글로벌 ICT 표준 컨퍼런스 2023

Global ICT Standards Conference 2023

(세션5) 사이버보안: 신뢰성 있는 디지털 환경 구축

글로벌 시장 주도권 확보를 위한 차세대 보안 표준화 로드맵

진승헌 책임연구원, ETRI

주최 과학기술정보통신부 Ministry of Science and ICT 특허청 Korean Intellectual Property Office
주관 국립전파연구원 National Radio Research Agency TTA IITP KEA kista ETRI

Index

01. 기술 개요

차세대보안 기술은 全산업의 초연결화·디지털화·지능화되는 환경에서 위/변조, 유출, 해킹, 서비스 거부 등을 비롯한 각종 불법 행위로부터 전달·저장되는 정보를 안전하게 보호하고, 물리적 공간에서의 보안 침해사고를 방지하기 위한 기술로 정의

<차세대보안 분야 개념도>

<기술분류>

-전통적인 보안기술을 정보 보안(암호, 디지털 ID 관리, 데이터 보안, 시스템 및 디바이스 보안, 네트워크 보안, 응용서비스 보안, 시험·평가)

-물리적 공간에서의 보안을 물리 보안(휴먼/바이오 인식, 영상 보안)

-ICT 기술과 밀접한 융합이 필요한기술을 융합보안으로분류(인공지능, 메타버스, 제로트러스트 및 공급망, 우주·항공, 선박·해양 등에서의 보안)

02. 표준기술 분류

중분류	소분류	요소 기술
정보 보안	암호	암호 설계, 암호 분석
	디지털 ID 관리(인증/인가)	범용 인증, 바이오 기반 인증, ID 관리 및 접근 제어
	데이터 보안	데이터 비식별화, 디지털 저작물 침해/권리 보호
	시스템 및 디바이스 보안	보안 취약성 분석, 침해 사고 대응, 서버 및 플랫폼 보안, 디지털 포렌식, 디바이스 보안
	네트워크 보안	사이버 위협 분석 및 대응, 유선 네트워크 보안, 무선 및 이동 통신 보안, 클라우드 및 에지 보안
	응용 서비스 보안	웹 보안, 이메일 보안, 전자화폐 보안, 블록체인 보안, 전자거래 보안
	시험 · 평가	IT제품 보안성 평가, 암호모듈 시험평가
물리 보안	휴먼/바이오 인식	바이오인식 센서, 바이오인식 알고리즘, 휴먼/바이오 인식 응용, 반려동물/바이오 인식 응용
	영상 보안	영상 시스템 보호, 지능형 영상분석, VMS/통합 관제 및 연동, 영상 보안 응용 서비스
융합 보안	인공지능 보안	인공지능 서비스 보안, 인공지능 보안 위협 분석 및 대응
	메타버스 보안	메타버스 인증 및 프라이버시 보호, 메타버스 플랫폼 및 디바이스 보안
	제로트러스트 및 공급망 보안	SW/HW 유통 보안, 데이터 유통 보안
	우주 · 항공 보안	무인항공기 시스템 및 통신 보안, UAM 인프라 및 기체 보안, 위성/지상 통신 보안, 위성 간 링크(ISL) 보안
	선박 · 해양 보안	스마트 선박 내부 보안, 선박/항만 통신 보안, 스마트 선박 인프라 통신 보안
	사물인터넷	IoT 디바이스 보안, IoT 서비스 보안
	스마트시티 보안	홈 · 시티 디바이스 보안 및 제어, 홈 · 시티 데이터 프라이버시
	스마트 모빌리티 보안	V2X 통신 및 응용 서비스 보안, 커넥티드카 침입 탐지 및 방지, URLLC를 지원하는 C-V2X 보안
	헬스케어 · 의료 보안	헬스케어 디바이스 · 센서 보안, 의료 데이터 보안 및 공유, 스마트헬스 시스템 및 서비스 보안
	산업 제어 시스템 보안	스마트공장 보안, 기반시설 보안, 스마트 에너지 보안

03. 주요 동향(국내 정책)

- 한미 전략적 사이버안보 협력 프레임워크 채택(2023.4.) 및 한미 사이버보안 공동지침 발표(2023.6.)
  * 사이버공간에서의 안정성을 향상시키고, 국제법상 각자의 의무 준수와 국제적으로 인식되는 사이버공간에서의 책임있는 평시 국가 행동의 자발적 규범을 존중, 장려함을 위한 협력

- 개인정보보호법 전면 개정(2023.3.)
  * 전 세계적인 디지털 대전환 추세에 따라 ▲데이터 경제 견인, ▲국민 개인정보 신뢰 사회 구현, ▲글로벌 스탠다드에 부합하는 개인정보 제도 전면 개정

- '대한민국 디지털 전략' 발표를 통한 6대 디지털 혁신 기술 분야의 연구개발 집중 투자 추진(2022.9.)
  * ① 인공지능, ② 인공지능 반도체, ③ 5G/6G 이동통신, ④ 양자, ⑤ 확장가상세계, ⑥ 사이버보안

- 사이버보안 역량 강화, 디지털 인증 활성화 등 120대 국정과제 발표(2022.7.)
  * 세계 최고의 네트워크 구축 및 디지털 혁신 가속화를 위하여 정보 역량 강화 및 디지털 인증 활성화 추진 예정

- 사이버보안 등 10개, 국가 필수 전략 기술 선정 발표(2021.12.)
  * 지속적으로 해킹 공격이 발생하고 네트워크 환경이 진화하고 있어, 사이버보안은 디지털사회 필수 안전장치로서 경제 · 안보 인프라 보호를 위해 자립화가 필수적인 기술 분야로 선정

03. 주요 동향(국외 정책)

- 미국, 적대적 머신러닝 및 사이버보안 관련 보고서 발표(2023.4.)
  * (1) AI 취약성에 대한 기존 사이버보안의 확장, (2) 정보 공유 및 조직의 보안 마인드 개선, (3) AI 취약성의 법적 지위 명확화, (4) AI보안 향상을 위한 효과적인 연구 지원
- 미국, IoT를 위한 사이버보안 보고서 발표(2023.4.)
  * 사이버보안 위험에 대한 우려가 IoT의 성장 및 적용을 저해하는 것으로 보고, 이를 검증하여 IoT활성화 방안 모색
- 미국, 사이버보안 기술 선도를 위한 국가 최상위 사이버보안 R&D 추진 전략 발표(2019.12.)
  * 사이버보안 국가 행동계획(CNAP): 1)사이버보안 내 인간 역할 증진, 2)효율적 사이버보안 관련 위험 관리, 3)사이버 공격 대응 방법 구상, 4) 안전 · 보안 · 사생활 보호 통합형 사이버보안 체계 구축, 5)지속가능한 사이버보안 시스템 개발

- OECD, 디지털 보안 정책 프레임워크 발표(2022.12.)
  * ① 디지털 보안 위협 관리(Digital Security Recommendation, 발표 예정), ② 국가 디지털 보안 전략(Strategies Recommendation, 발표 예정), ③ 핵심 활동의 디지털 보안(Critical Activities Recommendation, 2019), ④ 제품 및 서비스의 디지털 보안(Products and Services Recommendation, 발표 예정), ⑤ 디지털 보안 취약성 관리(Vulnerabilities Recommendation, 발표 예정)의 권고안에 기초를 두고 작성
- EU, 사이버 위기관리 능력 강화 등을 위해 사이버보안 정책 및 군사 이동성 실행 계획 2.0에 대한 성명 발표(2022.11.)
  * 4가지 영역의 이니셔티브로 구성된 새로운 사이버 방어 정책을 통해 사이버 공격에 대한 예방, 탐지, 방어, 복구, 억제 능력을 향상할 계획

03. 주요 동향(국내외 시장 동향)

(국내 시장)

- 2023년 국내 보안 시장 규모가 7조 437억으로 전망됨

  * 2023년에는 4.8% 성장한 7조 437억 원, 2024년에는 3.8% 성장한 7조 3,127억대로 전망됨

- 2022년 사이버보안 시장은 코로나 펜데믹이 불러온 비대면 이슈와 그로 인한 재택 · 원격근무의 증가, 그리고 공공과 기업의 디지털 전환에 따른 투자 등의 수혜를 입어 성장

(국외 시장)

- 전 세계 사이버보안 시장, 2조 달러 규모 성장 가능

  * 전 세계 사이버 공격으로 인한 피해가 2025년까지 연간 약 10조 5,000억 달러에 이를 것으로 예상

- 사이버보안에서 인공지능(AI)의 비중이 지속적으로 증가, 글로벌 시장 규모가 2023년 224억 달러(약 30조 원)에서 2028년에는 606억 달러(약 80조 원) 규모로 성장할 것으로 예측

  * 글로벌 시장 조사업체 마켓앤마켓은 사이버위협 사례와 데이터 보호에 대한 관심, 와이파이 네트워크의 취약성 증가 등에 따라 AI 사이버보안 시장이 2023~2028년 연평균 성장률 21.9%를 기록할 것이라고 예상

(출처)

1) 보안뉴스, https://www.boannews.com/media/view.asp?idx=114044
2) 보안뉴스, https://www.boannews.com/media/view.asp?idx=114107
3) 데이터넷, https://www.datanet.co.kr/news/articleView.html?idxno=178642
4) 맥킨지, https://www.mckinsey.com
5) AI타임스, https://www.aitimes.com

03. 주요 동향(특허 동향)

〈주요국 특허 통계(2003~2023)〉

(단위: 건)

구분	한국(KR)	미국(US)	일본(JP)	유럽(EP)	중국(CN)	합계
2003	27	113	56	36	56	288
2004	28	162	101	38	73	402
2005	28	137	87	48	81	381
2006	34	148	81	49	109	421
			≈			
2013	51	200	41	50	358	700
2014	62	203	65	46	384	760
2015	79	273	59	58	530	999
2016	109	281	63	66	592	1,111
2017	175	283	65	60	661	1,244
2018	185	369	77	60	810	1,501
2019	161	369	80	52	754	1,416
2020	155	307	50	41	816	1,369
2021	89	226	32	19	1,076	1,442
2022	14	66	10	2	602	694
2023	0	5	0	0	51	56
합계	1,376	4,061	1,248	832	8,009	15,526

- 중국의 경우, 정보 보안 강화에 대한 국가차원의 장려책과 TECENT, ALIBABA와 같은 전자상거래 플랫폼 업체의 관련 기술 개발에 힘입어 최근 들어 더욱 가파르게 특허출원이 증가하고 있음. 다만, 일부 글로벌 기업을 제외하고는 자국 내에서만 활동하는 출원인이 대부분(80% 이상)을 차지함

- 두 번째로 출원량이 많은 미국은 2003년부터 매년 100건 이상의 꾸준한 출원을 보이고 있으며, 75% 이상의 출원인이 해외 시장에도 진출하는 것으로 나타남

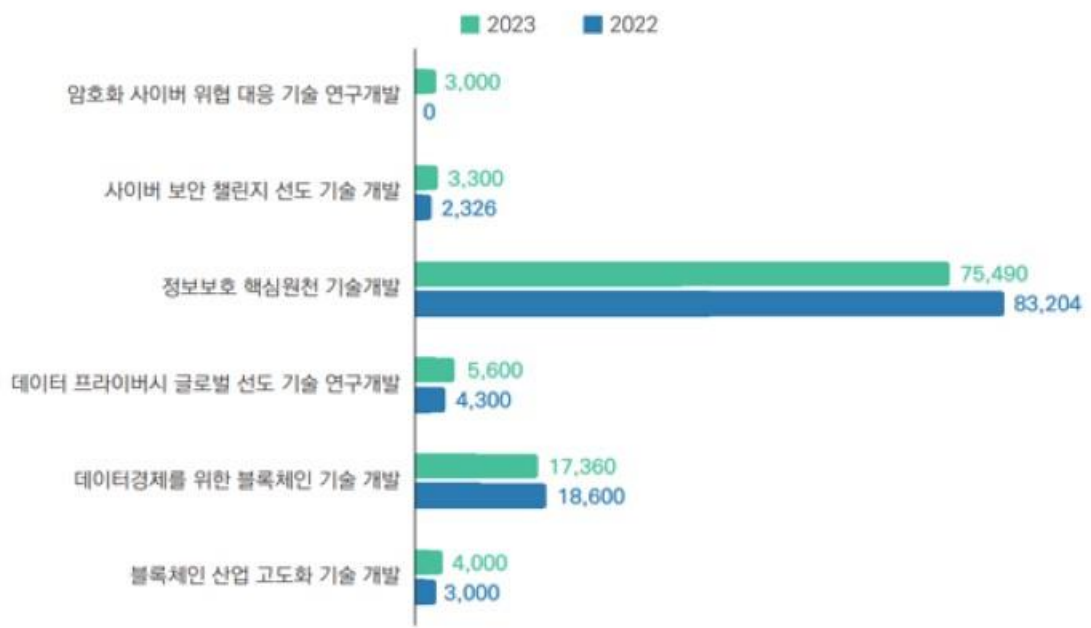
- 한국(8.9%)과 일본(8.0%)은 비슷한 특허출원 양상을 보이고 있으며, 미국과 중국 대비 시장 규모가 작아 상대적으로 낮은 관심도를 가지고 있는 것으로 분석됨

01. 기술 현황

구분	상대 기술 수준(100%)				
	한국	미국	일본	중국	유럽
기술 수준	85	100	80	80	90

※ 기술 수준은 "ICT 기술 및 표준 수준 조사" 설문조사에 의한 결과 활용

〈 보안 분야 정부 R&D 투자 현황('22~'23년) 〉



01. 기술 현황 - 국내

- (암호) 신규 ICT 환경보호를 위한 경량/고속/양자내성 범용 알고리즘 개발과 민감 정보를 포함하고 있는 데이터를 안전하게 처리하기 위한 활용성 강화 암호(동형암호 등) 개발 중
- (디지털 ID) 메타버스 등 新 플랫폼을 위한 인증기술의 연구시작 단계
- (데이터보안) 비식별화, 암호화 등을 통한 데이터 프라이버시 보호를 기반으로 데이터 활용성 강화 및 콘텐츠 저작권 보호 기술 개발 추진 중
- (시스템 및 디바이스보안) 취약점에 대한 버그바운티와 관리 방안에 대한 중요도 및 호스트 기반의 침해사고 대응 수요가 증가함에 따라 이에 대한 연구 개발이 추진 중
- (네트워크보안) 랜섬웨어 공격 대응, 인공지능 기반 지능형 보안관제 기술 및 근거리 무선 통신망을 포함한 5G 이동통신망과 클라우드 및 엣지의 융합 필요한 보안을 위한 다양한 기술 개발 추진 중
- (응용보안) 웹 보안, 이메일 보안, 전자화폐 보안, 블록체인 보안, 전자거래 보안 등의 다양한 기술들로 구성되어 있으며, 일상과 밀접한 관계를 갖는 서비스로 기술 개발 추진 중
- (시험평가) 인증기관과 평가기관, 제품 개발업체에서 정보보호시스템과 네트워크 장비의 국가·공공기관에 도입 시 필요한 평가 기술 및 기준 공동 개발 중
- (휴먼/바이오인식) 디지털ID 기술과 결합되어, 비대면 인증, 헬스모니터링 등에 적용되고 있으며, 최근 반려동물 개체식별로도 활용 중
- (영상보안) 영상정보 오남용 방지를 위한 On-CCTV 자율보호 체계 및 자유로운 기술 적용 확대를 위한 개방형 영상보안플랫폼 등에 대한 기술 개발이 추진 중

01. 기술 현황 - 국외

- (암호) NIST 국제 공모사업 중심으로 경량/양자내성 암호기술 확보 중, 블록체인, 클라우드 등 새로운 응용 환경 및 서비스를 대상으로 가용성/보안성 강화를 위한 암호 원천기술 개발 확대 중
- (디지털ID) 사용자의 디지털 신원과 자산 보호를 위한 새로운 패러다임의 인증 신기술이 도입되어 서비스 중이며, 디지털 지갑 기술의 활용 증가 추세
- (데이버보안) 개인 데이터 프라이버시 강화에 따라 차등 프라이버시, 신뢰·보안 컴퓨팅 등 암호/시스템기술과 디지털 콘텐츠, 생성형 AI 모델 저작권 보호의 제도적 대응 기술 개발 진행 중
- (시스템 및 디바이스 보안) 취약점의 버그바운티 관련 산업 발전 중, 가상화 관련 취약점 대응 체계와 위협 최소화 연구, 여러 기기의 데이터를 통합하고 연관 분석 디지털 포렌식 연구 진행 중
- (네트워크보안) ML/AI 기술을 적용한 네트워크 보안 제품 개발과 근거리 무선 통신망을 포함한 5G 이동통신망과 클라우드 및 엣지의 융합 필요한 보안 기술 연구 중
- (응용보안) 미래의 사이버공간의 서비스 보안과 밀접한 관계를 갖는 분야로 최근 국외 선진국은 Web 3.0 등에 대한 기술 개발을 추진 중
- (시험/평가) 보안성 평가 및 암호모듈 시험평가 관련 국제표준을 JTC1 SC27에서 개발 중
- (휴먼/바이오인식) 미국·유럽 등 주요 선진국에서는 바이오인식 센서부품·위변조 탐지 및 성능시험 기술 등의 원천기술을 개발, 생체신호 인증기술을 의료·국방분야에 활용 중
- (영상보안) 영상내에서 발생하는 전반적인 상황을 이해·묘사하고 징후를 감지하는 기술 연구와 고화질 CCTV 급증에 따른 AI 서버 부담 경감을 위한 고성능 SoC 내장 제품 개발 증가

01. 표준화 현황

구분	상대 표준 수준(100%)				
	한국	미국	일본	중국	유럽
표준 수준	80	100	80	80	90

※ 표준 수준은 "ICT 기술 및 표준 수준 조사" 설문조사에 의한 결과 활용

01. 표준화 현황 - 국내

구분	표준화 기구	주요 내용
단체 (TTA)	지능형 CCTV PG(PG427)	• 지능형 CCTV 시스템/데이터 보호를 위한 보안 프레임워크 및 비식별화, 분석된 메타정보 저장, 협업을 위한 포맷/인터페이스, 이종/다중 영상시스템간 표준 연동을 위한 규격 등을 정의
	정보보호기반 PG (PG501)	• 양자내성 암호를 포함한 범용 암호 알고리즘 규격 및 운용 기술 표준화 추진
	개인정보보호/ID관리, 블록체인 보안 PG (PG502)	• ID 관리(객체 식별, 본인확인, 인증, 접근제어) 기술, 블록체인 보안 기술, 디지털 거래 보안 기술, 비식별 프레임워크 및 검증자 확인을 위한 상호인증 분산ID 프레임워크 표준화 추진
	사이버보안PG (PG503)	• 클라우드 컴퓨팅, 미래인터넷 등 네트워크 보안기술, 사이버 보안기술 (해킹대응, 악성코드, 스팸대응 등), 사이버 범죄 대응기술 (역추적, 디지털 포렌식 등)에 관한 국내 표준기술 개발
	응용보안/평가인증 PG(PG504)	• 정보보호관리체계(ISMS), 공통평가기준(CC), 암호모듈검증(KCMVP) 등 보안성 인증 및 평가기술에 대한 표준화 진행
	바이오인식 PG (PG505)	• 모바일 바이오인식 전자금융서비스, 바이오정보 보호기술, 바이오인식시스템 성능 및 시험, 생체신호 기반의 텔레바이오인식 서비스, 바이오인식기반의 개체식별기술에 대한 표준화 진행
	메타데이터PG (PG606)	• 유통·활용 데이터 점검 방법, 학술자료 이미지 저작권 검증을 위한 메타데이터 및 DOI 등록 및 관리를 위한 메타데이터 등의 국내 표준화 추진
	블록체인기반기술 프로젝트그룹 (PG1006)	• 블록체인 데이터 분석 프레임워크 인터페이스 요구사항, 검증가능한 크리덴셜 기반 사용자 신원확인을 위한 프로파일 및 분산 식별자 기반 모바일 운전면허증 규격 등의 국내 표준화 추진
포럼	한국바이오인식협의회 (KBID)	• 민간분야 휴먼대상의 바이오인식시스템 성능시험 및 응용서비스, 민간/공공분야 반려동물 대상의 바이오인식기반 개체식별기술 및 성능시험인증서비스 표준화 추진
	분산원장기술 표준 포럼	• 분산원장기술 분야의 국내외 표준 개발 및 확산을 목적으로 하는 포럼으로, 분산원장 기반 자기주권적 ID 기술에 대한 국내외 표준 개발 중

01. 표준화 현황 - 국외

구분	표준화 기구		주요 내용
공식	ITU-T	SG17	**(Security)** ITU-T SG17은 ITU-T의 모든 스터디 그룹에서 추진하는 보안 관련 작업에 대해 전반적인 관여하며, 타 표준개발기구 협력을 통한 보안 관련 표준화 추진 - 사이버 보안, 보안 관리, 보안 아키텍처 및 프레임워크, 스팸 방지, ID 관리, 개인 식별 정보 보호, 데이터 보호의 운영 측면, 개방형 ID 신뢰 프레임워크, 양자 기반 보안 관련 표준화 추진 - 또한 사물 인터넷(IoT), 스마트 그리드, 스마트폰, 소프트웨어 정의 네트워킹, 웹 서비스, 빅 데이터 분석, 소셜 네트워크, 클라우드 컴퓨팅, 모바일 금융 시스템, IPTV, 분산 원장 기술을 위한 애플리케이션 및 서비스의 보안 관련 표준화 추진 중
		SG9	**(Broadband cable and TV)** 통합 광대역 네트워크로서 주로 텔레비전 및 사운드 프로그램을 가정으로 배포하기 위해 설계된 케이블 및 하이브리드 네트워크 관련 표준화 추진
	ISO/IEC JTC 1	SC 27	**(Information security, cybersecurity and privacy protection)** 보안 요구 사항 캡처 방법론, 정보 보안 관리 시스템, 보안 프로세스, 보안 통제/서비스, 신원 관리, 생체 인식/프라이버시, 정보보안 관리 시스템 분야의 적합성 평가, 인증/감사 요구사항 및 암호 원천기술(동형 암호, 양자내성 암호, 경량 인증 암호화, 다자간 계산 등) 등에 관한 표준화 추진
		SC 37	**(Biometrics)** 응용 프로그램과 시스템 간의 상호 운용성 및 데이터 교환을 지원하기 위한 생체인식 관련 용어/인터페이스/데이터 호환규격/표준적합성 시험/응용서비스/시스템 성능 시험기술 및 프라이버시 보호정책 등에 대한 표준화 추진
	ISO	TC 307	**(Blockchain and distributed ledger technologies TC)** 분산원장에서의 프라이버시 및 PII 보호 고려사항에 대한 기술보고서가 2020년 완료되었으며, 분산원장기술(DLT) 기반 분산 ID와 식별자 등에 대한 표준 개발 중
		TC 171	**(Document management applications)** 캡쳐/인덱싱/스토리지/검색/분포/표현 등 문서 관리 어플리케이션 기술 및 프로세스와 관련된 표준화

01. 표준화 현황 – 국외(사실)

구분	표준화 기구	주요 내용
사실	ABC	**(EXCO 집행위원회 그룹)** 아시아 8개국 지역의 지문·홍채 등 바이오인식제품에 대한 성능시험 및 표준적합성 상호인정 시험기술 사실표준을 개발하여 제품 호환성 검증을 진행 중임
	IETF	**(Security Area)** TLS, IPsec, MLS 등 주요 암호 프로토콜 규격 및 암호 알고리즘 적용 방법에 대한 표준화 추진 중
	IRTF	**(CFRG/Crypto Forum)** 암호 프로토콜에서 사용할 수 있는 공통 기반 암호기술 및 운용 가이드라인에 대한 표준화 추진 중
	3GPP	신규·진화된 서비스, 특징, 수용성 및 식별성을 고려한 전반적인 서비스(SA1) 및 3GPP 시스템의 요구사항 정의, 그리고 보안과 프라이버시를 위한 구조와 프로토콜 명세 등의 표준화 추진
	EUDI ARF	EU 신원지갑의 정의 및 목적과 생태계를 정의하고 PID 및 (Q)EAA 발급 요구사항과 아키텍처와 참조 레퍼런스 개발 추진
	W3C	웹 애플리케이션(자바스크립트)을 통해 생체인식, 보안토큰 등 다양한 인증 수단을 활용하기 위한 웹 인증(Web Authentication), 분산 ID의 핵심 아키텍처 및 데이터 모델 등, 검증 가능 크리덴셜 데이터 모델 등의 표준화 추진
	FIDO Alliance	패스워드를 대체하여 다양한 인증 수단을 수용할 수 있는 개방형 표준을 개발하는 조직으로, 인증 제품의 표준 적합성, 보안성, 생체인식 성능 등을 평가하기 위한 표준화 추진
	NIST	NIST는 암호모듈 시험기관으로 사이버 보안 개선, 사이버보안 및 위협관리 프레임워크, IoT 사이버보안 등의 표준화 추진 중하고 있으며, 최근 CNSA 2.0이 발표됨에 따라 신규 암호 알고리즘에 대한 시험 방법을 개발 진행 중
	CCRA/CCUF	보안성 평가를 위한 공통평가기준(CC)와 평가방법론(CEM)에 대한 표준 개발, 개정, 배포하고 있으며 ICT 환경의 변화에 따른 새로운 기술의 제품 평가를 위한 보호프로파일와 보조문서 지속적 개발 중
	OSSA	안드로이드 기반 영상보안시스템의 보안 프레임워크 및 영상분석 앱과의 데이터 표준 교환을 위한 API 정의 등의 표준화 추진

01. 표준구조모델 – 표준구조모델 개발 방법론

- (분류체계 후보군 조사) 타기관 로드맵, 산업기술 분류체계 참조
  * ICT 표준화 전략맵 Ver.2023 차세대보안 분류체계, IITP 기술로드맵 및 국가과학기술표준 정보보호 분류체계, ICT R&D 기술분류체계('21.3. 기준) 등
- (분류체계 키워드 구조화) 조사된 분류체계 후보군을 대상으로 Top-down 방식으로 키워드 분류 및 구조화를 통한 기술 분류체계 수립
  * IITP 기술로드맵의 분류체계를 중심으로 전략맵 Ver.2023 차세대보안의 중점표준화항목을 고려하여 분류체계 수립
- (기술 분류체계 상세화) 전통적 보안 분야 기술분류체계를 중심으로 세부 기술을 상세화
  * 레벨1: 정보보안, 물리보안, 융합보안
  * 레벨2: 각 레벨1에 해당하는 세부 기술을 분산 배치
  * 시험/평가 등 보안분야의 모든 세부 기술에 적용되는 세부 기술을 통합하여 하나의 기술 단위로 통합
- (제외사항) 융합보안의 경우 표준구조모델의 기술분류로 도출을 하나, 표준조사 및 표준화 후보기술 도출 하지 않음
  * 융합 보안과 관련된 세부 기술은 보안 분야의 핵심 기술을 대부분 도입하는 수준으로 보안 관련 핵심 기술과 중복되는 기술이 많음

01. 표준구조모델(정보보안)(1/3)

분류1	분류2	분류3	분류4
정보보안	암호	암호 설계	범용 암호 알고리즘
			데이터 활용성 강화 암호
			암호 프로토콜 운용
		암호 분석	*암호 알고리즘 분석*
			암호 부채널 분석
			양자 컴퓨팅 기반 분석
	디지털 ID 관리(인증/인가)	범용 인증	-
		바이오 기반 인증	-
		ID 관리 및 접근제어	-
	데이터 보안	데이터 비식별화	-
		디지털저작물 침해/권리 보호	-
	시스템 및 디바이스 보안보안	*보안취약성 분석*	*SW 취약점 분석*
			HW 취약점 분석
		침해사고 대응	침해사고 탐지
			침해사고 대응
		서버 및 플렛폼 보안	운영체제 보안
			가상화 보안
			시스템 접근통제
		디지털 포렌식	데이터 수집, 처리, 분석
			인증
		디바이스 보안	IoT 디바이스 보안
			웨어러블 디바이스 보안

01. 표준구조모델(정보보안)(2/3)

분류1	분류2	분류3	분류4
정보보안	네트워크보안	사이버 위협 분석 및 대응	랜섬웨어 대응 스토리지 보안
			그룹 이동 서비스 보안
			지능형 사이버위협 분석
			보안정보 분석 및 로그 관리
			보안 관제 및 오케스트레이션
		유선네트워크 보안	경계보안
			보안 연결
			DDoS대응
		무선 및 이동통신 보안	이동 통신망 보안
			무선근거리통신망보안
			네트워크 슬라이싱 보안
		클라우드 및 엣지 보안	가상화 플랫폼 보안
			클라우드 보안 서비스
			소프트웨어 정의(SDN) 보안
			엣지 컴퓨팅 보안
			클라우드 인프라/서비스 보안
	응용서비스 보안	웹 보안	-
		이메일 보안	-
		전자화폐 보안	-
		블록체인 보안	-
		전자거래 보안	전자거래 이상 행위 탐지
			거래·사기 방지

01. 표준구조모델(정보보안)(3/3) + (물리보안)

분류1	분류2	분류3	분류4
정보보안	시험.평가	IT제품 보안성 평가	보안 평가 핵심 표준
			지원 표준
			응용 표준
			역량 기준 표준
			일반 시스템 보안 보증 및 프로세스
		암호모듈 시험평가	-
분류1	분류2	분류3	분류4
물리보안	휴먼/바이오인식	바이오인식 센서	-
		바이오인식 알고리즘	-
		휴먼/바이오인식 응용	휴먼인식 및 검색
			생체신호기반 텔레바이오 인증
		반려동물/바이오인식 응용	-
	영상 보안	영상 시스템 보호	영상 프라이버시 마스킹
			영상 경량 암복호
			영상 무결성 검증
		지능형 영상 분석	지능형 영상분석 메타데이터
			영상 컨텍스트 묘사 및 검색
		VMS/통합 관제 및 연동	개방형 영상보안플랫폼
			다종 영상시스템 연동 및 제어
		영상 보안 응용 서비스	대인 검색기
			수화물/화물 검색기
			알람 모니터링
			무인전자경비 서비스

01. 표준구조모델(융합보안)

분류1	분류2	분류3	
융합보안	인공지능 보안	인공지능 서비스 보안	
		인공지능 보안 위협 분석 및 대응	
	메타버스 보안	메타버스 인증 및 프라이버시 보호	
		메타버스 플랫폼 및 디바이스 보안	
	제로트러스트 및 공급망 보안	SW/HW 유통 보안	
		데이터 유통 보안	
	우주. 항공보안	무인항공기 시스템 및 통신 보안	위성/지상 통신 보안
		UAM 인프라 및 기체 보안	위성간 링크(ISL) 보안
	선박. 해양 보안	스마트 선박 내부 보안	스마트선박 인프라 통신 보안
		선박/항만 통신 보안	
	사물인터넷	IoT 디바이스 보안	
		IoT 서비스 보안	
	스마트시티 보안	홈·시티 디바이스 보안 및 제어	
		홈·시티 데이터 프라이버시	
	스마트모빌리티 보안	V2X 통신 및 응용 서비스 보안	URLLC를 지원하는 C-V2X 보안
		커넥티드카 침입 탐지 및 방지	
	헬스케어. 의료 보안	헬스케어 디바이스·센서 보안	의료 데이터 보안 및 공유
		스마트헬스 시스템 및 서비스 보안	
	산업제어시스템 보안	스마트공장 보안	기반시설 보안
		스마트 에너지 보안	

02. 국제표준화 발전 전망

- (암호) 양자내성 암호 알고리즘의 표준화 추진이 일부 진행 중이며, 동형 암호 알고리즘과 비밀 분산 기반 다자간 안전계산 기술의 표준화 진행 중
- (디지털ID) 메타버스 표준 개발은 현재 개념정립 단계이나 사용자-아바타의 식별·인증, 프라이버시 보호 등을 위한 요구사항 및 상호연동을 위한 표준화 추진 전망
- (데이터보안) 비식별 처리 기술과 처리 절차, 개인정보가 노출되지 않도록 비식별 처리된 데이터의 처리 수준에 대한 요구사항이 표준화되어 실제 데이터 수준을 측정하는 방법에 대한 표준화 전망
- (시스템 및 디바이스 보안) 넓은 범위의 기술, 프로세스, 방법을 다루기 때문에 암호화, 신원 인증, 접근 제어 등 다양한 측면을 포괄하는 통합적인 보안 표준 형태로 개발이 진행될 것으로 전망
- (네트워크보안) 사이버공간에서 발생하는 침해사고 및 취약점 등에 대한 AI 기반 자동 대응, 정보공유, 보안 오케스트레이션 등에 대한 표준화 추진
- (응용보안) Open API 기반의 안전한 핀테크 서비스 활용을 위한 표준개발을 시초로 오픈소스 공급망과 같은 표준 개발 추진 전망되며, 분산화를 지향하는 Web 3.0 과의 융합이 활발하게 진행 중
- (시험/평가) 암호모듈 탬퍼에 대한 기술개발 및 표준 필요하며, 클라우드 제품에 대한 기본적인 평가 프레임워크를 제공하기 위해 CCUF의 클라우드 기술작업반(CCitC)과 협력하여 가이드라인 개발
- (휴먼/바이오인식) 바이오인식 기술을 이용한 자율주행차의 바이오 트윈관련 표준화로 진화·발전될 전망이며 반려견·반려묘·종마의 종자관리 및 개체식별 기술에 대한 국제표준화 추진 중
- (영상보안) 미국, 유럽 등 선진국 중심으로 이기종 기기간 연계·협업을 위한 사실 표준, 기술 및 스마트시티 모델 표준화 개발 및 확대 추진 중

03. 시사점

- 양자내성 암호 활용 기술, 데이터 활용성 강화 암호 기술은 표준화 초기 단계이므로 양자내성 암호 알고리즘, 비밀 분산 기반 암호 알고리즘 분산 수행 기술과 같은 실용화 전망이 높은 분야 위주의 핵심 기술 조기 확보 및 표준화 필요
- 메타버스 新디지털 플랫폼 및 가상 융합 경제에서 발생할 수 있는 사이버범죄로부터 이용자를 보호하는 기술 개발 및 표준화 추진 필요성 증가
- 현재 데이터 전문기관에서 비식별 처리 후 전문인력에 의한 적정성 평가를 직접 수행하고 있으나 데이터 보증 수준에 따른 비식별 처리 결과에 대한 자동화 측정 기술을 통한 효율화 요구 증가
- 시스템 및 디바이스의 보안 수준이 향상되면서 보안 사고의 원인이 세밀화되고, 사람의 실수에 기반한 형태로 제어할 수 없도록 진화 중이며, 시스템 및 디바이스만의 보안 시각을 확장해 보안 환경 전체의 시각에서 바라보고 각 기술이 연계된 보안 표준의 개발이 필요
- 지능화된 사이버 공격에 대처하기 위해 AI 기반 사이버 공격 방어 기술 및 제로 트러스트 기반의 보안 인텔리전스 기술 개발 요구 증가
- 리눅스 재단의 오픈소스 활동을 필두로 금융권의 Open API, 공급망 그리고 OpenAI에 이르기까지 그 발전 속도가 빠르므로 조직적 대응이 필요하며, 탈중화/분산화 모델의 보급이 Web 3.0 진영에서의 개시로 인하여 기술/표준 개발 가속화가 예상
- 이종/다중 영상 보안 시스템 간 연계, 협업 및 에지 지능의 고도화를 통해 관련 정부부처, 스마트시티 등으로 확대

04. 표준화 대상 후보 기술

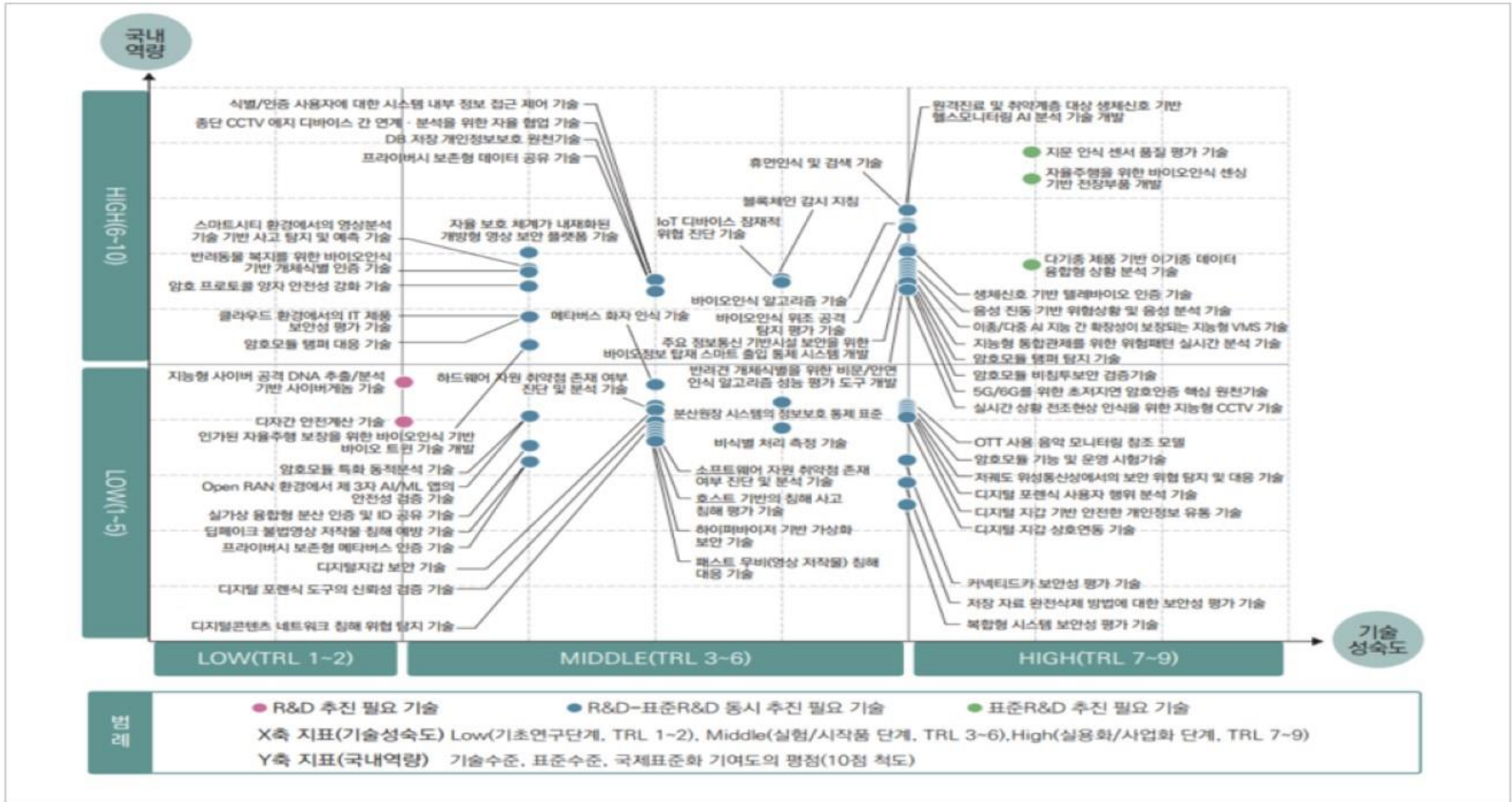
▪ 향후 5년 이내에 표준화 추진 가능성이 높은 기술 57개 선별(정보보안 46개, 물리보안 11개)

표준화 대상 후보 기술	
암호 (4)	다자간 안전계산 기술
	5G/6G를 위한 초저지연 암호인증 핵심 원천기술
	암호프로토콜 양자 안전성 강화 기술
	DB 저장 개인정보 보호 원천기술
디지털ID 관리 (인증/인가) (6)	디지털지갑 상호연동 기술
	디지털지갑 기반 안전한 개인정보 유통 기술
	디지털지갑 보안 기술
	메타버스 화자인식 기술
	프라이버시 보존형 메타버스 인증 기술
	실가상 융합형 분산 인증 및 ID 공유 기술
데이터 보안 (6)	비식별 처리 측정 기술
	프라이버시 보존형 데이터 공유 기술
	디지털콘텐츠 네트워크 침해 위협 탐지 기술
	딥페이크 불법 영상저작물 침해 예방 기술
	패스트 무비(영상저작물) 침해 대응 기술
	OTT 사용 음악 모니터링 참조 모델
시스템 및 디바이스 보안 (8)	하드웨어 자원 취약점 존재 여부 진단 및 분석 기술
	소프트웨어 자원 취약점 존재 여부 진단 및 분석 기술
	호스트 기반의 침해사고 침해 평가 기술
	하이퍼바이저 기반 가상화 보안 기술
	식별/인증 사용자의 시스템 내부 정보 접근 제어 기술
	디지털 포렌식 사용자 행위 분석 기술
	디지털 포렌식 도구의 신뢰성 검증 기술
	IoT 디바이스 잠재적 위협 진단 기술

표준화 대상 후보 기술	
네트워크 보안 (3)	Open RAN 환경에서 Third-part AI/ML 앱의 안전성 검증 기술
	저궤도 위성통신상에서의 보안위협 탐지 및 대응 기술
	지능형 사이버 공격 DNA 추출/분석 AI 기반 사이버계놈 기술
응용 서비스 보안 (2)	블록체인 감사 지침
	분산원장 시스템의 정보보호 통제 표준
시험/ 평가 (9)	암호모듈 탬퍼 탐지 기술
	암호모듈 탬퍼 대응 기술
	암호모듈 특화 동적분석 기술
	암호모듈 기능 및 운영 시험기술
	암호모듈 비침투보안 검증기술
	클라우드 환경에서의 IT 제품 보안성 평가 기술
	커넥티드카 보안성 평가 기술
	복합형 시스템 보안성 평가 기술
	저장자료 완전삭제 방법에 대한 보안성 평가 기술
영상 보안 (8)	자율 보호체계가 내재화된 개방형 영상보안플랫폼 기술
	이종/다중 AI지능간 확장성이 보장되는 지능형 VMS 기술
	실시간 상황 전조현상 인식을 위한 지능형 CCTV 기술
	다기종 제품 기반 이기종 데이터 융합형 상황 분석 기술
	스마트시티 환경에서의 영상분석 기술 기반 사고 탐지 및 예측 기술
	음성 진동 기반 위험상황 및 음성 분석 기술
	종단 CCTV 엣지 디바이스 간 연계-분석을 위한 자율 협업 기술
	지능형 통합관제를 위한 위험패턴 실시간 분석 기술

표준화 대상 후보 기술	
휴먼/ 바이오 인식 (11)	자율주행을 위한 바이오인식 센싱 기반 전장부품 개발
	반려동물 복지를 위한 바이오인식 기반 개체식별 인증기술 개발
	반려견 개체식별을 위한 비문/안면인식 알고리즘 성능평가도구 개발
	주요정보통신 기반시설 보안을 위한 바이오정보 탑재 스마트 출입통제 시스템 개발
	인가된 자율주행 보장을 위한 바이오인식 기반 바이오 트윈 기술 개발
	원격진료 및 취약계층 대상 생체신호 기반 헬스모니터링 AI 분석 기술 개발
	지문인식 센서 품질평가 기술
	바이오인식 위조 공격 탐지 평가 기술
	바이오인식 알고리즘 기술
	휴먼인식 및 검색 기술
	생체신호 기반 텔레바이오 인증 기술

04. 표준화 대상 후보 기술 검토



04. 표준화 대상 기술 선정

▪ 기존 R&D와 중복성 여부, 국제표준화 NP 채택 가능성 등을 고려하여 12개 기술 선정

표준화 대상 기술		세부 표준화 기술	비고
암호	다자간 안전계산 기술	다자간 분산 전자서명 생성 기법 표준, 암호 알고리즘 다자간 분산 수행 기법 표준	R&D 추진 필요 기술
	암호프로토콜 양자 안전성 강화 기술	범용 암호프로토콜 양자내성 암호 적용 표준 양자내성 암호 특화 암호프로토콜 표준	R&D-표준 R&D 동시 추진 필요 기술
디지털 ID 관리(인증/인가)	메타버스 화자인식 기술	메타버스 인증 서비스 요구사항 표준 메타버스 인증 기능적 모듈 및 연동 표준	R&D-표준 R&D 동시 추진 필요 기술
데이터 보안	비식별 처리 측정 기술	비식별 데이터 보증 요구사항 표준, 비식별 처리 측정 기술 표준발	R&D-표준 R&D 동시 추진 필요 기술
시스템 및 디바이스 보안	호스트 기반의 침해사고 침해 평가 기술	침해지표 관리 표준, 침해 평가 방법 표준	R&D-표준 R&D 동시 추진 필요 기술
네트워크 보안	지능형 사이버 공격 DNA 추출/분석 AI 기반 사이버게놈 기술	AI 사이버게놈 요구사항 표준, AI 사이버게놈 기능 구조모델 표준 AI 사이버게놈 데이터 포맷 표준	R&D 추진 필요 기술
시험/평가	암호모듈 탬퍼 대응 기술	암호모듈 침투공격 및 오류주입 대응 요구사항 표준 암호 칩 탬퍼 대응 요구사항 표준	R&D-표준 R&D 동시 추진 필요 기술
	클라우드 환경에서의 IT 제품 보안성 평가 기술	클라우드 환경에서 보안성 평가 가이드라인 클라우드 환경에서 보안성 평가 요구사항 표준	R&D-표준 R&D 동시 추진 필요 기술
휴먼/ 바이오인식	반려동물복지를위한바이오인식기반 개체식별인증기술개발	개체식별용 반려견·반려묘, 종마 바이오정보 DB 구축 지침, 바이오정보 보안관리 표준 바이오인식 기반 반려견·반려묘 종마 개체인증 성능시험 지침	R&D-표준 R&D 동시 추진 필요 기술
	안전한자율주행보장을위한바이오인식기반 바이오트윈기술개발	자율주행를 위한 바이오트윈 요구사항, 바이오트윈용 전자부품 기능 요구사항 표준 모빌러트 바이오트윈 프레임워크, 부품간 인터페이스, 모듈연동 및 통합검증 표준	R&D-표준 R&D 동시 추진 필요 기술
영상보안	자율 보호체계가 내재화된 개방형 영상보안플랫폼 기술	개방형 영상 프레임워크 표준, 지능형 VMS 표준 지능형 CCTV 통합관리 표준	R&D-표준 R&D 동시 추진 필요 기술
	스마트시티 환경에서의 영상분석 기술 기반 사고 탐지 및 예측기술	대규모 영상플랫폼간 연동 표준, 이기종 플랫폼간 연동 표준 대규모 영상플랫폼간 연동 성능평가, 대규모 플랫폼 분석 기반 위험 예측 표준	R&D-표준 R&D 동시 추진 필요 기술

01. 표준화 비전 및 목표

Vision

국제표준 선점을 통한 차세대보안 분야 기술 선도

		~2024	~2026	~2028
목표		• 바이오인식, 영상 보안 등 선도 표준 다수 확보 • 표준 선점을 위한 기술 개발 추진 • 국내 산 · 학 · 연 표준협력	• 데이터, 가상현실, AI 활용등에서 선도 표준 확보 • 개발 기술 기반 주요 표준 선점 • 국가 간 표준협력 전략	• 차세대보안 표준 선도 • 차세대보안 시장 선도 • 글로벌 표준협력 전략
추진 전략	정책/제도	• 산 · 학 · 연 표준협력 체계 정비	• 표준기술 활용을 위한 정책 마련	• 보안 기술 수출을 위한 정책 국제 공조
	기술 개발	• 데이터 보안, 가상현실 등에 필요한 보안 기술 개발 • 표준에 필요한 기술 개발 투자 확대	• 핵심 기술을 다양한 ICT에 결합한 융합 보안 기술 개발 • 우수 기술 공동개발을 위한 국제협력	• 차세대보안 글로벌 시장 선도
	표준 개발	• 바이오인식, 영상 보안, 전자화폐 보안 표준화 추진	• 데이터, 가상현실, AI활용 분야 등에서 국제표준 선점	• 우주, 항공, 해양 등 신규 ICT 보안을 위한 표준 개발

02. 표준화 대상 기술별 확보 전략(1/12)

❶ 다자간 안전계산 기술 (R&D 추진 필요 기술)

▪ (개요) 분산된 다수의 사용자들이 특정 함수의 계산에 참여할 때, 정확한 함수 결과값을 획득하면서 결과값을 제외한 다른 정보(다른 사용자의 입력값 등)를 알 수 없도록 보장하는 기술

▪ **(표준 필요성)**

- 블록체인과 같은 특정 응용 서비스에서 다자간 안전계산 기술이 효율적으로 활용되기 위해서는 기존 응용 서비스의 변화 최소화 및 계산 결과의 신뢰성을 보장 필요
- 다수 사용자가 독립적으로 참여하는 특정 암호 알고리즘 연산 결과의 신뢰성을 보장하기 위해 표준 필요

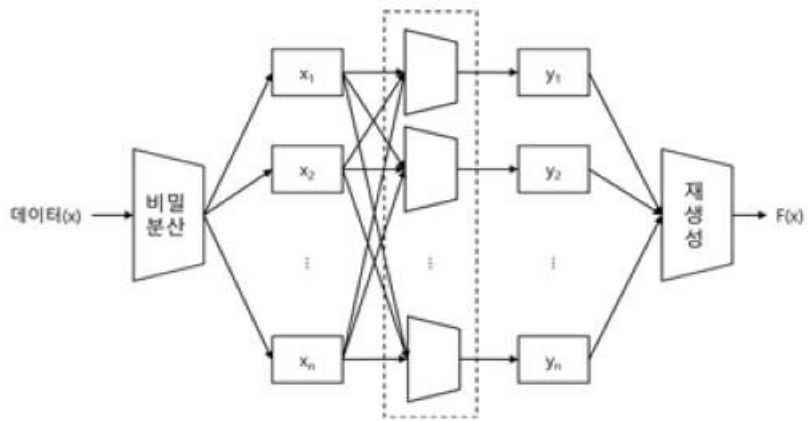
▪ **(기술 확보 전략)**

- 미국 NIST의 암호 알고리즘 다자간 분산 수행 기법 공모 제안 방식 분석 및 개선 연구 추진
- 다자간 안전계산 기술의 성능 개선에 특화된 요소 암호기술 식별 및 개발 추진

▪ **(표준 확보 전략)**

- JTC1 SC27 WG2와 IETF CFRG에서 국내 기업, 학계와의 협력을 통해 적극적인 표준화 활동 참여

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(2/12)

● 암호 프로토콜 양자 안전성 강화 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 양자 컴퓨팅 기술 발전으로 인한 사이버 환경의 응용 서비스 보안 위협에 사전 대응하기 위해, 핵심 기반 기술인 양자내성 암호 알고리즘의 운용 방식을 정의하는 기술

▪ **(표준 필요성)**

- 양자내성 암호의 응용 서비스 활용을 위해서는 암호 알고리즘의 규격뿐만 아니라 이를 운용하는 방법에 대한 규격의 표준화 필요
- 양자내성 암호 특성에 따라 암호 프로토콜 규격 변화도 필요할 수 있어, 안전성과 효율성, 신뢰성을 보장할 수 있는 암호 프로토콜에 대한 기술 개발 및 표준화 검토 필요

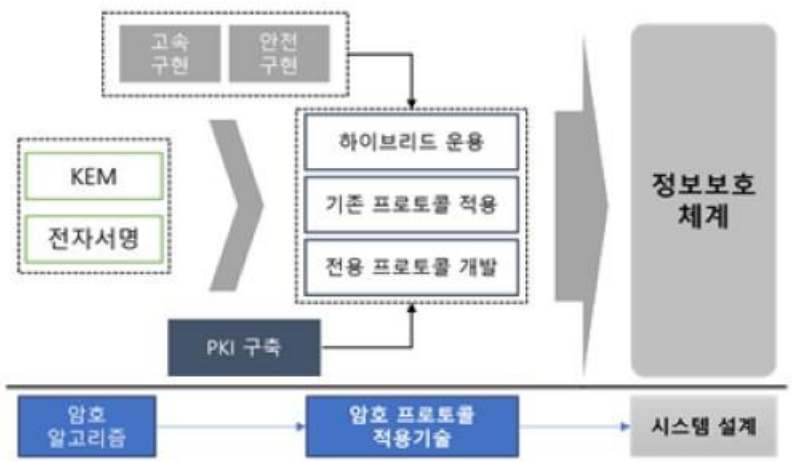
▪ **(기술 확보 전략)**

- 응용 서비스의 다변화 및 양자내성 암호 알고리즘 특성 등을 반영한 기존 암호 프로토콜 개선 및 신규 암호 프로토콜 설계 추진

▪ **(표준 확보 전략)**

- IETF에서 국내 기업과의 협력을 통해 적극적인 국제 표준화 활동 참여

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(3/12)

● 메타버스 화자 인식 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 메타버스의 가상세계 환경에서 사용자(아바타) 식별 및 인증 절차의 편의성 향상을 위해 아바타 간 소통 시에 활용되는 음성 데이터(텍스트 독립적 화자 인식)를 사용해 사용자(아바타)를 인증하는 기술

▪ (표준 필요성)

- 메타버스가 차세대 플랫폼으로 자리 잡을 근미래를 대비 메타버스 사용자에 대한 신뢰성 확보를 위한 다양한 신원 확인 기술 개발과 함께 관련 표준 개발이 필요

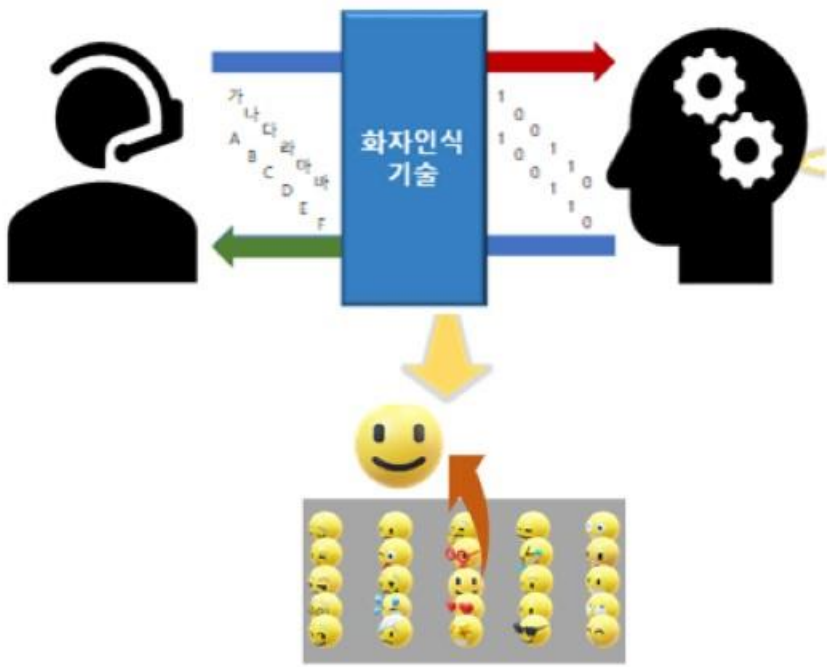
▪ (기술 확보 전략)

- 기존의 인증 인터페이스(키보드, 마우스 등)로는 메타버스 환경에서 인증에 적용하기에는 한계가 있으므로 음성과 함께 사용자(아바타)의 다양한 행위 등과 통합 인증 기술 개발

▪ (표준 확보 전략)

- TTA PG502 & 505에서 국내 표준 개발 주도
- JTC1 SC27 WG5(IDENTITY MANAGEMENT AND PRIVACY TECHNOLOGIES)에 관련 기고서를 지속해서 제출하고 발표를 통해 에디터쉽 확보

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(4/12)

● 비식별 처리 측정 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 다양한 기법으로 비식별 처리된 결과 데이터에 대한 비식별 수준을 측정하기 위한 검증 기술로서 비식별 정보의 안전성 평가 지표와 수준별 검증 지표, 비식별 정보의 위험도 평가 기술, 가명 정보 이용 추적을 위한 평가 기술

▪ **(표준 필요성)**

- 현재는 비식별 처리 결과에 대해 전문인력이 문서기반의 적정성 평가를 수행
- 데이터 처리 결과를 자동적으로 수준 측정하여 적정성 평가를 자동화하여 효율화하도록 하는 표준 필요

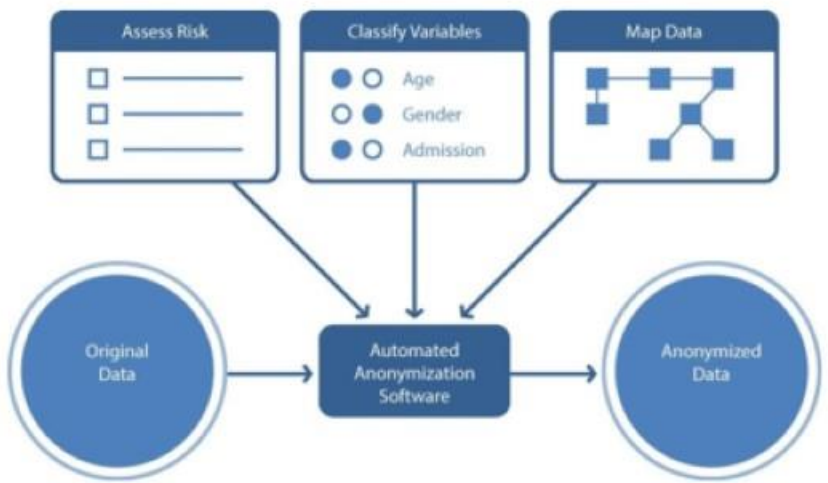
▪ **(기술 확보 전략)**

- 데이터에 대한 비식별 처리 기술보다는 처리된 결과의 비식별 보증 수준 요구사항에 부합하는 검증 방법에 대한 연구를 통해 표준화 요구사항을 구현

▪ **(표준 확보 전략)**

- ITU-T SG17에서 기존 비식별 표준화(X.1771, X.1148)를 통해 확보한 에디터쉽을 바탕으로 신규 권고안을 제안하여 신규 권고안 에디터쉽 확보

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(5/12)

● 호스트 기반의 침해 사고 침해 평가 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 침해 사고 로그와 익스플로잇 공격을 분석해 침해 지표를 생성하고 이를 체계적으로 관리하고 생성된 침해 지표를 기반으로 다수의 호스트에서 잔존 위협이 존재하는지 식별하는 기술

▪ **(표준 필요성)**

- 침해사고 대응 분야의 대부분을 차지하고 있는 CERT/관제는 드러난 위협만을 제거하는데 초점이 맞춰져 있음
- 사고의 재발방지를 위해 공격자의 대체 채널을 파악할 수 있도록 대상 호스트를 평가, 침해에 이용되었는지 식별 필요

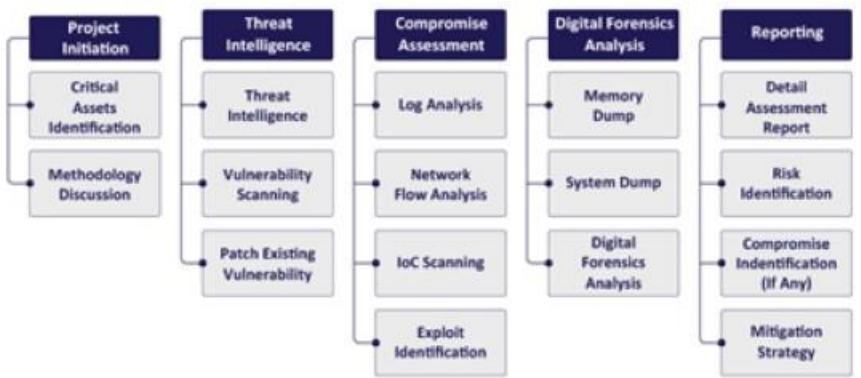
▪ **(기술 확보 전략)**

- 침해사고의 분석 데이터를 기반으로 해당 사고를 정의할 수 있는 고유한 침해지표를 생성하고, 이를 입력받아 호스트 상에서 간단히 진단할 수 있는 포터블 평가 도구 개발

▪ **(표준 확보 전략)**

- 자동화된 패치 관리와 취약점 스캐닝 등을 통해 시스템의 취약성을 최소화 가능,
- 침해지표 관리 및 침해 평가 방법 등의 표준을 TTA PG503에서 국내 표준 개발을 주도 필요

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(6/12)

● 지능형 사이버 공격 DNA 추출/분석 기반 사이버게놈 기술 (R&D 추진 필요 기술)

▪ (개요) 사이버상의 위협 분석 및 차단을 위해 네트워크 이상행위/공격패턴 DNA 데이터를 추출하고 분석하는 인공지능 기반 사이버게놈 기술

▪ **(표준 필요성)**

- 지능화된 사이버 위협에 능동적인 대처를 위하여 AI 기반 사이버 공격/방어 기술 및 정밀한 공격패턴 분석에 대한 표준 개발이 시급

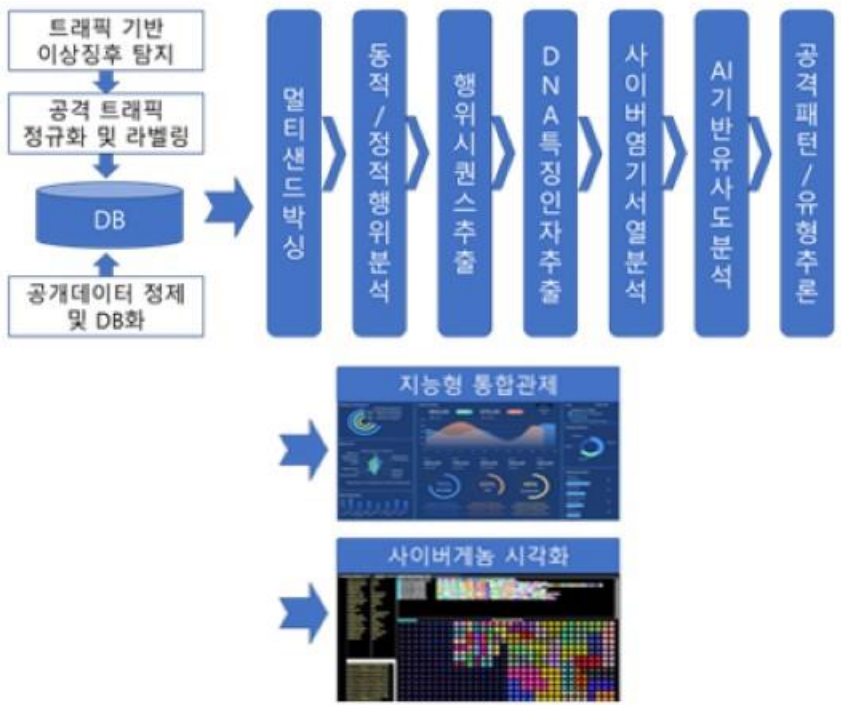
▪ **(기술 확보 전략)**

- 사이버상의 위협 분석 및 차단을 위해 네트워크 이상행위/공격패턴 데이터를 추출하고 분석하는 인공지능 기반의 새로운 보안 패러다임의 기술 개발

▪ **(표준 확보 전략)**

- ITU-T SG17에서 관련 기고서를 지속해서 제출하고 발표를 통해 에디터쉽 확보

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(7/12)

● 암호모듈 탬퍼 대응 기술 (R&D-표준 동시 추진 필요 기술)

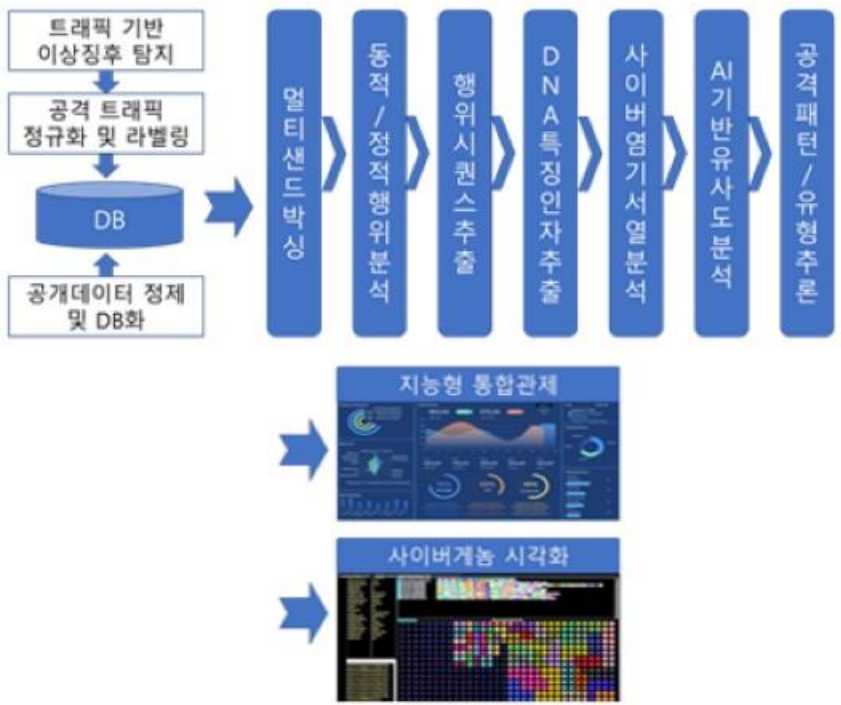
▪ (개요) 파손 유발, 프로빙 및 역공학으로 모듈을 파괴하여 정보를 획득하는 침투 공격 및 오류 주입, 클록/전압, 온도를 이용한 모듈의 일부 손상을 주는 준침투 공격에 대응하기 위한 기술

▪ **(표준 필요성)**
- 현재 표준인 ISO/IEC TS 30104의 경우, 개념 단계로만 존재하여 심도 있는 연구와 시험평가 요소 발굴 필요
- 기술적으로 부족한 IC 개발업체는 도태될 수밖에 없는 현실이므로 기술 우위와 선제 대응 필요

▪ **(기술 확보 전략)**
- 안전한 칩을 설계하고 검증하는 원천 기술 개발 추진
- 국가경쟁력 확보 및 기술 우위를 위한 선제대응 방안 마련

▪ **(표준 확보 전략)**
- TTA 응용보안/평가인증(PG504)에서 국내 표준 개발을 주도하고 JTC1 SC27 국제 표준화 활동 추진
- JTC1 SC27 WG3에 관련 기고서를 지속해서 제출하고 발표를 통해 에디터쉽 확보

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(8/12)

❶ 클라우드 환경에서의 IT 제품 보안성 평가 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 다양한 클라우드 토폴로지 환경(예를 들어, SaaS, IaaS, PaaS 등)에서의 IT 보안성 평가 기술

▪ **(표준 필요성)**

- 다양한 분야에서 클라우드 기술이 안전성과 신뢰성을 보장 받으며 효율적으로 활용되기 위해서는 기존의 평가인증 기술과 클라우드 기술의 융복합 필요

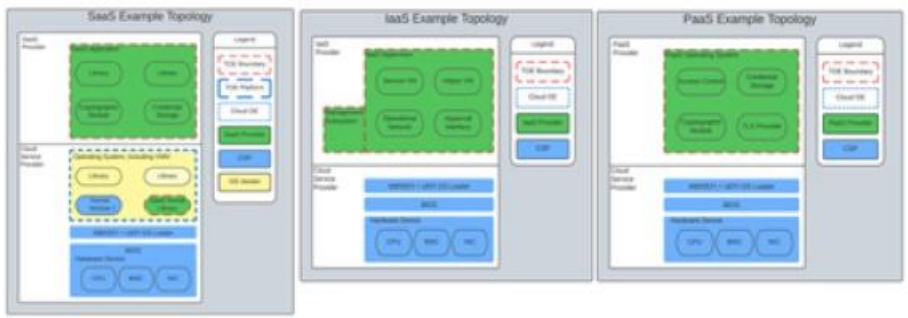
▪ **(기술 확보 전략)**

- 새로운 서비스보다는 기존에 추진하고 있는 비즈니스 모델에서 클라우드 기술을 활용한 보안 제품을 도입하려는 형태에서의 평가기술 개발

▪ **(표준 확보 전략)**

- CCUF의 CCitC 기술작업반, ISO/IEC JTC 1/SC 27/ WG 3에서 표준개발 주도 및 ISO/IEC 15408, 18045 국제 표준화 활동 추진

< 기술 개념도 >



*출처 : CC in the Cloud contribution to CC Roadmap TR7677

02. 표준화 대상 기술별 확보 전략(9/12)

❶ 반려동물 복지를 위한 바이오인식 기반 개체식별 인증 기술 (R&D-표준 동시 추진 필요 기술)

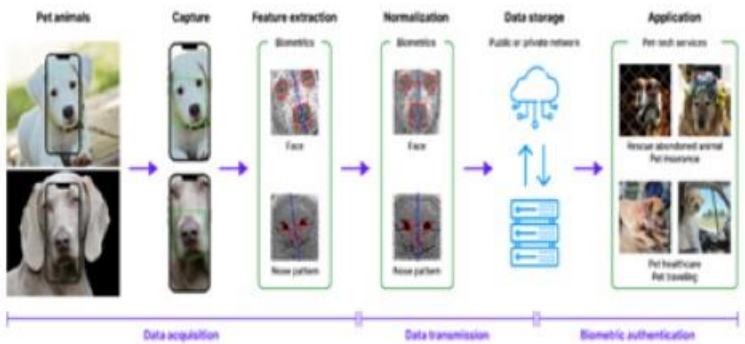
▪ (개요) 반려동물의 비문 · 안면 등 신체적 특징과 걸음걸이 · 생체신호 등 행동적 특징을 자동화된 IT 기술로 추출 · 저장하여, 다양한 IT 기기로 반려동물의 개체를 식별하는 기술

▪ **(표준 필요성)**
- 생체이식칩 부정적 인식, 외장형 목걸이 분실 등 현재의 반려견 개체식별방식으로 반려동물 사회적 문제해결 불가
- 비문 등 반려견의 신체적 유일성 특징을 이용하는 바이오인식기반 반려동물 개체식별 기술 및 표준 개발 필요

▪ **(기술 확보 전략)**
- 반려동물의 비문·안면 등 신체적 특징과 걸음걸이·생체신호 등 행동적 특징을 자동화된 IT 기술로 추출·저장하여, 다양한 IT 기기로 반려동물의 개체를 식별기술 개발

▪ **(표준 확보 전략)**
- 바이오인식 기반 반려동물 개체식별 기술 및 성능시험 기술에 대하여 TTA PG505 국내표준화 및 ITU-T SG17 Q10에서 국제표준화 활동 추진

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(10/12)

❶ 인가된 자율주행 보장을 위한 바이오인식 기반의 바이오 트윈 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 자율주행 차량인증 · 운전자 식별 및 건강상태 자동분석을 위한 지문 · 안면 · 홍채 · 음성 · 생체신호 인증 기술과 인포테인먼트 및 커넥티드 서비스 기술과 연계되는 바이오 트윈 기술

▪ **(표준 필요성)**

- 스마트카에 대한 차량탈취 및 불법주행, 운전자 위급상황에서의 안전한 자율주행 보장을 제공하기 위하여 지문·안면·홍채·음성·생체신호 등을 이용하는 바이오인식기반 바이오 트윈기술 연구개발과 병행하여 표준화 추진 필요

▪ **(기술 확보 전략)**

- 자율주행 차량인증·운전자 식별 및 건강상태 자동분석을 위한 지문·안면·홍채·음성·생체신호 인증기술과 인포테인먼트 및 커넥티드 서비스기술과 연계되는 바이오 트윈기술

▪ **(표준 확보 전략)**

- 바이오인식기반 바이오 트윈기술 및 바이오인증 성능시험 기술에 대하여 TTA PG505 국내표준화 및 ITU-T SG17 Q10에서 국제표준화 활동 추진

< 기술 개념도 >

02. 표준화 대상 기술별 확보 전략(11/12)

❶ 자율 보호 체계가 내재화된 개방형 영상 보안 플랫폼 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 누구나 접근가능한 안드로이드 기반 영상 보안 시스템의 자율방어 체계를 보장하고 실시간 영상위험의 온-디바이스 대응을 위한 자율방어 · 안전 초지능이 내재화된 개방형 영상 보안 플랫폼 기술

▪ **(표준 필요성)**

- 글로벌 사실 표준인 OSSA를 준용하는 영상보안 통합 프레임워크 표준화 기술 개발 및 다양한 보안분석 솔루션 개발, 성능 시험 등이 시급

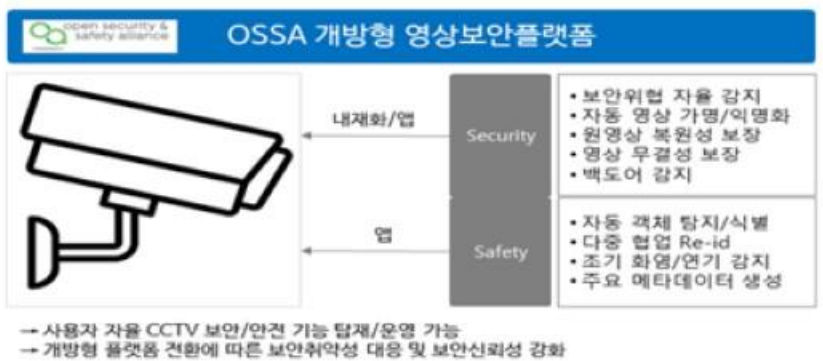
▪ **(기술 확보 전략)**

- 누구나 접근가능한 안드로이드 기반 영상보안시스템의 자율방어체계를 보장하고 실시간 영상위험의 온-디바이스 대응을 위한 자율방어·안전 초지능이 내재화된 개방형 영상보안 플랫폼 기술

▪ **(표준 확보 전략)**

- 국내 TTA 표준화 활동 추진을 통한 OSSA 글로벌 사실 표준개발 주도
- TTA PG427에서 OSSA 국내 표준화 추진 및 산업계 요구사항 추가 반영 추진

< 기술 개념도 >



02. 표준화 대상 기술별 확보 전략(12/12)

❶ 스마트시티 환경에서의 영상분석 기술 기반 사고 탐지 및 예측 기술 (R&D-표준 동시 추진 필요 기술)

▪ (개요) 스마트시티 단위에서 물리 보안 제품 간 연계 및 데이터 수집을 위한 연동표준기술을 개발하고, 이를 기반으로 수집되는 대규모 데이터를 통하여 실시간 위협을 예측 · 대응 및 사고발생 시 확산 방지를 위한 최적의 대응 방법을 찾는 지능형 플랫폼 기술

▪ **(표준 필요성)**

- 스마트시티 관련 다양한 특허들이 발생하고 있어, 대규모 영상분석 기술, 이기종 기기 연동기술, 사고확산방지 예측 기술 등 관련한 기술 개발 및 표준, 성능시험 등이 시급

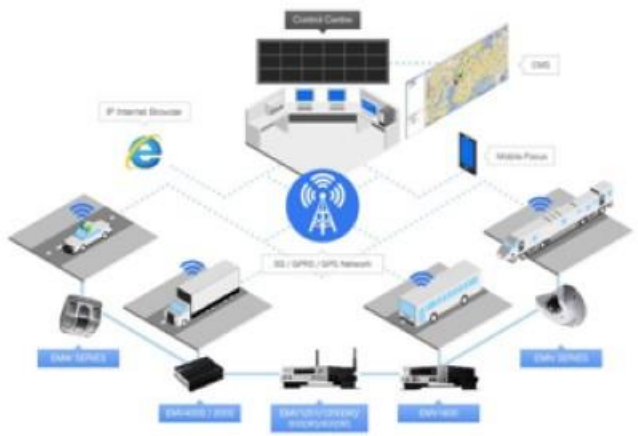
▪ **(기술 확보 전략)**

- 스마트시티 단위로 물리보안 제품간 연계 및 데이터 수집을 위한 연동표준 기술을 개발하고
- 이를 기반으로 수집되는 대규모 데이터를 통하여 실시간 위협을 예측·대응 및 사고발생 시 확산 방지를 위한 최적의 대응 방법을 찾는 지능형 플랫폼 기술

▪ **(표준 확보 전략)**

- 스마트도시표준화포럼(SCSF) 등에서 스마트시티 통합 관리 및 상호연동을 위한 표준화를 추진

< 기술 개념도 >



03. 표준화 로드맵

구분		2023	2024	2025	2026	2027	2028
다자간 안전계산 기술	기술	● 범용 다자간 안전계산 기술					
		● 암호 알고리즘 다자간 분산 수행 기술					
	표준	● 다자간 분산 전자서명 생성 기법 표준					
						● 암호 알고리즘 다자간 분산 수행 기법 표준	
암호 프로토콜 양자 안전성 강화 기술	기술		◑ 범용 암호 프로토콜 양자내성 암호 알고리즘 적용 기술				
		● 양자내성 암호 특화 암호 프로토콜 설계					
	표준		◑ 범용 암호 프로토콜 양자내성 암호 알고리즘 적용 표준				
				● 양자내성 암호 특화 암호 프로토콜 표준			
메타버스 화자 인식 기술	기술		◑ 텍스트 독립적 화자 인식 기술				
				○ 메타버스 환경 적응형 화자 인식 고도화 기술			
					○ 프라이버시 보존 음성 데이터 비식별화 기술		
	표준			◑ 메타버스 인증 서비스 요구사항 표준			
					◑ 메타버스 인증 기능적 모듈 및 연동 표준		
비식별 처리 측정 기술	기술	◑ 비식별 처리 검증 방법 기술					
		◑ 비식별 데이터 프라이버시 침해 위험 검증 기술					
				◑ 프라이버시 강화형 데이터 공유 기술			
	표준	◑ 비식별 데이터 보증 요구사항 표준					
			◑ 비식별 처리 측정 기술 표준				

(○: R&D 추진 필요 기술, ◑: R&D-표준 R&D 동시 추진 필요 기술, ●: 표준 R&D 추진 필요 기술)

03. 표준화 로드맵

구분		2023	2024	2025	2026	2027	2028
호스트 기반의 침해 사고 침해 평가 기술	기술		◑침해 지표 생성 및 관리 기술				
				◑침해 평가 항목 및 방법론			
					◑침해 평가 도구		
	표준		◑ 침해 지표 관리 표준				
				◑ 침해 평가 방법 표준			
지능형 사이버 공격 DNA 추출/분석 기반 사이버게놈 기술	기술		◑ 네트워크 위협 대응 AI 사이버게놈 기술				
					○ AI 사이버게놈 고도화 기술		
	표준		◑ AI 사이버게놈 요구사항 표준			◑ AI 사이버게놈 데이터 포맷 표준	
				◑ AI 사이버게놈 기능 구조 모델 표준			
암호모듈 탬퍼 대응 기술	기술		◑ 침투 공격 기반 암호모듈 탬퍼 대응 기술				
				◑ 오류 주입 기반 암호모듈 탬퍼 대응 기술			
				◑ 암호 칩 기반 탬퍼 대응 기술			
	표준			◑ 암호모듈 침투 공격 및 오류 주입 대응 요구사항 표준			
					◑ 암호 칩 탬퍼 대응 요구사항 표준		
클라우드 환경에서의 IT제품 보안성 평가 기술	기술		◑ 클라우드 환경을 위한 제품/서비스별 보안 위협 및 요구사항 및 분석				
				◑ 클라우드 환경을 위한 보안 기술			
					◑ 클라우드 보안 플랫폼 모델 정립		
	표준			◑ 클라우드 환경에서 보안성 평가 가이드라인			
					◑ 클라우드 환경에서 보안성 평가 요구사항 표준		
반려동물 복지를 위한 바이오인식 기반 개체식별 인증 기술	기술	◑ 비문 - 안면인식 기반 반려견 - 반려묘 개체식별 인증 서비스 기술					
			◑ 걸음걸이 등 바이오인식 기반 종마 개체식별 인증 서비스 기술				
				◑ 반려동물 개체식별 성능 시험 기술		○ 반려동물 개체식별 공인 시험 인증 서비스	

(○: R&D 추진 필요 기술, ◑: R&D-표준 R&D 동시 추진 필요 기술, ●: 표준 R&D 추진 필요 기술)

03. 표준화 로드맵

구분		2023	2024	2025	2026	2027	2028
반려동물 복지를 위한 바이오인식 기반 개체식별 인증 기술	표준	◑ 개체식별용 반려견 · 반려묘 바이오정보 DB 구축 지침		◑ 개체식별용 종마 바이오정보 DB 구축 지침		○ 반려견 · 반려묘 전생애주기 바이오정보 통합관리 표준	
		◑ 바이오인식 기반 반려견 · 반려묘 개체인증 성능 시험 지침		◑ 바이오인식 기반 종마 개체인증 성능 시험 지침			○ 종마 종자관리용 바이오정보 보안 관리 표준
인가된 자율주행 보장을 위한 바이오인식 기반의 바이오 트윈 기술	기술		◑ 자율주행을 위한 바이오 트윈 요구사항 분석		○ 모빌리티 바이오 트윈 플랫폼 모델 정립		
				◑ 모빌리티 바이오 트윈용 전자부품 기술			
					◑ 완전차량과 바이오 트윈 모듈 연동 기능 구현 및 통합검증		
	표준	◑ 자율주행을 위한 바이오 트윈 요구사항 표준			◑ 모빌리티 바이오 트윈용 전자부품 기능 요구사항 표준		
			◑ 모빌리트 바이오 트윈 프레임워크 표준			○ 모빌리티 바이오 트윈용 부품 간 인터페이스 표준	
					◑ 모빌리티 바이오 트윈 모듈 연동 및 통합검증 표준		
자율보호 체계가 내재화된 개방형 영상 보안 플랫폼 기술	기술		◑ 자율보호 내재형 개방형 영상 보안 플랫폼 기술				
				◑ 지능형 VMS 기술			
					◑ 예지 영상 지능 통합관리 기술		
	표준		◑ 개방형 영상 프레임워크 표준				
			◑ 지능형 VMS 표준		◑ 지능형 CCTV 통합관리 표준		
스마트시티 기반 물리 보안 데이터 연동 및 분석 기술	기술		◑이기종 데이터 기반 대응 기술				
				◑스마트시티 간 연계 및 분석 기술			
	표준	◑대규모 영상 플랫폼 간 연동 표준		◑이기종 플랫폼 간 연동 표준			
			◑대규모 영상 플랫폼 간 연동 성능 평가 표준		◑대규모 플랫폼 분석 기반 위협 예측 표준		

(○: R&D 추진 필요 기술, ◑: R&D-표준 R&D 동시 추진 필요 기술, ●: 표준 R&D 추진 필요 기술)

01

차세대 보안의 중요성

全산업이 초연결화/디지털화/지능화되는 ICT 환경의 안전성 확보를 위해서는 차세대보안기술 확보가 중요

02

표준 확보 전략 마련

개발된 우수 보안기술을 활용하기 위해서는 표준화가 필요하며 우리의 상황에 맞는 표준 확보 전략을 마련하는 것이 필요함

03

주요 이슈 대응체계 확보

코로나로 인한 비대면 서비스 증가, 가상현실 및 AI 활용 증가, 5G/6G 보급, 양자컴퓨터 등장, 악성코드 위협 증가 , 데이터 노출 위협 등에 대한 주요 기술 개발 방향과 연계

감사합니다.

진승헌 책임연구원, ETRI
jinsh@etri.re.kr