개인정보보호 강화 및 비대면 서비스 활성화를 위한 차세대 보안기술

2019. 08. 12.

차세대보안분과장

권대성

목차

1. 표준화 개요

- 데이터3법 제정에 따른 개인정보 보호필요성이 증가하고, 감염병 질병으로 인한 비대면 서비스 확대에 따라 해킹, 위변조 등 각종 불법 행위로부터 전달・저장되는 (개인)정보・데이터를 안전하게 보호하는 기술

- 구분: 암호기술, 인증기술, 물리보안기술, 사이버위협 대응기술, 보안관리/평가 기술 등과 데이터 활용을 위한 비식별 처리 등을 데이터보안(신규)으로 구분

2. 표준화 목표

표준 경쟁력 강화

- 개인정보보호 및 데이터 보안의 핵심기술인 형태보존암호, 동형암호 및 활용, 비식별 데이터 보증수준에 관한 표준 선점
- 차세대 동물등록제에 필요한 비문.홍체인식 등을 이용한 반려동물 개체식별기술 제안 등 바이오인식 분야 국제표준화 선도

중소기업 경쟁력 강화

- 공인인증제도 폐지 후 다양한 사설인증 서비스의 상호운영을 위한 기술 규격을 마련하여 전자거래 전 분야의 서비스 활성화에 기여
- 분산 ID 관리 (Decentralized Identity Management) 기술의 수요가 핀테크, 모바일 신분증 등 신사업 분야에서 급격히 증가하고 있어, 이에 대한 표준 마련 및 국제표준화 추진으로 국제 경쟁력 확보
- 암호모듈을 안전하게 사용하기 위한 검증 및 시험 기준, 물리적인 복제방지기능(PUF) 기술 등에 대한 적극적 대응을 통하

2. 표준화 목표

국민행복 안전보장

- 화상회의, 원격수업, 언택트 결제 등 비대면 서비스에서의 사용자 신원검증 기술과 원격 의료 서비스 등에서의 생체신호 기반 텔레바이오 인증기술 등으로 포스트코로나 시대의 비대면 서비스의 안전성 제공
- 양자컴퓨터 위협에 대비하기 위한 양자암호기술의 조기 실용화를 위한 보안규격, 시험평가 기준 마련
- 중앙화 된 신원관리의 정보 오남용 문제점을 해결하고 자기 정보를 응용서비스에 맞추어 선택적으로 이용할 수 있는 신원관리 기법 확보
- 사이버 침해정보 분석 및 공유기술을 기반으로 지능화된 사이버 위협으로부터 주요 ICT 인프라 보호

3. 중점 표준화 항목

→ 6개 분류, 12개 중점 표준화 항목 도출

중점 표준화 항목		표준화 내용
암호	암호 알고리즘	신규 ICT 환경(IoT,Cloud, 빅데이터, 스마트기기, DBMS 등)의 정보보호에 적합한 차세대 암호 알고리즘 규격
	양자 암호기술	양자키분배(QKD) 기술 규격, 안전성 평가기술/기준
인증	ID 관리 기술	통합 ID 관리 또는 분산 ID 관리(DID) 서비스를 통해 개체(사용자, 기기, 서비스) 자격증명 및 속성 공유를 위한 공통 데이터 포맷 및 상호연동 표준
	프라이버시 인증기술	영지식 증명, 프라이버시 강화 암호기법 등을 이용하여 사용자의 프라이버시를 보호하는 인증 표준
	비대면 신원 확인 기술	비대면 서비스에서 사용자 신원 확인을 위한 사용자 인증 및 본인확인 기술과 다양한 인증 서비스 간의 상호운영을 위한 기술 규격
물리 보안	바이오인식 응용 서비스	위변조 방지, 분산 바이오인식 응용기술 등 바이오정보 보호기술, AI 딥러닝기반의 바이오인식 응용기술, 바이오인식기반 반려(축산)동물 개체식별기술
	생체신호기반 텔레바이오 인증기술	생체신호 인증메커니즘 보안성 평가표준, 생체신호 측정 장비 기기인증 및 보안대책, 생체신호인증기반의 헬스모니터링 분석 표준, 생체신호를 이용한 의료정보 보호기술 등
사이버위협 대응	능동형 사이버보안 침해정보 수집 및 보존 기술	사이버 침해정보를 수집 및 보존하기 위한 기능 및 구현 지침 표준
	악성코드 분석 정보 공유 포맷	악성코드 표현 방법, 정상 및 악성파일의 속성 정보, 데이터 스키마, 메타 데이터 등의 악성코드 분석 정보에 대한 교환 포맷 표준
보안관리/보안평가	암호모듈 시험평가 기준	암호모듈 검증 및 시험기준 표준, 암호모듈 시험자 및 시험기관 역량기준 표준화
데이터 보안	비식별 데이터 보증 수준을 위한 요구사항	비식별 처리 데이터의 보증 수준 정의, 재식별 위협 분류, 비식별 처리 모델별 데이터 보증 수준 요구사항 정의
	동형암호기반 데이터 유출 방지 지침	데이터 처리과정에서 개인정보 및 정보유출을 방지하기 위한 동형암호 기술을 활용

4. 주요 기술개발 현황 – 암호 기술

국내

(암호알고리즘) 국내외 차세대 암호 알고리즘 개발 수요를 반영하여, 국가보안기술연구소(NSR)는 경량・고속 암호와 DBMS 적합형 암호 알고리즘을 개발하였으며, 서울대는 동형 암호, 서울대 고려대/서강대/NIMS 등은 양자내성 암호 등을 개발

(양자암호기술) 산업계(SKT, KT)의 유선 양자키분배(QKD) 개발 주도와 함께, 출연연 중심의 양자키분배(QKD) 소형화 기반 기술 및 무선 양자키분배(QKD) 핵심기술 개발

국외

(암호알고리즘) 미국과 유럽은 각각 국가 기관, 산업체와 학계를 중심으로 차세대 암호 알고리즘의 개발 및 국제표준화를 통한 시장 주도권 선점을 추진 중

- **(미국 IBM, Microsoft 등)** 다수의 동형 암호 알고리즘을 개발하고 의료 분야 등 다양한 응용서비스 적용 기술 개발 중

(양자암호기술) 중국은 기간망 및 인공위성 양자암호통신 구축을 완료하였고, 유럽, 미국은 장거리 양자키분배(QKD) 및 네트워크 운용기술 개발 추진 중

4. 주요 기술개발 현황 – 인증 기술

국내

(ID 관리 기술) ETRI, SKT 등은 분산원장기술 또는 블록체인상에서 분산형 ID를 지원하는 ID 관리 기술 개발 중

(프라이버시 보호 인증기술) ETRI, SKT, 충남대 등은 영지식 증명 등을 이용한 프라이버시 보호형 ID 관리 기술을 개발 중

(비대면 신원 확인 기술) 2020년 공인인증서 제도가 폐지되면서 비대면 신원 확인을 위한 기존 사설인증 서비스가 웹플랫폼 기업, 통신사, 금융권을 중심으로 확대 재편되는 중

국외

(ID 관리 기술) 오픈소스를 중심으로 블록체인 관련 프로젝트가 활발히 진행 중. 하이퍼레저(Hyperledger) 인디(Indy)를 중심으로 자기주권 신원(Self-Sovereign Identity) 모델 및 분산형 ID 관리를 실증하는 서비스들을 글로벌 기업, 스타트업, 정부기관 등이 개발 중

(프라이버시 보호 인증기술) 영지식 증명을 이용한 선택적 노출 기능 및 프라이버시 보호를 제공하는 기술을 활발히 개발 중

(비대면 신원 확인 기술) 화상회의, 온라인 교육, 원격의료 등의 서비스가 확대되면서 기존 패스워드 대신 생체인식 등을 적용한 비대면 신원 확인 기술 개발 및 제품 출시

4. 주요 기술개발 현황 – 물리 보안

국내

(바이오인식 응용 서비스) 한국바이오인식협의회 등은 모바일 바이오인식제품의 성능시험기술, 바이오인식 제시형 공격탐지 시험기술을 개발

- **(슈프리마)** 지문·안면인식 등 사용자 고유의 생체정보의 성능시험기술 개발 및 적용
- **(한국바이오인식협의회)** 조달청 지문보안토큰의 위조지문 평가기술을 개발 및 시험서비스 진행

(생체신호기반 텔레바이오 인증기술) KISA에서는 심전도 등 생체신호를 이용한 텔레바이오 인증기술을 개발완료하였으며, 생체신호 인증기반의 헬스모니터링 분석기술을 연구중

국외

(바이오인식 응용 서비스) 미국·유럽 등 주요선진국에서는 바이오인식 성능시험 및 모바일 바이오정보 위변조 탐지 시험인증서비스 개발 및 제공

(생체신호기반 텔레바이오 인증기술) 생체신호센서, 다중 생체신호 인증기술 중점 개발 중

- (Texas Instrument, 미국 워싱턴대) 뇌파·심전도·심박수·근전도 등 생체신호 측정용 의료장비 및 웨어러블 디바이스, 생체신호센서용 MoC IC칩 등 미국 TI(Texas Instrument)사를 중심으로 상용화가 진행 중이며, 미국의 워싱턴대 등 대학교를 중심으로 뇌파·심전도·심박수 등 생체신호 개인식별 기술에 대한 연구가 활발히 진행 중

4. 주요 기술개발 현황 – 사이버 위협대응

국내

(침해정보 수집 및 보존 기술) 보안정보 및 자산정보의 수집, 공유를 기반으로 동적 방어 및 보안 기술에 대한 연구개발(ETRI, ADD, KISA, GIST 등) 중

(악성코드 분석 정보 공유 포맷) 기하급수적으로 증가하는 악성코드에 대응하기 위해 전통적인 분석 절차 일부를 정형화하여 자동분석 및 대응 기술을 고도화하고, 악성코드 수집 및 정보공유를 위한 기술개발을 추진 중

국외

(침해정보 수집 및 보존 기술) 기존 보안기술 분야에 동적 변이 기술 개발을 통해 **능동적이고 선제적인 보안을 제공**하기 위한 연구 개발이 진행되고 있으며, 미국을 중심으로 **서로 다른 기관간의 보안정보 공유를 통한 협력기반의 연동 프레임워크** 기술에 대한 연구를 활발히 진행 중 또한 최근 네트워크에서 **수집한 정보를 기반으로 공격 가능성을 테스트하는 Breach and Attack Simulation(BAS)** 기술에 대한 기술 개발이 진행 중

(악성코드 분석 정보 공유 포맷) Micosoft, 카스퍼스키랩, VirusTotal과 같이 대형 글로벌 기업이 평판기반, 화이트리스트 기반, 클라우드 기반의 백신 서비스를 위한 악성코드 분석 및 정보공유 기술을 보유 중

4. 주요 기술개발 현황 – 데이터 보안

국내

(비식별 데이터 보증 수준) 금융보안원, KISA, 서강대, 이지서티, 파스닷컴 등에서 다양한 기법의 비식별 기술 솔루션 프로그램을 개발 중

(동형암호기반 데이터 유출 방지) 삼성SDS 등에서 비신뢰 환경에서 민감정보 유출 방지, 비식별처리 및 협업환경에서 안전한 데이터 처리를 위한 동형암호의 응용 플랫폼 구축 표준 개발 중

국외

(비식별 데이터 보증 수준) 핀테크 기술로서 빅데이터를 분석 및 이용 시 개인정보보호를 위한 처리 기술로 비식별 처리 기법 및 평가 방법 개발이 진행 중

(동형암호기반 데이터 유출 방지) 기업과 학계를 중심으로 동형암호 개발이 주도되고 있으며, 통계적 분석, 기계학습과 더나아가 인공지능까지 암호화된 상태로 계산을 목표하며, 국제표준화를 통한 시장 주도권 선점을 추진 중

4. 주요 표준화 현황

국제

(JTC1 SC27 WG1) 정보보호통제 표준인 ISO/IEC 27002의 개정안 개발을 개시하였으며 정보보호통제 평가지침인 ISO/IEC 27008은 2차 개정판을 발행, 분야별 통제 표준인 270011(통신), 27017(클라우드), 27019(에너지), 29151(개인정보) 등 ISO/IEC 27002에 기반한 분야별 통제 표준을 지속적으로 개발 및 재개정 중

(JTC1 SC27 WG2) 신규 기술 수요에 따른 차세대 암호(형태보존 암호, 동형 암호, 경량 인증 암호화 등) 표준화 항목 및 대상 증가 전망, 양자컴퓨팅 위협에 대비한 암호기술의 표준화 논의 중

(JTC1 SC27 WG3) IT제품의 보안성 평가기준표준인 ISO/IEC 15408과 평가방법론 ISO/IEC 18045를 2020년 개정할 예정, 암호모듈 검증기준인 암호모듈 보안요구사항 ISO/IEC19790 과 시험기준인 ISO/IEC 24759의 개정이 개시되어 2023년 발행 예정

(JTC1 SC27 WG5) 바이오정보 보호기술(24745R1) 개정안을 개발 중. WG1과 공동으로 ISO/IEC 27552 개인정보 보호경영을 위한 27001 확대 요구사항 표준 개발 진행 중

(JTC1 SC37 WG2) 객체지향형 바이오인식 호환규격(30106-4), 객체지향형, 바이오인식 호환성 시험기술(30106-1AMD1) 개발

(JTC1 SC37 WG5) 얼굴인식을 결합한 지능형 CCTV 성능시험기술 개발 중

4. 주요 표준화 현황

국제

(ITU-T SG17 Q.3) 정보보호 활동 기준 표준 및 침해사고 대응 활동 가이드 개발 등

(ITU-T SG17 Q.4) 사이버보안 침해증거 수집 및 보존 관련 **사이버보안 침해사고 증거를 수집 및 보존하는 도구를 위한 가이드라인 표준** 개발을 진행 중, 샌드박스 환경에서 악성코드 동적분석을 위한 요구사항 및 가이드라인 표준 개발을 진행 중, **양자난수발생기(QRNG) 아키텍쳐** 표준 제정(X.1702) 및 **양자키분배(QKD) 개발 고려사항**에 대한 기술문서(TR.sec-qkd) 승인완료 및 관련 권고안 2건(X.sec_QKDN_ov, X.cf_QKDN) 개발 진행 중, **동형암호기반의 기계학습에서 데이터 협업**을 위한 정보보호 지침 (TR.sgfdm)가 신규 표준아이템으로 채택(2020.03)

(ITU-T SG17 Q.7) 개방형 핀테크 플랫폼 정보보호 프레임워크(X.1149) 및 데이터 비식별화 처리 표준 (X.1148) 개발 완료, 비식별화 정보보증의 요구사항 표준 개발중(X.rdda)

(ITU-T SG17 Q.9) 생체신호를 이용한 텔레바이오 인식 인증기술(X.1094) 국제표준 채택, 생체신호 인증기반 헬스케어 텔레바이오 인식 응용서비스기술 표준화를 ISO TC215와 공동 추진 예정, 텔레바이오인식기술을 이용한 반려동물 개체식별 인증서비스(X.pet_auth) 국제표준 제안 승인되어 표준초안 개발 중

4. 주요 표준화 현황

국내

(TTA PG501) 응용서비스 보안을 위한 기반 암호기술 및 양자내성 암호 표준 개발 중

(TTA PG502) 분산ID를 활용한 신원관리 프레임워크, 분산원장 기반 분산형 신원에 대한 보안 고려사항 및 가상 자산 송금 이용자 신원 확인 서비스 모델 등 개발 중

(TTA PG503) 구조화된 위협 정보 표현 규격(STIX 2.0)에 대한 시리즈 표준과 유스케이스 표준 제정, 가상화 기반 이기종 백신 서비스 제공을 위한 시스템 요구사항 표준 개발 중

(TTA PG504) 응용 보안 평가 인증 부문 정보통신단체 표준 제·개정, 정보보안 평가 및 검증 기술 실무반(WG5041)을 2018년 신설하여 시험/평가 및 검증 분야 국내 표준 개발 중

(TTA PG505) 바이오인식 응용서비스 관련, 바이오인식과 IC카드를 이용한 접근제어용 개인확인 및 반려동물 개체식별 시스템, 정보분할에 의한 바이오정보보호 등을 개발 중이며 생체신호기반 텔레바이오 인식기술 관련, 생체신호를 이용한 헬스케어 응용서비스 기술보고서를 개발 중

(개인정보보호포럼) 개인정보보안 기술 관련 국내/국제 표준 개발 및 제.개정, 스마트그리드, 클라우드, 스마트 폰 보안, 암호알고리즘 등 보안 및 개인정보보호 기술 국외 표준 개발

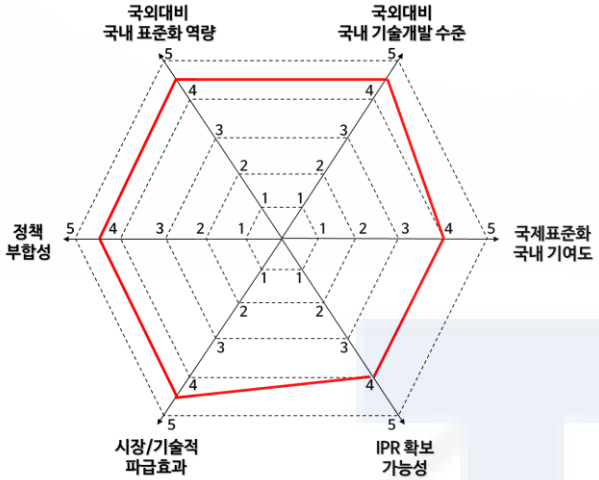
5. 중점 표준화 항목 추진 전략

SWOT 분석

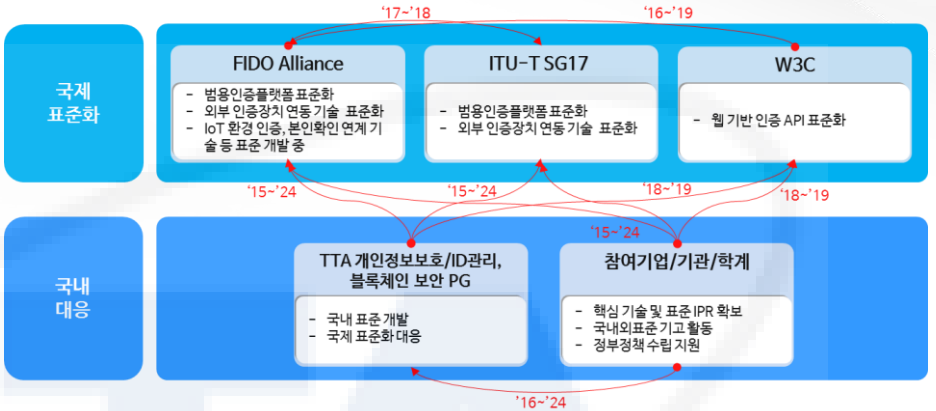
【강 점】 ㅇ 보안 필요성에 대한 높은 범사회적 인식 ㅇ 감염성 질병(COVID-19 등)으로 비대면 인증, 비식별화 기술 개발에 정부의 투자 증가 ㅇ 침해사고 대응체계 구축 및 풍부한 운용 경험 보유 ㅇ 보안 분야에서 국내 전문가의 국제표준화 기여도 높음	**【약 점】** ㅇ 국내 보안시장 규모 협소 ㅇ 국내개발 암호기술의 제품 적용사례 미흡 ㅇ 차세대 암호・인증 기술, 정보보호 관리체계 구축 등 관련 고급 개발인력 부족 ㅇ 정부기관 중심으로 표준화 진행하며, 산업체의 참여 미흡 ㅇ 융합보안 분야에 보안기술 적용 협력 미흡
【기 회】 ㅇ 감염성 질병(COVID-19 등)으로 인한 비대면 회의, 온라인 교육 등의 시장 규모 확장 ㅇ 개인 정보보호에 대한 지속적 수요 ㅇ 해킹기술의 고도화 등으로 정보보호 강화 요구 증가 ㅇ 국제표준화 기구에서 생체인증, 데이터보안 관련 표준화 선도 가능	**【위 협】** ㅇ 다양한 보안 분야에서 글로벌기업의 독점 우려 ㅇ 상호운용성 확보 및 개발 규모를 이유로 국내 개발 암호기술의 제품 적용 기피 ㅇ 국가 차원의 보안 원천기술 확보 경쟁 심화 ㅇ 일부 국가와 기업에서 보안 핵심 원천기술에 대한 기술적 우위 선점 ㅇ 북미,유럽, 표준화 단체 중심 국제 표준화 추진

5. 표준화 추진 전략 : 비대면 식원확인 기술

[전략적 중요도/국내역량]



[표준화 대응체계]



[표준화 필요성]

◦ **감염병 질병 시대 대응**
- 비대면 서비스 확산에 따라 비대면 신원 확인 관련 정책 및 기술 개발 증가

◦ **표준화 추진**
- KISA,ETRI, 금융보안원 등 정부(출연)기관과 SKT, 삼성 등 기업체에서 국내 표준화 우선 가능항목을 도출하고 추진 계획 수립 및 추진 모색

[표준화 단계]

국내	□과제기획↦□과제승인↦□개발↦□검토↦■표준채택
국제	□과제기획↦□과제승인↦□개발↦□검토↦■표준채택

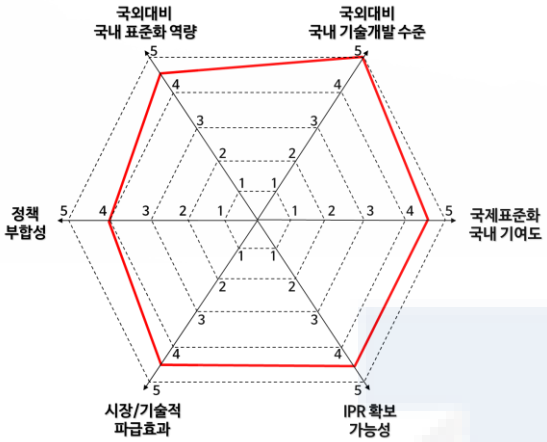
[표준화 전략]

◦ **국제 표준화 대응방안**
- (표준화 계획) FIDO는 2018년도에 ITU-T 국제표준으로 제정, 2019년도에 W3C 국제표준으로 제정되어, FIDO 기반 비대면 신원 확인 서비스의 확산 및 응용 기술 표준화 추진
- (국제표준화기구 활동) ITU-T SG17를 통해 화상회의, 원격 의료·교육 등 비대면 서비스의 신원 확인 기술에 대해서 학계, 기업과의 협력을 통해 응용 프로토콜 규격의 적극적인 표준화 활동 참여

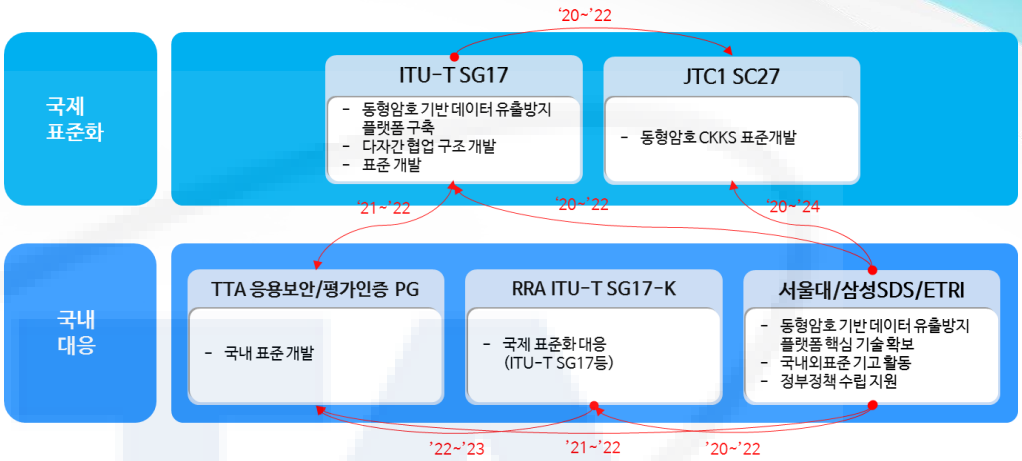
◦ **국내 표준화 추진계획**
- TTA 개인정보보호/ID관리, 블록체인 보안PG(PG502)에서 화상회의, 원격의료·교육 등의 비대면 신원 확인을 위한 요구사항과 공인인증서 이후의 다양한 신원 확인 기술의 상호운영성 확보를 위한 표준 개발 추진

5. 표준화 추진 전략 : 동형암호 기반 데이터유출 방지

[전략적 중요도/국내역량]



[표준화 대응체계]



[표준화 필요성]

◦ **동형암호의 활용**
- 동형암호는 암호화된 상태로 기계학습을 하는 분야에 주로 적용 중
- 개인정보보호와 더불어 다양한 영역에서 활용 가능

◦ **국제 표준화 추진**
- 산업계(삼성SDS)를 중심으로 연합학습 등의 응용서비스 발굴 및 표준화 추진

[표준화 단계]

국내	■과제기획↦□과제승인↦□개발↦□검토↦□표준채택
국제	□과제기획↦■과제승인↦□개발↦□검토↦□표준채택

[표준화 전략]

◦ **국제 표준화 대응방안**
- (표준화 계획) 비신뢰 사이버환경에서 민감정보의 유출없이 다자간에 협업을 가능한 데이터 처리를 가능하게 하는 동형암호 메커니즘을 기반으로 인공지능의 기계학습 분야에서 데이터의 분석 및 추론을 안전하게 수행할 수 있도록, 데이터 처리를 위한 플랫폼의 구조, 기능 및 운용조건등에 대한 지침에 대한 표준을 2022년 제정 목표
- (국제표준화기구 활동) ITU-T SG17에서 개발되고 있으며, 한국에서 주에디터를 맡고 있으며, 이를 통하여 동형암호기반의 응용서비스 및 플랫폼 분야의 국제표준 선도경쟁을 목표중

◦ **국내 표준화 추진계획**
- ITU-T SG17 국제표준 제정과 병행하여 TTA 응용보안 PG(PG504)에서 관련 표준화 추진


Q&A