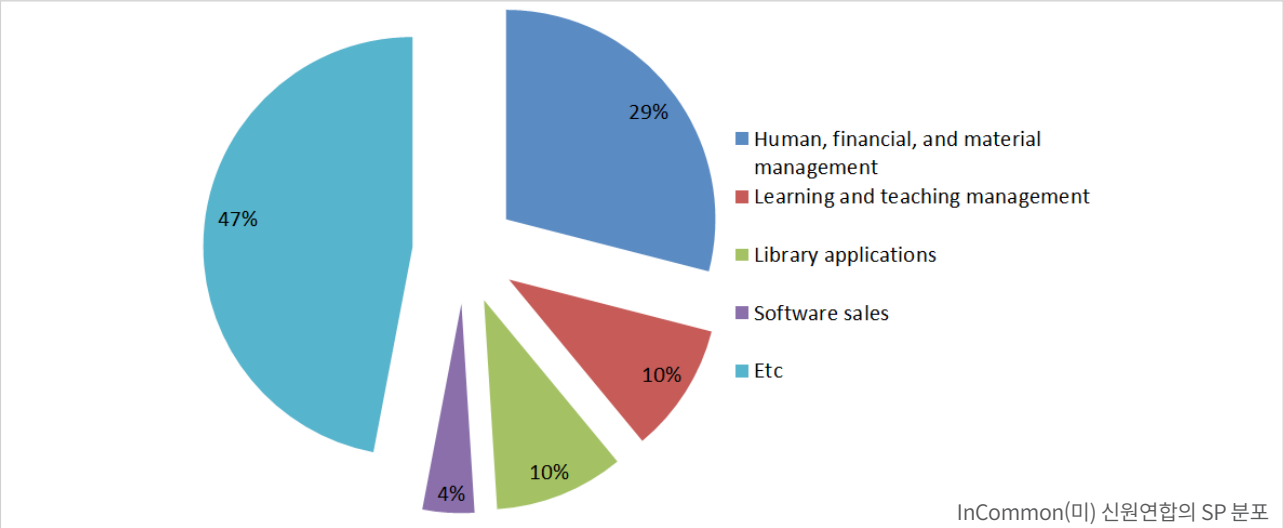
출처) REFEDS(https://met.refeds.org)

- 국가 단위 신뢰관리 인프라는 클라우드 산업체의 플레이그라운드 역할 수행, 미국은 200개 산업체가 InCommon을 통해 4,000여 클라우드 서비스를 자국 내 학·연 기관에 제공

※ 재무/인력/경력 관리 등 기관 활용 행정서비스와 학습/교수 관리서비스가 전체 클라우드 서비스의 약 40%를 점유

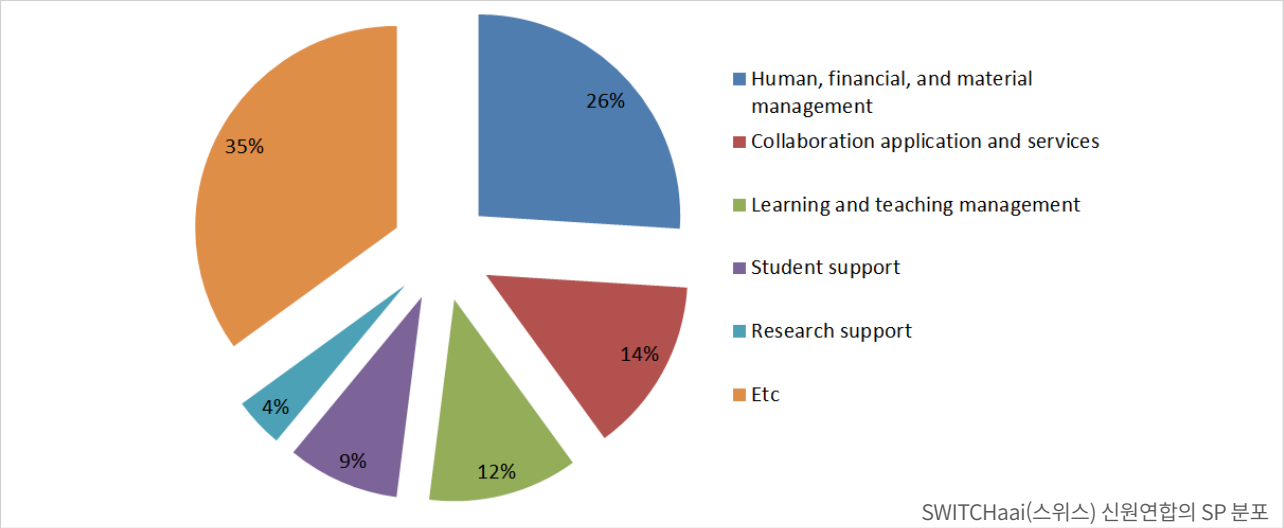
5) 가상조직(Virtual Organization, VO) 정보를 활용하는 과학기술 응용서비스의 특성으로 인해 VO 관리를 위한 중앙 관리기관 필요

<그림 4> 미국 및 스위스 신뢰관리 인프라 제공 클라우드 서비스 분포



InCommon(미) 신원연합의 SP 분포

<그림 4-1> 미국 및 스위스 신뢰관리 인프라 제공 클라우드 서비스 분포



SWITCHaai(스위스) 신원연합의 SP 분포

- 운영기관의 역할과 책무에 의해 신원연합의 서비스 방향이 종속: 중립성의 확보를 위해 공공부문의 종합 인프라(데이터/컴퓨팅/네트워크/콘텐츠) 서비스 기관에서 운영하거나 독립법인 형태의 신원연합 운영이 바람직

  ※ 영국 신원연합 UKAF와 일본의 GakuNin은 각각 합동정보시스템위원회(JISC)와 국립정보학연구소(NII)에서 운영, 운영기관의 역할에 따라 전자저널 등 지식정보콘텐츠가 서비스제공자의 50% 이상 점유

  ※ 미국 신원연합 InCommon과 호주의 AAF는 유한책임회사의 형태로 운영되어 서비스 중립성 확보

- 호주 정부는 국가 협업연구 인프라 전략(NCRIS)의 일환으로 시작된 NeCTAR[6] 프로젝트를 통해 생물정보, 정보컴퓨팅 등 16개 연구분야를 대상으로 클라우드 기반 가상실험실을 구축하고 신뢰관리 인프라를 통해 상호 연동(Coddington, 2020)

  ※ 데이터 및 e-인프라의 공동활용 환경 조성

6) National eResearch Collaboration Tools and Resources: 2010년부터 호주정부의 예산 투입으로 국가연구클라우드와 가상연구실 등 클라우드 기반의 연구협업 인프라를 구축하는 사업으로 현재는 ARDC(Australian Research Data Commons)가 지원

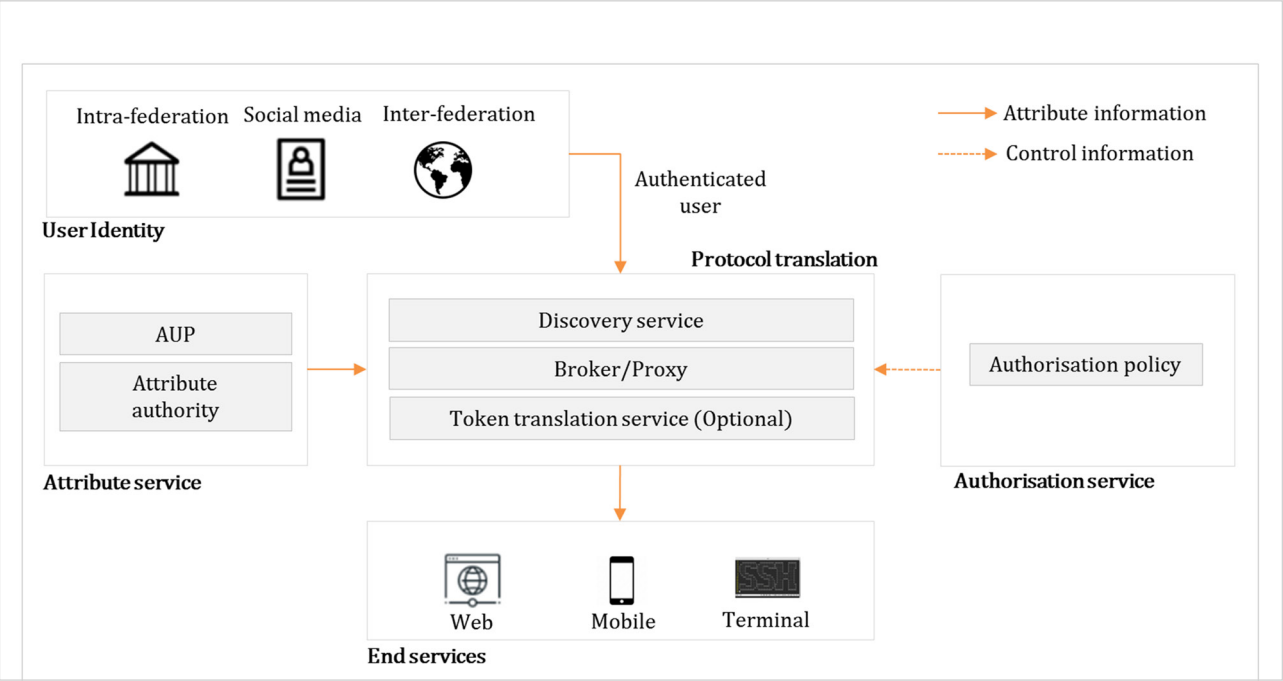
연합 신원모델의 e-인프라 적용

- **(공동활용 촉매제)** 과학적 난제 해결을 위해서는 대규모 e-인프라의 국가 및 기관 간 공동활용이 필수적, 신뢰관리 인프라는 공동활용을 촉진하기 위한 촉매제로 작동

  - 신원연합의 신뢰관리 인프라는 2세대 연합 신원모델인 메시지 브로커의 도입으로 OAuth2/OIDC, Moonshot(SSH 등 터미널응용 지원) 등 이질적 인증규약에 종속되지 않는 서비스 접속환경 구축 가능(Atherton, 2018)

    ※ 이질적 학·연 분야 e-인프라를 신원계층(Identity layer)에서 통합

<그림 5> 2세대 연합신원 모델의 메시지 브로커 구조



- **(표준기술 적용통한 호환성 확보)** 유럽 연구망 GEANT은 AARC BPA를 통해 2세대 연합신원 모델의 준 표준 메시지 브로커 구조를 제시, 1세대 연합 신원모델을 채택한 다수의 연구 분야 e-인프라가 2세대 모델로 진화

  ※ ELIXIR 등 데이터보호가 중요한 생명과학 분야에서 자기주권 신원모델 도입을 위한 개념연구가 진행(Linden, 2022) 중으로 향후 연합 신원모델과 자기주권 신원모델이 병행 활용될 전망

  - 메시지 브로커는 이질적 종단서비스(End services)의 통합인증을 가능케 함

    ※ 인증규약 변환(Protocol translation), 권한관리(Authorisation service), 속성관리(Attribute service) 기술이 이종 종단서비스 간 호환성 제공

<표 3> 1/2세대 연합 신원모델이 적용된 신뢰관리 인프라의 학·연 분야 e-인프라 적용

연구영역	커뮤니티	참여국	1세대 모델	2세대 모델	비고
인문사회	CLARIN	22	○	-	
	DARIAH	55	○	○	
생명	ELIXIR	22	○	○	
고에너지물리	WLCG	43	○	-	예정
광자 및 중성자	-	11	○	×	
기후	ESGF	13	○	-	고려
지구관측	ESA/EOP	30+	○	×	
중력파	LIGO	20	○	○	
	KAGRA	15	○	×	
	Virgo	6	○	×	
핵물리	FAIR	50	-	-	
감마선천문	CTA	32	○	○	
전파천문	MWA	6	○	○	
	SKA	20	○	○	
광물리	VAMDC	30	-	○	
전리층대기	EISCAT	9	-	-	예정
전염병	NIH/NIAID	15	○	○	
오픈액세스	OpenAIRE	27	○	-	
IT	EOSC	27	○	○	
	EGI	-	○	○	

출처) Atherton, 2018

- 우리나라는 2세대 모델의 메시지 브로커 구조 중, 인증규약 변환 기술과 권한관리 기술을 확보하고 있으나 속성관리 기술이 개념연구 중인 단계로 국내 학·연 분야 e-인프라의 공동활용 환경 조성을 위해 조속한 기술력 확보 노력 필요

4. 결론 및 제언

결론

- **데이터 보호, 클라우드 등 온라인 소프트웨어 산업 육성, 데이터와 e-인프라의 공동활용 촉진을 위해 학·연 분야 신뢰관리 체계의 조속한 확보 필요**
  - 미국과 유럽연합 등 기술 선행국은 정부 차원의 신뢰관리 전략을 수립하고 민간으로 가이드라인을 전파해 안전한 사이버공간 구현 선도
  - 세계 82개 국가는 학·연 분야 신뢰관리 인프라를 구축해 e-인프라의 국가 간 경계 없는 공동활용 환경을 조성하고 클라우드 등 소프트웨어 산업의 플레이그라운드로 활용
  - 특히, FAIR 데이터 원칙 실현을 위한 요소기술로 신뢰관리 인프라가 적합
- **학·연 분야 국제 e-인프라는 사일로 형태의 개별 신원모델에서 벗어나 1/2세대 연합 신원모델을 채택 또는 자기주권 신원모델로 진화하고 있어 관련분야 신원관리 핵심기술의 확보 필요**
  - 유럽 연구망 GEANT은 데이터 및 e-인프라들의 상호 호환성 제고를 위해 2세대 연합 신원모델의 준 표준 구조를 제시
  - 기술 선도국은 특정 인증규약에 종속되지 않는 프로토콜 불가지론적(Protocol-agnostic) 인증 등 2세대 연합 신원모델의 핵심 기술을 확보
  - 유럽연합은 EU 디지털 신원지갑의 구현을 위해 자기주권 신원모델을 도입, 유럽 학·연 분야도 EU 전략에 따라 자기주권 모델의 개념증명 단계
- **학·연 연구자의 기관 또는 국가 간 디지털 이동성 확보와 협업연구 촉진을 위해 신뢰관리 인프라의 구축과 학·연 분야 확대 적용 필요**
  - 국외의 경우, 2세대 연합 신원모델이 적용된 신뢰관리 인프라를 생명, 고에너지물리, 중력파, 천문관측, 전염병, IT 등 다양한 연구영역에서 광범위하게 활용

제언

- **민·관 협력을 통한 국가적 연합 신원관리 인프라의 구축과 육성 노력 필요**
  - 국내에서도 네트워크, 데이터 플랫폼, 고성능 컴퓨팅과 함께 신원관리를 핵심 국가 연구 인프라로 인식 필요
  - 정부는 개인정보보호, 정보시스템 관리 등과 관련된 국가법령이나 정부지침을 효과적으로 거버넌스하기 위한 도구로 연합 신원관리 인프라를 활용 가능

    ※ 개인정보의 유출과 오남용으로 인한 사회적 문제 완화

- 학·연 기관은 e-인프라의 공동활용을 통한 연구생산성 제고, 기관 간 정보격차의 해소, 디지털 전환의 촉진을 위해 활용 가능
- 산업체는 클라우드 서비스, 신원 및 접근관리 제품의 시장 진입과 확대 또는 신규 시장 창출을 위한 플레이그라운드로 활용 가능

● **학·연 분야 기술자립을 위한 신원 모델별 핵심기술 확보**

- 선도국에 비해 5년 이상의 기술격차를 갖는 프로토콜 불가지론적 인증기술의 국산화를 통해 기술 자립
- 국내 데이터센터 등에서 활용 중인 공인인증서의 이용폐기 방침(유럽입자물리연구소)에 따라 토큰인증 전환을 위한 개념증명 및 토큰인증의 신원모델 통합 필요
- 학·연 분야 신원 모델의 방향성이 불분명하나 자기주권 신원모델로의 패러다임 변화에 선제적으로 대응하기 위해 학·연 분야 특화 블록체인 인프라 확보 필요
- 자기주권 신원모델의 핵심 기술인 분산원장의 국내 학·연 분야 적용방안 수립을 위해 조속한 개념증명 수행 필요

● **학·연 공동관리 거버넌스 체계의 확보와 활용 확산**

- 국내 신원연합의 파편화 운영을 방지하기 위해 통일된 거버넌스 체계와 공동 관리운영 방안의 수립 등 다부처 산하기관 간 긴밀한 협력 필요
- 국제 신원연합과 협력을 통해 신원관리 보증수준, 데이터보호 수행지침 등 정책프레임워크를 개발하고 국가 간 호환성 확보위한 노력 수행
- 사일로 형태의 개방형 연구 플랫폼에 연합 신원모델을 조기 정착하기 위해 탑다운 방식의 정책 집행이 요구됨
- 신뢰관리 인프라 내 서비스 수요와 공급의 주체인 학·연 기관과 온라인 소프트웨어 산업체 간에 협력 채널 구축 필요

참고문헌

- 권동승, 이현, 박종대 (2019), 「디지털 신뢰 사회 실현을 위한 디지털 아이덴티티 동향」, 2019.
- 이강효, “블록체인, 웹3.0 기술 생태계 동향”, TTA Journal, Vol.200, 2022.
- 한국데이터산업진흥원, 2021 데이터산업 백서, 2021.
- AARC, AARC Blueprint Architecture, 2022. Available at https://aarc-project.eu/.
- Australia (2016), 2016 National Research Infrastructure Roadmap, Australian Government, 2016.
- BLOCKO (2020), 「DID(분산ID)와 SSI(자기주권신원), 단순 로그인을 넘어서」, 2020.10
- BMWi (2020), GAIA-X: The European project kicks off the next phase, Federal Ministry for Economic Affairs and Energy, 2020.6.
- B. Bockelman et al, “WLCG Authorisation: from X.509 to Tokens,” The European Physical Journal Conferences, 2020.1.
- C. J. Atherton et al, Federated Identity Management for Research Collaborations, Whitepaper, 2018.7.
- CISA (2022), “Cloud Security Technical Reference Architecture V2.0,” 2022.6
- DTL (2021), European Commission embraces the FAIR principles. 2021.4.
- eIDAS (2014), Electronic identification and trust services for electronic transactions in the internal market, Regulation (EU) No.910/2014, 2014.7.
- ENISA, Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust, European Union Agency for Cybersecurity, 2022.1.
- G. Hannah et al, Identity federation governance: Catalyst for the Identity Ecosystem, Deloitte, 2014.
- G. D. Braekeleer, “Results, challenges and Q&A,” TF-DLT meeting, 2022.2.
- M. Negreiro and M. Niestadt (2022), Updating the European digital identity framework, European Parliament briefing, 2022.10.
- M. Barker, R. Wilkinson, and A. Treloar (2019), “The Australian Reearch Data Commons,” Data Science Journal, Vol.18, No.44, pp.1-7.
- M. Linden, “Why AAI (Authentication and and Authorization Infrastructure) matters: current developments in EOSC and in the Life Science area,” 2022.6.
- M. Linden and J. Lauros, “Self-Sovereign Identity Proof of Concept,” Common Infrastructure for National Cohorts in Europe, Canada, and Africa (CINECA), 2022.6.
- N. Sargent (2012), “Federated Identities in the Real World,” 2012.
- N. Tate, “Overview, history and Australian Access Federation (AAF),” eResearch Australasia, 2008.
- Okta, Top 9 Identity & Access Management Challenges with Your Hybrid IT, Okta Whitepaper, 2021.
- P. Coddington, Virtual Laboratories and the Nectar Research Cloud, Australian Research Data Common (ARDC), 2020.

참고문헌

- SURF, Technical exploration Ledger-based Self Sovereign Identity, 2021.
- The White House (2011), National Strategy for Trusted Identities in Cyperspace: Enhancing online choice, efficiency, security, and privacy, 2011.4.
- TTA (2017), 클라우드 상호운용성 확보 가이드 라인 Vol.2, 2017.
- Verizon (2021), Data Breach Investigation Report Master's Guide, Verizon White Paper.
- Verified Market Research (2022), Cloud Computing In Education Sector Market Size And Forecast, 2022.
- Y. A. Gao et al, "SciTokens SSH: Token-based Authentication for Remote Login to Scientific Computing Environments," PEARC '20, 2020.7.

저 자

조진용
KISTI 과학기술디지털융합본부
과학기술연구망센터 책임연구원
T. 042-869-0585
E. jiny92@kisti.re.kr

김승해
KISTI 과학기술디지털융합본부
과학기술연구망센터 책임연구원
T. 042-869-0582
E. shkim@kisti.re.kr

조부승
KISTI 과학기술디지털융합본부
과학기술연구망센터 책임연구원
T. 042-869-0584
E. bscho@kisti.re.kr

KISTI ISSUE BRIEF 제50호

발 행 일 2022. 12. 12.

발 행 인 김재수

편 집 위 원 조민수, 최희석, 이준, 정한민, 함재균, 이준영, 이상환, 곽영

발 행 처 34141 대전광역시 유성구 대학로 245
한국과학기술정보연구원 정책연구실
https://www.kisti.re.kr

I S S N 2635-5728