10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

ICT 미래혁신 표준 세미나: 디지털 혁신기술과 기반기술

AI 및 양자시대의 ICT 안전성 확보를 위한 사이버보안 표준화 전략

권대성 연구위원
ETRI 부설연구소

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA kista ETRI

Index

01 개요 및 현황

02 표준화 환경 분석 및 시사점

03 비전·목표 및 중점 표준화 항목

04 중점 표준화 항목별 추진 전략

00. Abstract

발표 요약

본 발표는 **차세대보안 분야의 국제표준 선점을 위한 중장기 표준화 전략**을 제시합니다.

1

기술 정의·분류체계

차세대보안 기술의 정의와 분류체계, 국내외 정책·시장·특허·기술·표준화 현황

2

환경 분석 · 시사점

SWOT 분석을 통한 표준화 추진 방향과 시사점 도출

3

비전 · 목표 · 전략

표준화 비전·목표와 7대 추진전략, 17개 중점 표준화 항목

4

항목별 추진 전략

중점 표준화 항목별 표준화 주요 이슈 및 표준 개발 내용

7대 추진전략

AI 사이버쉴드 돔 | 암호체계 | 디지털 ID·데이터 | 지능형 네트워크 | 시험·평가 | 휴먼/바이오인식 | 지능형 영상보안

01

SECTION 01

개요 및 현황

Overview & Current Status

01. 개요 및 현황

사이버보안 기술 정의

사이버보안 기술 전 산업의 초연결·디지털·지능화 환경에서 위·변조, 유출, 해킹, 서비스 거부 등 불법행위로부터 정보를 보호하고 물리적 보안 침해를 방지하는 기술

정보 보안

- AI 보안
- 암호
- 디지털 ID 관리
- 데이터 보안
- 시스템·디바이스 보안
- 네트워크 보안
- 응용 서비스 보안
- 시험·평가

물리 보안

- 휴먼/바이오 인식
- 영상 보안

물리 공간의 보안 침해 사고를 방지하고 생체·영상 기반으로 사람과 사물을 인식·보호

융합 보안

- 메타버스
- 제로 트러스트·공급망
- 우주·항공
- 선박·해양
- IoT·스마트시티
- 스마트 모빌리티
- 헬스케어·의료
- 산업제어시스템

01. 개요 및 현황

| 사이버보안 기술 정의 (계속)

AI 보안	AI 시스템 자체의 보안성 확보 + AI 활용 위협 탐지·대응·예방
암호	양자컴퓨팅 공격 대응, 민감정보의 기밀성·무결성·인증·부인방지 제공
디지털 ID 관리	분산ID, 디지털 신분증·지갑, PKI·MFA·FIDO 기반 신원확인·자격검증
데이터 보안	비식별화(가명·익명), 유출 방지, 디지털 저작물 권리 보호
시스템·디바이스	취약점 분석, 악성코드·랜섬웨어 대응, 서버·플랫폼 보안, 포렌식
네트워크 보안	유·무선/이동통신/슬라이싱, 클라우드·에지, 제로 트러스트 보안
응용 서비스	웹·이메일·전자화폐·블록체인·전자거래 보안
시험·평가	CC(15408)·18045, 암호모듈(19790)·24759 기준 지속 개선
휴먼/바이오인식	지문·안면·홍채·정맥·심전도 등 바이오정보 기반 인증·동물식별
영상 보안	CCTV 지능형 분석, 관제·추적·예측 및 영상 오·남용 차단

01. 개요 및 현황

| 추진 배경 및 필요성

글로벌 사이버보안 시장 ('21→'30)

$2,205억 → $5,016억

약 314조 → 715조 원 (Spherical Insights)

주요국, 사이버보안을 국가안보 직결 문제로 인식 → 정책 경쟁적 발표

미국	EU	영국	일본	중국
사이버전략 '26.3	사이버복원력법	국가 사이버전략	대응능력강화법	사이버보안법 개정

국내 「범부처 정보보호 종합대책」('25.10) — 1,600여 개 주요 IT 시스템 취약점 점검, AI 기반 탐지·망분리 개선·SW 공급망 보안·PQC 전환 등 차세대 보안체계 강화

글로벌 경쟁력 확보

- 급성장하는 사이버보안 시장에서 기술 우위와 보편적 시장 적용성 확보를 위한 국제표준화 요구

신기술 위협 선제 대응

- AI·양자 등 신기술 보안위협 식별 및 제로 트러스트·공급망 신규시장 확보를 위한 선제적 국제표준화

전략적 수단화

- 단순 기술 호환성을 넘어 국가안보·산업 경쟁력·글로벌 신뢰체계 선점을 위한 전략적 표준화

01. 개요 및 현황

AI 기반 보안 위협의 심각성

AI의 이중 위협 구도 현실화

공격의 도구 | 공격의 대상

공격 고도화 속도가
방어 발전 속도를 추월

AI 보안 시장 '24 $254억→'30 $938억
24.4% CAGR

주요 AI 기반 공격

자동화 피싱	딥페이크 인증 우회	LLM 사회공학	AI 생성 악성코드	Zero-day 탐지	적대적 공격·모델 도난	데이터 오염	피지컬 AI 융합공격

미국

첨단 AI 혁신·안보 행정명령('26.6)

NSA 등 정보기관 주도로 상용 첨단 AI 모델 출시 전 취약점 평가·탈옥 통제

국내

과기정통부·KISA AI 보안 위협 대응 매뉴얼 ('26.7)

AI 기반 사이버위협 단기 대책 및 기존 보안 체계의 AI 전환 추진, 중소기업 취약점 점검 등 보안역량 강화 (AI 레드티밍 가이드 병행)

국제표준

ITU-T SG17 Q16(AI Security) 신설

다중 에이전트 AI의 창발적·오정렬 행동 식별·완화 표준화 착수

01. 개요 및 현황

| 양자컴퓨팅 위협과 양자내성암호(PQC) 전환

양자 위협 공개키 암호(RSA·ECC) 무력화 가능성 + 지금 수집·향후 해독(Harvest Now, Decrypt Later) 노출 → 선제적 국가 암호체계 전환 시급

「양자 과학기술·양자산업 육성법」 개정('26.5) 국가기관의 양자 보안체계 구축 의무화(제18조의2)

주요국 PQC 전환 로드맵

구분	목표 시기	주요 내용
미국	2030 / 2031	EO 14412 — 암호 키 설정 2030, 전자서명 2031까지 PQC 전환 강제
EU	2035.12	NIS 협력그룹 공동 이행 로드맵(3단계), 디지털 인프라 PQC 전환 중점
영국	2035	NCSC 양자내성 암호 전환 3단계 로드맵
일본	2035	정부기관 공개키 암호 전환, CRYPTREC 역할·전환 전략 제시
중국	국가 인프라	제15차 5개년계획 — 양자기술 7대 미래산업 격상, PQC 통합 명시

국내 「범국가 양자내성 암호체계 전환 종합 추진계획」('25.9) + KpqC 국가공모('24)로 국내 개발 알고리즘 선정 → 규격·프로토콜 국내외 표준화가 활성화 선결과제 (하이브리드·암호 민첩성 병행)

01. 개요 및 현황

| 추진 체계

- 산·학·연 전문가 기반 분과위원회를 구성하여 중점 표준화 항목 및 추진전략 도출

중분류별 분과위원회 구성

AI 보안	암호	디지털 ID 관리	데이터 보안	시스템·디바이스
네트워크 보안	응용서비스	시험·평가	휴먼·바이오인식	영상보안

국제 표준화 기구

- **공식표준** JTC1 SC27(정보보안), ITU-T SG17(보안)
- **사실표준** IETF, 3GPP, W3C, CCRA 등에서 보안 기술 활용 표준 추진

국내 표준화 기구

- **TTA** PG427, TC5 등 프로젝트그룹 중심 표준화
- **협의회·포럼** 한국바이오인식협의회, 한국 제로 트러스트 포럼 등

01. 개요 및 현황

| 국외 정책 현황

- 미국 중심으로 암호·AI·네트워크·신원 전 영역에서 국가안보 차원의 정책 추진

암호

- **백악관 EO 14412 ('26.6)** 암호 키 2030, 전자서명 2031까지 PQC 전환 강제

총괄 전략

- **「미국을 위한 사이버 전략」('26.3)** 억제·민관 협력·연방망 현대화(ZT·클라우드·PQC)·핵심 인프라·신기술 우위·인재 6대 축

AI 보안

- **첨단 AI 혁신·안보 EO ('26.6)** 상용 첨단 AI 출시 전 취약점 평가
- **AI 액션플랜('25.7)** Security by Design, AI-ISAC 설립

디지털 ID

- **NIST SP 800-63-4 ('25.8)** 패스키·생체 MFA·디지털 지갑, 딥페이크·합성신원 사기 대응

네트워크

- **제로 트러스트 구현지침 SP1800-35('25.6)** '26년말까지 연방·국방부 ZT 성숙도 달성 목표

영상 보안

- **DHS·국경수비대 지능형 CCTV 확대** 국방수권법 통한 중국산 CCTV 조달 금지 등 신뢰 인프라 구축

01. 개요 및 현황

| 국내 정책 현황

- 「국가 사이버안보 전략」·「AI 기본법」을 축으로 예방 중심 체계로 전환 가속

AI 정책

- **AI 기본법('25.1) / AI 행동계획('26.2)** 보안 취약점 신고·조치·공개 제도 로드맵
- **국정원 AI 보안가이드북('25.12)** 프롬프트 인젝션·적대적 입력 대응

양자·암호

- **양자산업 육성법 개정('26.5)** 국가기관 양자 보안체계 의무화
- **범국가 PQC 전환 종합계획('25.9)** 암호체계 전환 원칙·기술전략

개인정보·데이터

- **개인정보보호법 개정('26.3)** 매출 최대 10% 과징금, ISMS-P 의무화
- **가명정보 가이드라인 전면개정('26.3)** 위험도 기반 판단체계 도입

디지털 신원

- **모바일 주민등록증 전국 확대('25.3)** 전자정부법 개정('26.1)으로 실물과 동일 효력

네트워크·인프라

- **N2SF 보안 가이드라인 1.0('25.9)** 망분리 중심→위험기반·제로 트러스트 전환
- **범부처 정보보호 종합대책('25.10)**

바이오·기타

- **생체인식 동물등록 여건조성('25.2)** 비문 등 생체인식 기반 동물등록 호환규격 표준화 추진

01. 개요 및 현황

| 시장 및 특허 현황

- 글로벌·국내 시장의 지속 성장과 대규모 특허 축적 — 정보보안·물리보안 통합 성장

글로벌 사이버보안 시장 ('25 $2,276억→)
$3,519억 '30

AI 보안 '24 $254억→'30 $938억
24.4% CAGR

'24 국내 정보보호산업 (전년比 +10.5%)
18.6조 원

IP5 유효특허 ('05~'25.4, keywert)
19,829 건

국내 시장 구조

- **정보보안** 7조 1,244억 원
- **물리보안** 11조 4,701억 원
- **정책 목표** '27년까지 시장규모 30조 원 확대 (정보보호산업 글로벌 경쟁력 확보 전략)

특허 현황 (IP5)

- **분석 대상** 한·미·일·유럽·중국 공개·등록 유효특허 19,829건 ('05.1~'25.4)
- **핵심 키워드** 보안·암호·인증·식별·서명 / security, cipher, cryptography, signature, authentication

01. 개요 및 현황

| 국외 기술 개발 현황

- 양자·AI 위협 대비 및 5G/6G·AI·클라우드 기반 통합 사이버보안 기술 중심으로 변화

AI 보안

- **DARPA·NIST·NSF** 적대적 방어·설명가능 AI ·편향완화 R&D, 보안성 검증 벤치마크
- **에이전틱 AI 거버넌스** 섀도우 AI 통제, NHI 관리, 자율형 SOC

암호

- **NIST** 양자내성 전자서명, 암호 다자간 분산수행, 인증 암호 운영모드 신규 확보

디지털 ID

- **FIDO 패스키 Passwordless** W3C VC2.0, OpenID4VCI/VP, EU EUDI Wallet ARF 상호운용

데이터 보안

- **PETs 중심 발전** 고성능 AI·에이전트 확산 대응 개인정보보호 강화기술, NIST PETs Test bed

네트워크

- **클라우드 API·ASM** Open RAN 보안, 6G FMSC·NTN, 네트워크 슬라이스 인증 강화

시험·평가

- **CC/CEM 체계(SC27 WG3)** CCRA 18개국, EU EUCC 채택, 미국 FIPS 140-3·CMVP ·CAVP/ACVTS

01. 개요 및 현황

| 국내 기술 개발 현황

• 양자·AI 위협 대응 및 5G/6G·클라우드 기반 제로 트러스트 환경 구축 중심으로 기술개발 변화

AI 보안

- **Security for AI + AI for Security** 입력검증·모델보호·학습데이터 무결성
- **KISA·ETRI·삼성SDS** 보안관제·이상탐지·악성코드 분석 AI 자동화

암호

- **KpqC('24) 국내 알고리즘 선정** 규격 표준화 및 암호 프로토콜 적용방법 개발

디지털 ID

- **모바일 신분증 전국 확대** 민간앱 개방(10개), 분산ID·VC 기반 디지털 지갑 실증

데이터 보안

- **위험도 기반 재식별 측정** 가명·익명 처리, 비정형 데이터 개인정보 탐지

네트워크·영상

- **제로 트러스트 가이드 2.0** 6G·클라우드 원천기술
- **영상보안** 개방형 플랫폼·멀티모달 AI·VLM 관제

R&D 투자

- **정보보호핵심원천기술 1,074억 원('26)** 데이터·네트워크 보안, 신산업 가상융합보안, 공공서비스 보호, 국제협력
- AI생태계보안내재화핵심기술개발, 범국가양자내성 암호전환핵심기술개발 등 신규 추진

01. 개요 및 현황

국제 표준화 현황

- JTC1 SC27·ITU-T SG17 중심 + 사실표준화기구(IETF·3GPP·W3C 등)에서 병행 추진

표준화 기구	주요 표준화 내용
ISO/IEC JTC1 SC27	27090(AI 위협)·27091(AI 프라이버시), 15408/18045(보안성 평가), 19790/24759(암호모듈), 18033-2(PQC KEM), 14888(PQC 전자서명)
ITU-T SG17	Q10(디지털 신원)·Q13(차량통신)·Q16(AI 보안), X.sfdiw(디지털지갑), X.Spud(비정형 가명처리)
ISO TC307	블록체인·DLT — JWG4(보안·프라이버시·신원)에서 SC27과 공동 표준 개발
IETF / IRTF	OAuth 2.0 확장 AI 에이전트 대리 인가, WIMSE 에이전트 신원, CFRG PQC 규격화
3GPP / ITU-R	IMT-2030(6G) 권고안(M.2160)·TPR 개발 완료('26.6), SA3 연계 6G 보안 아키텍처
Onvif / IEC TC79	개방형 영상보안(OSSA) 프레임워크, 대규모 영상 플랫폼 연동 규격 표준화
W3C / OpenID / FIDO	VC Data Model 2.0, OpenID4VCI·VP, 패스키 기반 인증 사실표준 주도

01. 개요 및 현황

국내 표준화 현황

- TTA 정보보호 PG(501~507)·PG427 중심 + 협의회·포럼에서 신기술 표준화 추진

표준화 기구	표준화 내용
TTA PG501 (정보보호기반)	암호 알고리즘·프로토콜, 양자내성 암호 규격·적용방법, 다자간 분산 수행
TTA PG502 (개인정보·ID·블록체인)	디지털 지갑 보안, 모바일 신분증 상호운용, 위험도 기반 가명·익명 처리 평가
TTA PG503 (네트워크 보안)	클라우드·6G·제로 트러스트 전환 관련 보안 표준화
TTA PG504 (응용보안·평가인증)	암호모듈 시험평가, 정보보호제품 평가·인증, 차량보안
TTA PG505 (바이오인식)	바이오인식 데이터 포맷, 반려동물 개체인증 데이터 포맷·저장구조
TTA PG507 (AI 보안, '26.5 신설)	AI 보안 평가 프레임워크, 시험·인증 절차, AI Red Teaming·취약점 검증
TTA PG427 (지능형 CCTV)	개방형 영상보안 API, 멀티모달 지능형 물리보안 연동, 영상기기 운영지침
협의회·포럼 (KITSTA 등)	동물 개체식별, 바이오인식, 제로 트러스트, 블록체인 보안 표준화

02

SECTION 02

표준화 환경 분석 및 시사점

Environment Analysis & Implications

02. 표준화 환경 분석 및 시사점

SWOT 분석

S

(시장) 보안 이슈 대응을 위해 기업·기관의 보안장비 구매 증가
(기술) 정부·공공기관의 적극적 AI 보안 연구·사업화 추진, 양자내성암호 전환에 대한 국가적 추진, 민간기업의 빠른 기술 적용
(표준) 보안 분야에서 국내 전문가의 국제표준화 기여도 높음

W

(시장) 세계 시장 대비 국내 보안시장 규모 협소
(기술) 기반기술 분야 핵심원천기술 확보 미흡, AI 보안 전문 기업 부족 및 AI 보안과 기존 IT 보안 간 통합 평가 기술 미흡
(표준) ICT 개발을 주도하는 국내 산업체 참여 미흡

O

(시장) AI·양자컴퓨팅 위협 선제 대응과 AI 보안 수요 증가에 따른 보안 시장 개편 필요성 대두
(기술) AI 등 신기술의 중요성과 더불어 보안의 중요성이 부각되며 ICT 개발에 보안 내재화 추진
(표준) JTC1, ITU-T 등 국제표준 기구에서 보안 표준화 활동 활발

T

(시장) 글로벌 보안기업 및 특정 국가의 표준화 주도에 따른 기술 독점·종속 우려
(기술) 국가 차원의 보안 원천기술 확보 경쟁 심화, AI 보안 위협의 다양화·고도화, 법적·규제 리스크 증가
(표준) 핵심기술에 대한 미국·유럽 표준화 단체 중심의 국제표준화 추진

02. 표준화 환경 분석 및 시사점

시사점: 레거시 보안에서 차세대 신뢰 거버넌스로 패러다임 전환

AS-IS (레거시 보안)		TO-BE (차세대 신뢰 거버넌스)
AI Safety 중심, 독립적 사각지대 존재	→	AI Security 포함 신뢰 거버넌스, 실시간 위협 데이터 공유(CTI)
양자내성 암호 알고리즘 확보 수준	→	국제 표준 반영 및 프로토콜 적용, 다자간 안전계산(MPC)
중앙집중식 인증, 정성적 위험 식별	→	자기주권형 신원(SSI)/DID, 자동화된 재식별 위험 측정
온프레미스/클라우드/엣지 분리, 서명 기반 탐지	→	통합 AI/SOAR 대응, 제로트러스트 아키텍처
탬퍼 대응 개념 단계, 클라우드 평가 불가	→	탬퍼 검증, 클라우드 및 차량통신망 보안 보증

03

SECTION 03

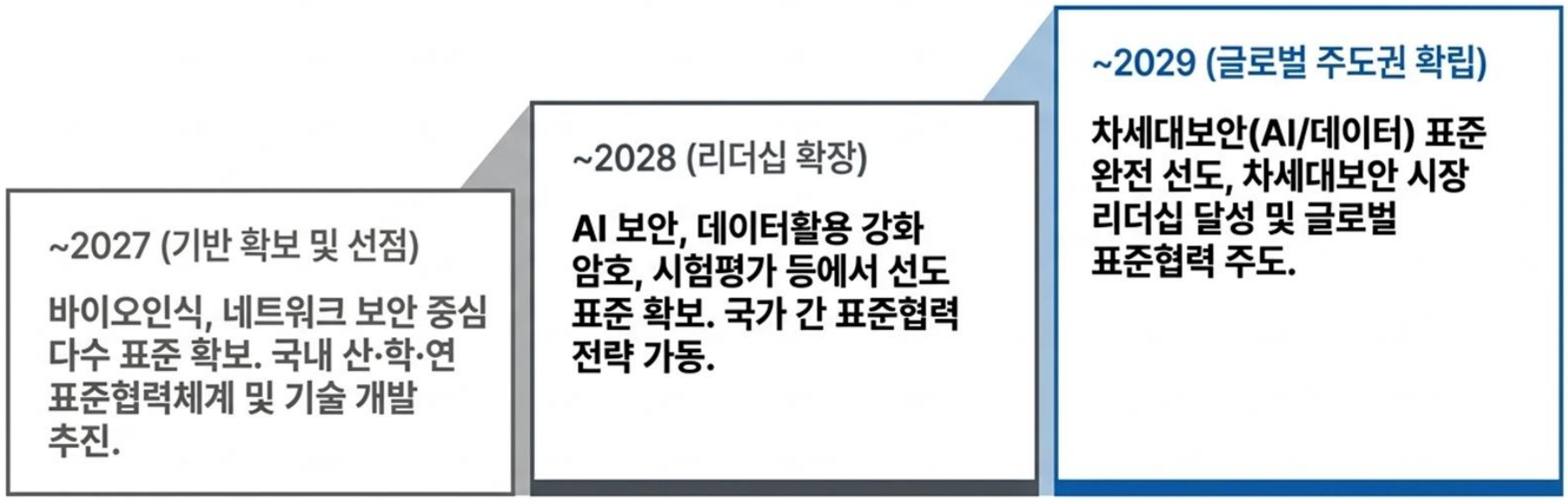
비전·목표 및 중점 표준화 항목

Vision, Goals & Key Items

03. 비전·목표 및 중점 표준화 항목

비전: 국제 표준 선점을 통한 차세대보안 분야 기술 선도

목표



03. 비전·목표 및 중점 표준화 항목

7대 추진 전략

선정 기준 표준개발의 시급성·개발가능성(1단계) → 국가핵심기술·정부정책 검토(2단계)로 중점 표준화 항목 선정

선정 결과 **7대 추진전략** · **17개 중점 표준화 항목**

1	2	3	4	5	6	7
국가 AI 사이버쉴드 돔 구축을 위한 보안 기술 확보 (4개 항목)	국가·공공 및 민간 응용서비스 암호 체계 안전성 강화 (2개 항목)	디지털 ID 관리 및 데이터 보안성 확보 (2개 항목)	지능형 네트워크 위협 대응 및 신뢰성 강화 (2개 항목)	시험/평가 기술 확보를 통한 보안성 향상 (3개 항목)	휴먼/바이오인식 기술 선제적 확보를 통한 안전·신뢰성 보장 (2개 항목)	재난 및 사회 안전 확보를 위한 지능형 영상 보안 기술 개발 (2개 항목)

03. 비전·목표 및 중점 표준화 항목

7대 추진전략 및 17개 중점 표준화 항목

추진전략	중점 표준화 항목
1. 국가 AI 사이버쉴드 돔 구축을 위한 보안 기술 확보	1-1 네트워크 공격에 능동적 대응을 위한 지속 학습 기술 / 1-2 AI 서비스 보안성 평가 기술 1-3 AI 에이전트 신원인증 및 권한위임 기술 / 1-4 AI 기반 사이버위협 데이터 공유 모델 및 연동 인터페이스 기술
2. 국가·공공 및 민간 응용서비스 암호 체계 안전성 강화	2-1 데이터 활용성 강화 기술(암호 알고리즘 다자간 분산 수행) / 2-2 암호 프로토콜 양자 안전성 강화 기술
3. 디지털 ID 관리 및 데이터 보안성 확보	3-1 디지털 지갑 보안 기술 / 3-2 비정형 데이터 처리 및 재식별 위험성 측정 기술
4. 지능형 네트워크 위협 대응 및 신뢰성 강화	4-1 클라우드 및 모바일 통신 환경에서의 보안기술(IMT-2030) / 4-2 제로트러스트 기반 신뢰성 강화형 네트워크 보안 기술
5. 시험/평가 기술 확보를 통한 보안성 향상	5-1 암호모듈 탬퍼 대응 기술 / 5-2 클라우드 환경에서의 IT 제품 보안성 평가 기술 / 5-3 차량 통신망 보안성 평가 기술
6. 휴먼/바이오인식 기술 선제적 확보를 통한 안전·신뢰성 보장	6-1 반려동물 개체인증을 위한 생체인식 호환 데이터 포맷 / 6-2 생체인식 기반 가축동물 개체식별 관리지침
7. 재난 및 사회 안전 확보를 위한 지능형 영상 보안 기술 개발	7-1 자율 보호체계가 내재화된 개방형 영상보안플랫폼 기술 / 7-2 대규모 영상 플랫폼 간 연동 기술

03. 비전·목표 및 중점 표준화 항목

[추진전략 1] 국가 AI 사이버쉴드 돔 구축을 위한 보안 기술 확보

AS-IS

- 네트워크 공격에 단순 분석적 기술을 기반하여 정보보호 대응 서비스 구축
- 차별금지·편향성·인간존엄성 보장 등 AI Safety를 중심으로 한 AI 거버넌스 구축
- 챗GPT 등 챗봇 기반 AI 모델들의 보안 위협 및 프라이버시 연구를 진행
- 기관/기업별 독립적 사이버 위협 탐지 체계 운영으로 사각지대 발생 / 정형화된 인터페이스 부재로 AI 보안 모델 간 연동 시 수작업 변환 필요

TO-BE

- 자율적 결정·행동 기반 자율 인공지능의 지능형 위협에 능동 대응하는 신뢰성 평가 서비스 구축
- AI Security를 포함하여 의사결정 투명성·책임성·검증가능성을 아우르는 인공지능 신뢰 거버넌스 체계 정립
- 에이전틱 AI의 자율적 다중 행동 및 피지컬 AI의 사이버-물리 융합공격에 대한 보안 위협 연구 확대
- 실시간 AI 기반 위협 데이터 공유 모델로 공공·민간 통합 방어 생태계 구축 / AI 보안 모델 간 API 표준 정의

목표

자율적 결정·행동하는 자율 인공지능의 신뢰성 및 서비스 보안 평가 체계 및 연동 인터페이스 국제 표준화 선도

기대효과

AI 대전환 시대에 AI 안전·전·신뢰성 확보 및 AI Trust를 미래 혁신·전 첵산업으로 육성, EU AI Act 준수 인증 연계를 통한 글로벌 시장 선점

국제표준

ITU-T SG17 Q16 중심 Agentic AI 자율행동 보안·AI 공급망 신뢰·Physical AI 대응 의제 주도, JTC1 SC27 ISO/IEC 27090·27091 및 15408·18045 확장 의견 반영

국내표준

TTA PG507에서 AI 보안 평가 프레임워크, AI Red Teaming, 자율행동 감사·XAI 기반 신뢰 검증, Physical AI 시험·인증, AI CTI 공유 모델 표준 개발

03. 비전·목표 및 중점 표준화 항목

[추진전략 2] 국가·공공 및 민간 응용서비스 암호 체계 안전성 강화

AS-IS	TO-BE
- 블록체인 등장, 개인정보보호 강화 등 응용 환경과 정책의 변화에 따라 원천기술의 실용화 연구 가속화 - 양자내성 암호 분야는 국내 개발 암호 알고리즘 확보 수준이며, NIST 표준 등은 국제 표준화 추진 중 - 안전성과 효율성 및 신뢰성을 보장할 수 있는 신규 암호 프로토콜 관련 기술 확보 필요	- 현재 기술을 활용한 시범 사업 추진을 통해 기술 수요 식별 및 신규 기술 개발 - 다자간 안전계산 프로토콜 요소기술 국제 표준화 추진 - 양자내성 암호 알고리즘 규격 및 활용 방법 표준화 추진 - 국내 개발 양자내성 암호 알고리즘의 국가표준화 및 대외 신뢰성 확보를 위해 국가 간 협력 강화

목표	암호 체계의 안전성 고도화 및 서비스 가용성 강화를 위한 핵심 요소기술 표준화 추진	기대효과	국가 사이버 환경 전반의 신뢰성 보장, 외산 암호장비 수입 대체 및 국내외 정보보호시장 점유율 확대
국제표준	JTC1 SC27 표준 에디터 수임을 통한 다자간 안전계산 요소기술 리더십 확보, IRTF CFRG·IETF sec에서 국내 개발 PQC 규격/적용 표준화	국내표준	TTA PG501에서 국내 개발 PQC 알고리즘 규격 및 암호 프로토콜 적용 방법 단체표준 개발, RRA를 통한 국가표준 추진

03. 비전·목표 및 중점 표준화 항목

[추진전략 3] 디지털 ID 관리 및 데이터 보안성 확보

AS-IS	TO-BE
- 메타버스·AI 에이전트 등 신 플랫폼을 위한 신원 인증 기술이 초기 실증 단계 - 기존 인증 서비스는 중앙집중식 신원 인증 중심으로 발급기관 간 상호운용성 제한 - 비식별 정보 활용 시 사전 위험 식별이 정성적 판단에 의존하여 개인정보 보호 및 프라이버시 침해 위험 존재	- 실·가상 융합 환경에서 사용자–AI 에이전트 간 신뢰성 확보를 위한 다양한 신원 확인 기술 개발 - 자기주권형 신원(SSI)·분산ID·검증가능한 자격증명(VC) 기반 탈중앙화 디지털 신원 프레임워크 및 디지털 지갑 통합 인증 체계로 전환 - 위험도 기반(Risk-based)으로 비식별 처리 전 주기에서 재식별 가능성을 자동 측정·시각화하여 안전성 검증 및 사전 통제

목표	기대효과
디지털 신원(ID) 프레임워크 및 위험도 기반 비식별 처리·재식별 위험성 측정 자동화 표준화 추진	안전한 개인정보의 빅데이터·AI 활용 활성화, 전자상거래·전자정부·금융·헬스케어 분야 비즈니스 기회 창출
국제표준	**국내표준**
ITU-T SG17 X.sfdiw(디지털 지갑 보안 프레임워크) 표준화 추진, W3C VC 2.0·EUDI ARF 정합성 확보를 통한 상호운용 표준 도출	TTA PG502에서 디지털 지갑 보안 요구사항, 모바일 신분증 민간개방 상호운용 프레임워크, 위험도 기반 비식별 적정성 및 재식별 위험성 측정 표준화

03. 비전·목표 및 중점 표준화 항목

[추진전략 4] 지능형 네트워크 위협 대응 및 신뢰성 강화

AS-IS

- 단편적 보안 체계: 온프레미스와 클라우드, 5G/6G 엣지 환경 분리로 통합 위협 관리 불가
- 수동적 위협 대응: 보안 전문가 분석 의존으로 대규모 트래픽 실시간 대응 한계
- 사후 대응 중심: 서명 기반 탐지 위주로 신종 지능형 위협 예측 부재
- 정형화된 제로 트러스트 아키텍처 및 전환 지침 표준 개발 필요

TO-BE

- 통합 지능형 보안: 클라우드·5G/6G·엣지·OT 환경의 통합 플랫폼 구축 및 위협 인텔리전스 공유
- AI 기반 자동 대응: AI/LLM 활용 실시간 분석 및 SOAR 기반 자동 대응 체계 구축
- 행위 기반 능동적 위협 예측: 위협 사전 예측 및 선제적 차단(XDR) 체계 구축
- AI 기반 제로트러스트 플랫폼 구현 및 한국 주도로 ITU-T SG17 국제표준 개발 추진

목표

클라우드 공격 표면 관리, 6G 네트워크 구조 기반 보안, AI 보안 거버넌스 제로 트러스트 공통 보안 능력에 대한 선제적 표준 개발

기대효과

6G 필수 표준특허 기반 로열티 수익 확보
제로 트러스트·AI 보안 솔루션 생태계 조성으로 신규 보안 시장 창출

국제표준

클라우드·제로 트러스트 보안은 한국 주도로 ITU-T SG17 국제표준 추진
6G 보안은 3GPP·ITU-R 연계 SG17 국제표준 개발

국내표준

TTA PG503에서 AI 네이티브 6G 아키텍처 내재화 보안 기능 설계 및 제로 트러스트 전환 실증 기반 국내 표준 개발

03. 비전·목표 및 중점 표준화 항목

[추진전략 5] 시험/평가 기술 확보를 통한 보안성 향상

AS-IS

- 현재 암호모듈 표준인 ISO/IEC TS 30104는 개념 단계로만 존재
- 정보보호시스템과 네트워크 장비 도입 시 필요한 평가 기술/기준 개발 중
- 기존 평가 방법론으로는 클라우드 환경의 제품/서비스 보안 보증 불가능
- 보안성 평가는 국가별 이해관계가 상이하며 글로벌 기업의 시장지배력이 높음
- 차량통신 응용 서비스 보안에 대한 표준 미흡

TO-BE

- 안전한 칩을 설계하고 검증하는 원천 기술 개발
- 모듈 정보를 획득하거나 일부 손상을 주는 준침투 공격에 대응
- 클라우드 환경에서의 IT 보안성 평가 기술 및 표준 개발
- 클라우드 융복합 서비스·상품에 대한 안전성 및 공공성 평가인증
- 스마트 모빌리티 응용 서비스 보안 표준 개발

목표

시험/평가 기술 확보를 위한 핵심 요소기술 표준화 추진

기대효과

정보보호제품/서비스의 보안성 향상 및 시장 경쟁력 강화,
신환경·최신 트렌드 기술 우위 확보 및 선제 대응

국제표준

JTC1 SC27 표준 에디터 수임을 통한 탬퍼 대응 및
클라우드 평가기술 리더십 확보,
ITU-T SG17 의장단 수임을 통한 차량통신 보안 표준 개발

국내표준

TTA PG504에서 암호모듈 시험평가, 정보보호제품 평가/인증,
차량보안 등 응용보안/평가인증 단체표준 개발

03. 비전·목표 및 중점 표준화 항목

[추진전략 6] 휴먼/바이오인식 기술 선제적 확보를 통한 안전·신뢰성 보장

AS-IS	TO-BE
- 기존 반려동물 개체식별 방식(마이크로칩 등)으로는 유기·유실견, 펫보험 사기 등의 문제 해결 어려움 - 고가의 마필·한우 종자관리, 경주마 도핑테스트와 보험사기 예방을 위해 가축동물 개체식별의 중요성이 크게 부각됨	- 바이오인식 기반 반려동물 개체 인증을 위한 관련 기술 및 관련 표준 개발 - 바이오인식 기반 마필·한우 등 가축동물 개체식별 기술 및 관련 표준 개발
목표	**기대효과**
휴먼·동물 간 공존과 동물 복지를 위한 바이오인식 기반 동물 개체식별 인증기술에 대한 국내외 표준화 추진	유기견 예방, 펫보험 사기 등 반려동물 사회적 문제 해결 및 바이오인식 기반 등록제도 도입 기여 (글로벌 펫 보안시장 진출)
국제표준	**국내표준**
한국IT융합표준·인증협회(KITSTA)를 통하여 ITU-T SG17 Q10(텔레바이오인식)에서 동물 개체식별기술 국제표준화(X.1095 후속) 추진	TTA PG505 중심 데이터 포맷 및 저장 구조 표준화, KITSTA 수집·품질 기준 기반 국가 방역망 연계 인터페이스 단체표준 개발

03. 비전·목표 및 중점 표준화 항목

[추진전략 7] 재난 및 사회 안전 확보를 위한 지능형 영상 보안 기술 개발

AS-IS

- 기존 영상보안 기술은 단순 위험감지 수준으로 복합적 상황 이해와 사전 징후 인지 한계
- 해킹·백도어 등에 의한 개인/보안영상 유출과 오·남용 등 사회적 문제 발생
- 개별적으로 구축된 단일 영상보안 시스템 중심으로 광역·통합 대응 한계

TO-BE

- 영상 내 전반적인 상황을 자율적으로 이해·묘사하고 징후를 감지하는 Agentic AI CCTV 기술 개발
- OSSA를 준용하는 영상보안 통합 프레임워크 표준 기술 및 성능시험 표준 개발
- 대규모 영상 플랫폼 간의 융합을 통해 통합적인 보안·위험 대응을 위한 연동 표준 개발

목표

개방형 영상보안 프레임워크의 글로벌 사실 표준(Onvif) 개정 및 대규모 영상 플랫폼 간의 연동 표준(IEC TC79) 추진

기대효과

단말 제조사·영상분석 서비스·통합관제업체 협업 기반 시장 발판 마련, VSaaS 시장 신규 비즈니스 모델 제시

국제표준

Onvif에서 국내 제정된 개방형 프레임워크를 OSSA 표준으로 개정 추진, IEC TC79에서 대규모 영상 플랫폼 간 연동 규격 제정

국내표준

TTA PG427에서 개방형 CCTV 보안·앱 인터페이스 규격, 대규모 영상 메타데이터 규격 및 연동 시험, 멀티모달 AI 이상탐지 표준 추진

04

SECTION 04

중점 표준화 항목별 추진 전략

Standardization Strategy by Item

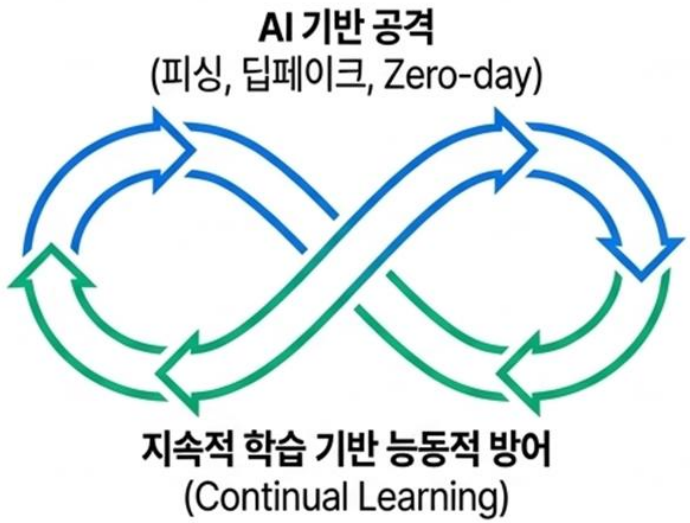
04. 중점 표준화 항목별 추진 전략

[중점항목 1-1] 네트워크 공격에 능동적 대응을 위한 지속 학습 지침

이슈: AI 공격(자동화 피싱, 딥페이크 인증우회) 속도가 방어 기술을 추월. 상시 갱신되는 능동적 방어 체계 필수.

표준 개발 핵심

- AI 공격·방어 참조모델 (자동화·강화학습 시나리오)
- 진화형 공격(랜섬웨어 2.0 등) 대응 요구사항 정립
- 방어 모델의 학습 데이터 품질 및 갱신 프로세스



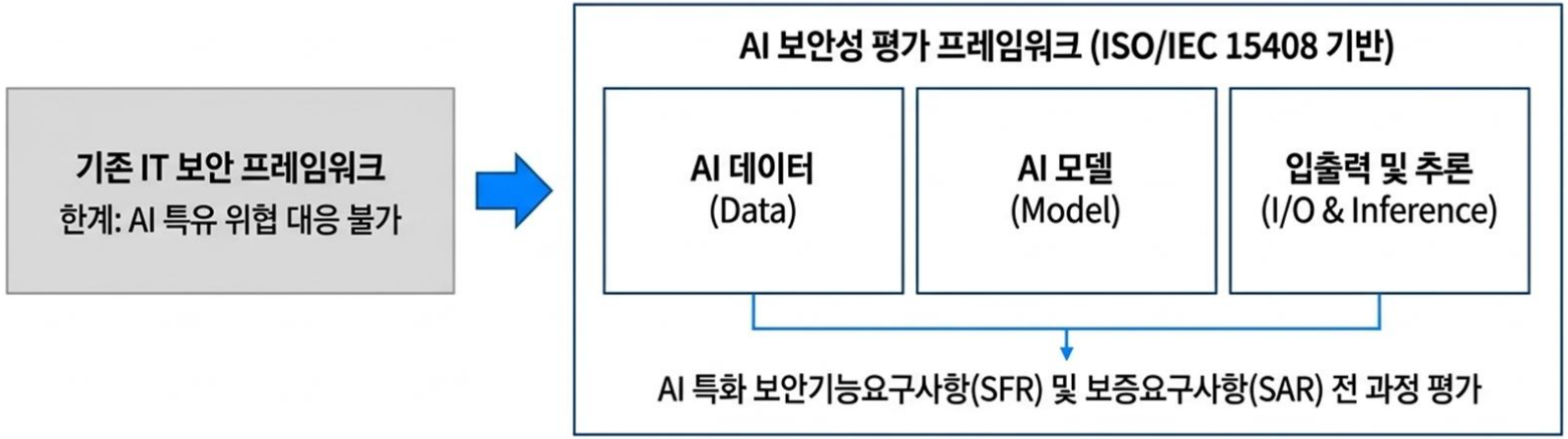
국내외 추진 전략

- **국내:** TTA 중심 참조 모니터, AI 모델 생명주기 보안 제정
- **국제:** ITU-T SG17, JTC1 SC27·SC42 지속 학습 참조모델 개발

04. 중점 표준화 항목별 추진 전략

[중점항목 1-2] AI 서비스 보안성 평가 표준

전략적 맥락: 글로벌 빅테크 중심의 평가 프레임워크 확산에 따른 기술 및 인증 종속 리스크 선제적 방어.



국제 표준화 리더십: JTC1 SC27 중심 AI 보안성 평가 요구사항 국제표준 주도를 통한 국내 기업 글로벌 진출 기반 확보

04. 중점 표준화 항목별 추진 전략

[중점항목 1-3] AI 에이전트 신원인증 및 권한위임 체계 표준

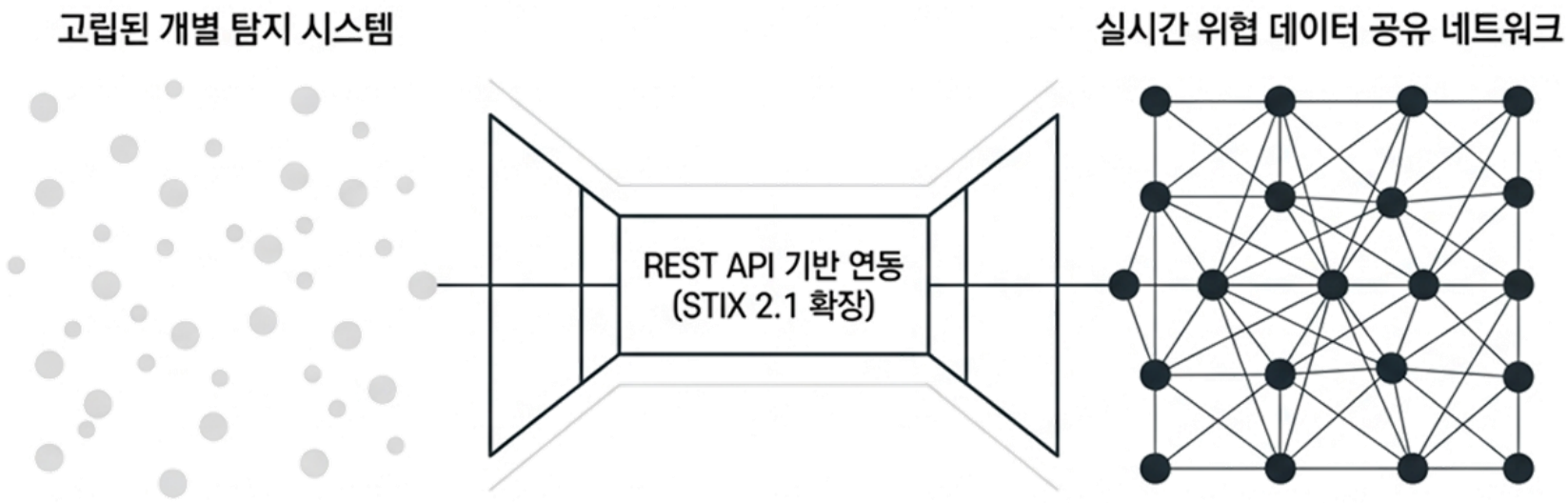
인간 중심 신원 (Traditional Identity)	비인간/AI 에이전트 신원 (NHI)
인간 사용자 (NIST SP 800-63 기반)	자율적 행위를 수행하는 AI 에이전트
ID/Password, 생체인식	고유 식별자 발급 체계 (SPIFFE ID, DID)
직접 인가 (Direct Access)	대리 인가 (On-Behalf-Of) 및 위임 범위 제한 (OAuth 2.0/2.1 확장)
단일 세션 검증	멀티에이전트 신뢰체인 검증 및 Correlation ID 추적

추진 전략: ITU-T SG17 Q10·Q16 연계 에이전트 전용 크리덴셜 발굴 및 NIST AI Agent Standards Initiative 등 글로벌 선도 그룹 선제 대응

04. 중점 표준화 항목별 추진 전략

[중점항목 1-4] AI 기반 사이버위협 데이터 공유 모델 및 연동 인터페이스 표준

핵심 과제: 고도화된 AI 위협 앞 방어 최전선에서 고립된 개별 기관. AI 탐지 결과(신뢰도, XAI 설명 등) 교환을 위한 상호운용성 부재.



메타데이터 공유
모델 버전 및 학습 기간
메타데이터 공유 포맷 정의

AI 확장 객체
AI 분석 결과 및 탐지
신뢰도 표현을 위한 데이터 모델 확장

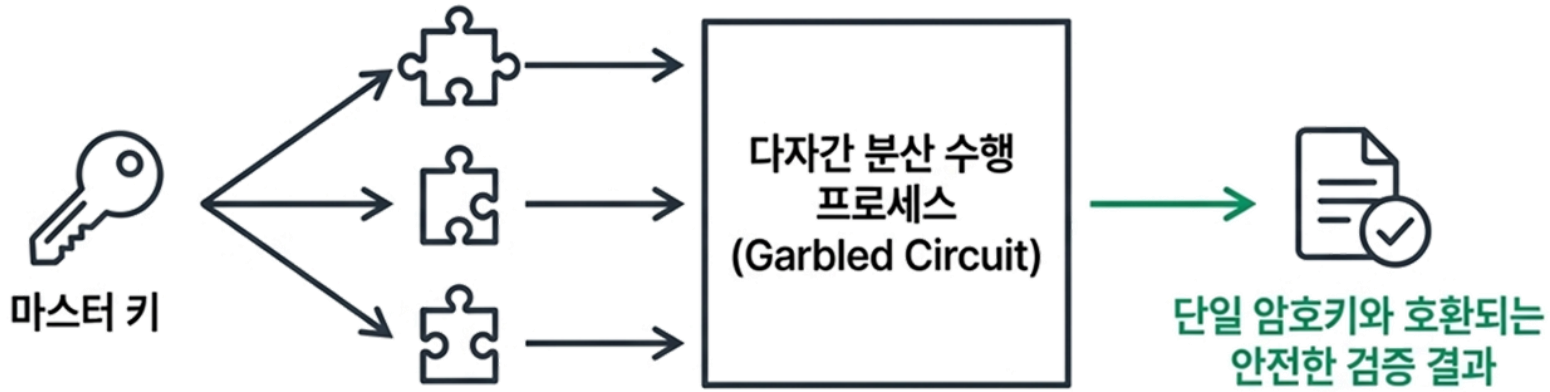
연동 인터페이스
이기종 보안 시스템 간
STIX 2.1 기반 확장 SDO/SCO 정의

기대 효과: 국경 없는 실시간 데이터 공유 체계 확립 (ISO/IEC 27090 연계)

04. 중점 표준화 항목별 추진 전략

[중점항목 2-1] 암호 알고리즘 다자간 분산 수행 기법 표준

이슈: 임계 전자서명 위주 적용되나 참조 표준 부재. 단일 암호키 사용 시의 호환성과 안전성 동시 확보 필요.



표준 개발 내용

- 안전성을 극대화하는 분산 관리 프로토콜 규격
- MPC를 지원하는 일반 암호 알고리즘 설계
- 안전한 시스템 모델 및 운영 시나리오 제시

추진 전략

전략: JTC1 SC27 표준 에디터 수임을 통한
요소기술 리더십 확보 및 NIST 공모 동향 병행 분석

04. 중점 표준화 항목별 추진 전략

[중점항목 2-2] 양자내성 암호 알고리즘과 활용 방법 표준

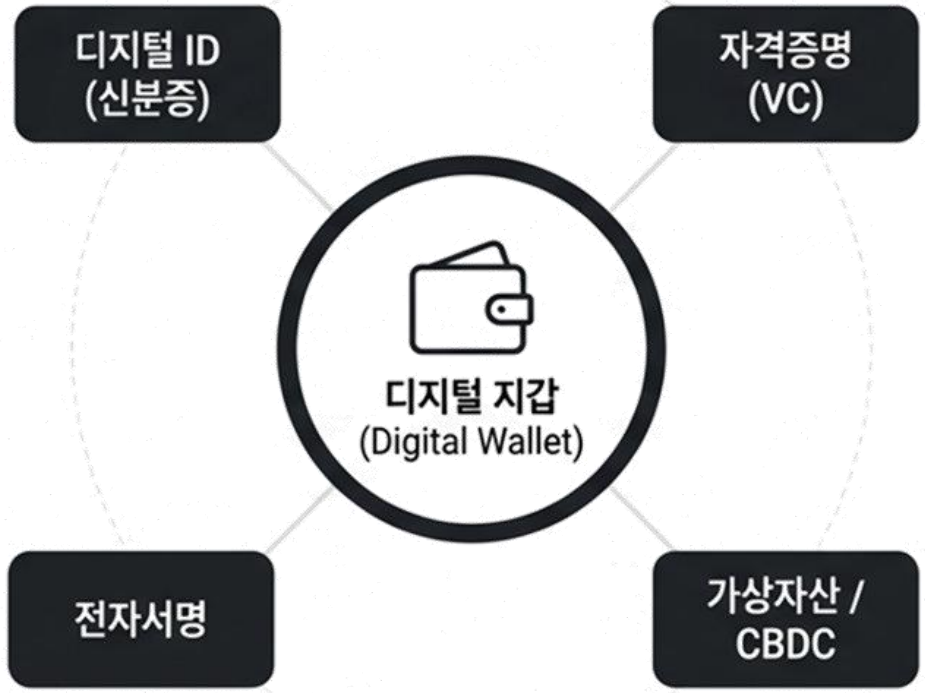


세부 개발 내용		
국내 국가공모(KpqC) 선정 알고리즘 규격 표준화	특정 암호 프로토콜에의 알고리즘 적용 방법 및 영향 범위 정의	상호운용성 확보를 위한 파라미터 설정 및 안전한 운용 고려
국제 협력 전략		
글로벌 대응: 국내 KpqC 알고리즘 표준화 후 IETF sec 제안 및 NIST PQC 전환 프로젝트 적극 참여		

04. 중점 표준화 항목별 추진 전략

[중점항목 3-1] 디지털 지갑 프레임워크 표준

배경: 민간앱 10개 지갑 체제 확대 및 모바일 신분증 1,500만 돌파 전망. 다양한 발급기관 간 상호운용 가능한 개방형 기술표준 시급.



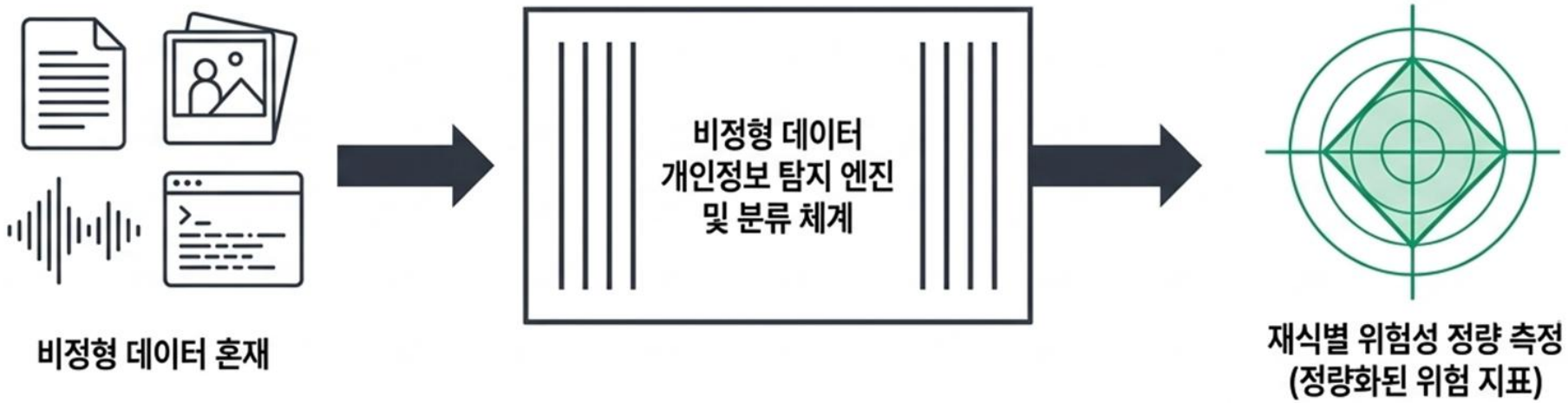
프레임워크 핵심 구성 요소
1. 플랫폼 상호운용 API 및 VC 발급/검증 프로토콜
2. 프라이버시 보호를 위한 선택적 공개(Selective Disclosure) 메커니즘
3. 지갑 유형별 공통 보안 요구사항 정의

글로벌 정합성: EU EUDI ARF v2.8, W3C, ISO/IEC 18013-5(mDL) 참조 및 ITU-T SG17 X.sfdiw 연계

04. 중점 표준화 항목별 추진 전략

[중점항목 3-2] 비정형 데이터 처리 및 재식별 위험성 측정 기술 표준

이슈: 기존 비식별 가이드라인은 정형 데이터 중심. 텍스트, 이미지, 영상, 음성 등 비정형 데이터의 자동 탐지 및 정량적 처리 기준 미흡.



위험도 산정 기준

위험도 산정 = 민감도 + 식별가능성 + 특이성 + 외부 결합 가능성

추진 전략

국내 비정형 데이터 R&D 연계 및 ITU-T SG17 X.Spud (비정형 데이터 가명처리 보안요구사항) 연계 표준 협력 주도

04. 중점 표준화 항목별 추진 전략

[중점항목 4-1] IMT-2030 보안 기능 및 요구사항 표준

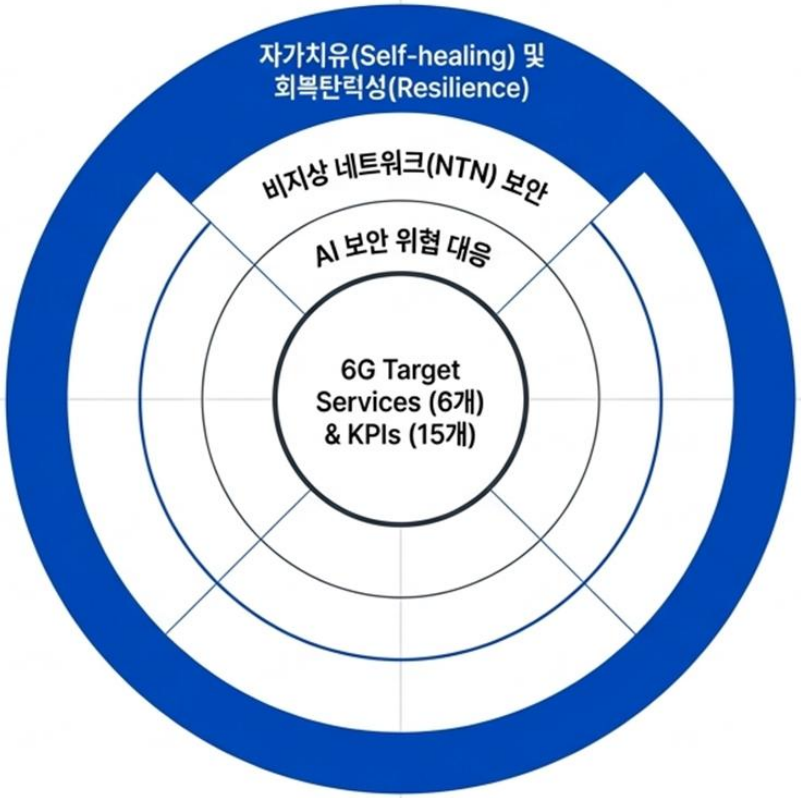
주요 이슈

ITU-R M.2160 프레임워크 권고안 제정에 따른 기술성능요구사항(TPR) 보안 기준 개발 완료 목표 ('26.6).

설계 단계부터 보안을 내재화하는 'Security-by-Design' 원칙 필수.

EU AI Act, 미국 NIS2 등 글로벌 규제 강화에 대응하는 법적 기반 표준 연계 시급.

EU AI Act, 미국 NIS2 등 글로벌 규제 강화에 대응하는 법적 기반 표준 연계 시급.



추진 전략

(국내) TTA PG503 중심 표준화 및 한국 ITU 연구위원회 WP5D 활동.

(국제) ITU-T SG17 6G 보안 프레임워크 신규 과제 제안, JTC1 SC27 연계 공동 개발, 3GPP SA3 협력 대응.

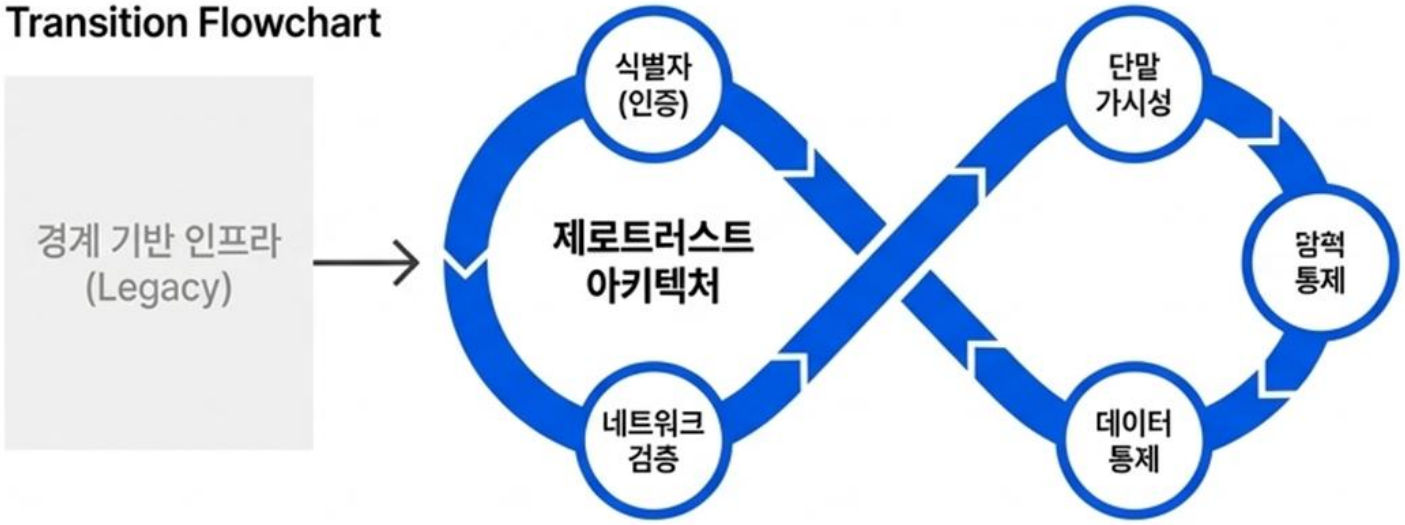
04. 중점 표준화 항목별 추진 전략

[중점항목 4-2] 제로트러스트 기반 신뢰성 강화형 네트워크 보안 기술

주요 이슈

- NIST SP 800-207 기반 가이드라인은 존재하나, 조직별 재구성으로 인한 파편화 발생.
- 기존 인프라의 전환 지침 및 이기종 제품 간 상호운용성을 위한 '공통 보안 능력(Capability)' 정의 부재.

Transition Flowchart



추진 전략

- (국내) TTA PG503 및 한국 제로트러스트 포럼 연계. 가이드라인 2.0('24.12) 및 성숙도 모델 해설서('25.12) 기반 실증 표준 개발.
- (국제) 국가별 구현 방법 분석을 바탕으로 한국 주도의 ITU-T SG17 국제표준 개발.

04. 중점 표준화 항목별 추진 전략

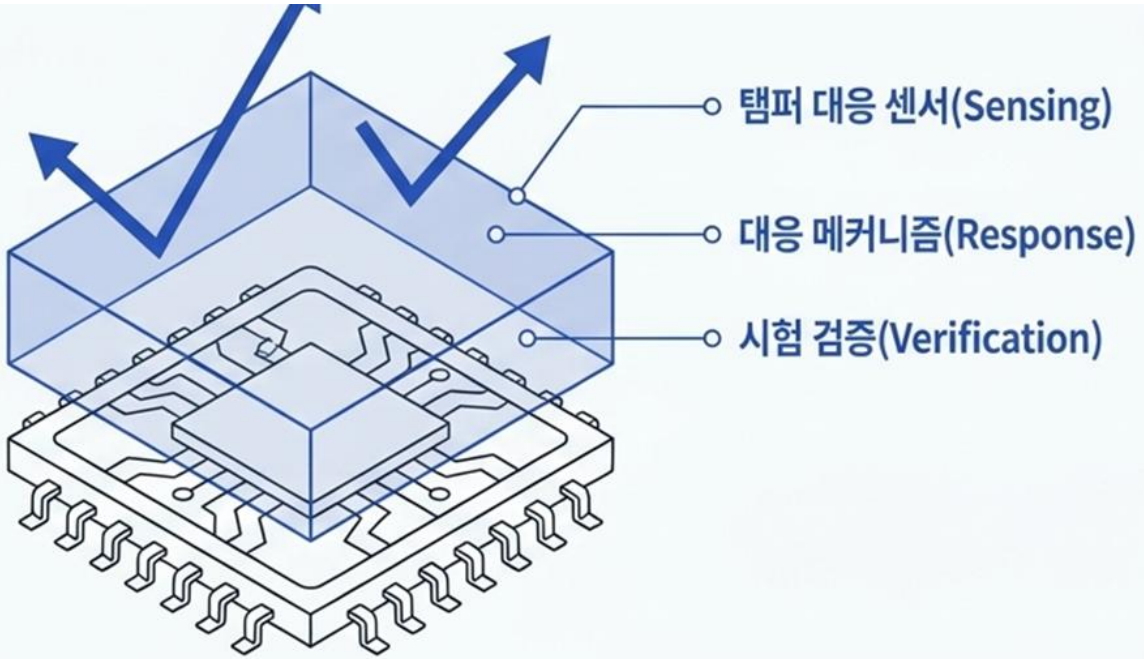
[중점항목 5-1] 암호 칩 탬퍼 대응 요구사항 표준

주요 이슈

ISO/IEC TS 30104는 개념만 제공할 뿐 구체적 시험 방법 부재.

NIST Hardware Project 및 TCG TPM 규격 확산에 따른 물리적 보안 검증 요구 증가.

글로벌 기업의 노하우 은닉 및 원천 기술 표준 선점으로 인한 종속 우려.



추진 전략

(국내) TTA 응용보안/평가인증 PG(PG504) 중심 원천기술 확보 병행.

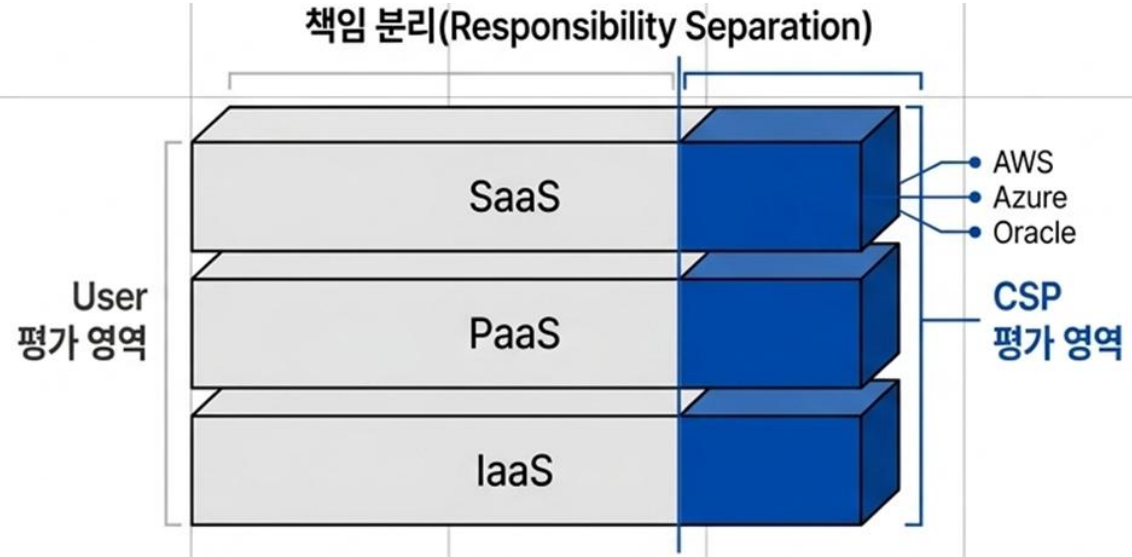
(국제) 신기술 선점 전략(병행). JTC1 SC27 표준 에디터 수임을 통한 암호모듈 탬퍼 대응 요소기술 글로벌 리더십 확보.

04. 중점 표준화 항목별 추진 전략

[중점항목 5-2] 클라우드 환경에서 보안성 평가 요구사항 표준

주요 이슈

- 기존 IT 제품 중심의 CC(Common Criteria) 프레임워크 한계 노출.
- 미국 NIAP의 서비스 중심 평가 전환 환 공식화 및 CCUF CCitC 가이드 제시('25.2).
- EUCS 공식 시행 임박. 국내 기업의 평가 기술 종속 리스크 급증.



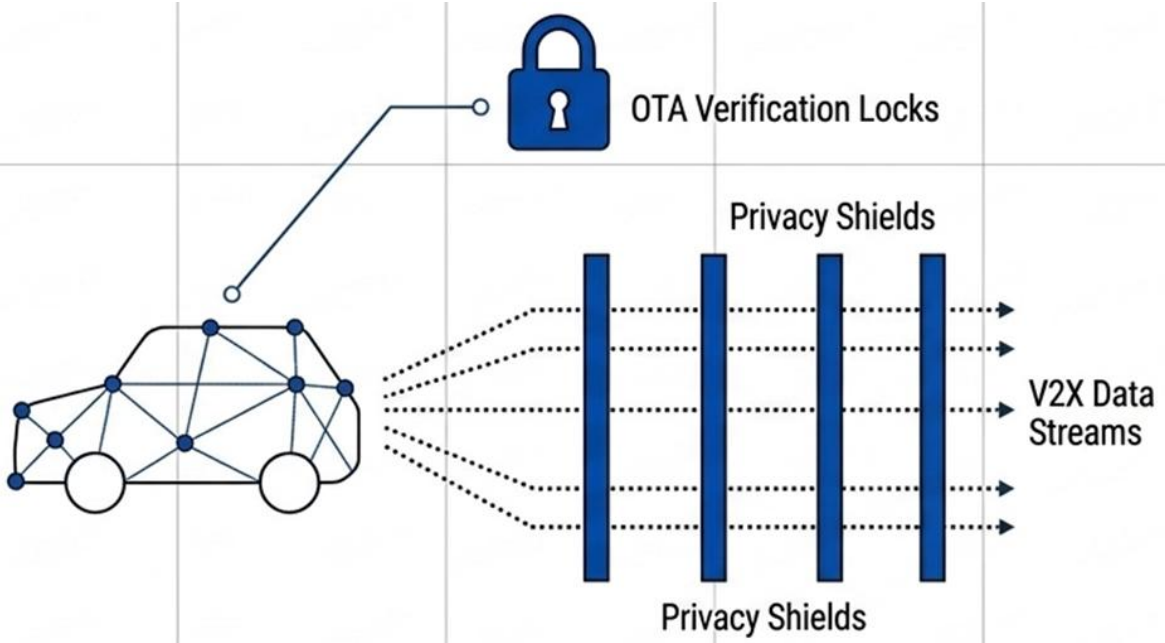
추진 전략

- (국내) TTA PG504의 클라우드 보안인증제 운영 경험을 바탕으로 신규 평가 방법론 선제 도입.
- (국제) JTC1 SC27 표준 에디터 수임을 통해 제품에서 '서비스 중심'으로 전환되는 평가기술 글로벌 표준 주도.

04. 중점 표준화 항목별 추진 전략

[중점항목 5-3] 차량통신 및 응용서비스 보안 표준

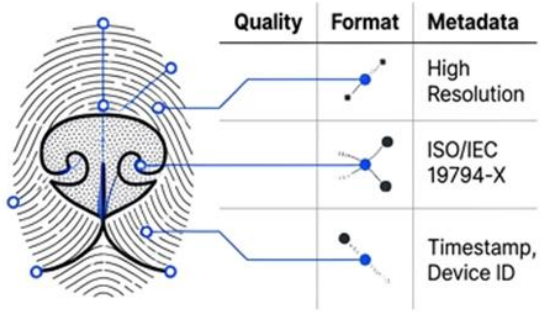
주요 이슈	• 차량통신 응용 서비스 고도화 대비 표준화 미비로 운전자·보행자 생명 안전 위협. • 차량 내·외부 센서를 통한 무분별한 개인정보 수집 및 프라이버시 훼손 심각성. • 소프트웨어 원격 업데이트(OTA) 해킹 리스크 및 보안성 평가 부재.
추진 전략	• (국내) TTA PG504 중심 기반 마련 (차량 내부 네트워크 TTAK.IT-X.1381, V2X TTAK.KO-12.0432, SDV TTA.KO-12.0420). • (국제) ITU-T SG17 Q13 의장단 수임 활용, 커넥티드카 OTA 보안 표준(X.ota-sec) 추진.



04. 중점 표준화 항목별 추진 전략

[중점항목 6-1] 반려동물 개체인증을 위한 생체인식 호환 데이터 포맷 표준





주요 이슈

- 현행 마이크로칩(RFID) 및 외형 기반 등록은 판독 오류, 장비 의존성, 위·변조 취약.
- 비문(코무늬) 및 안면 데이터는 비접촉식으로 신뢰성이 높으나, 수집 절차, 저장 포맷, 품질 기준 전반의 표준 전무. 표준 전무.
- 국가 동물등록 시스템 연계를 위한 데이터 정합성 필수.

추진 전략

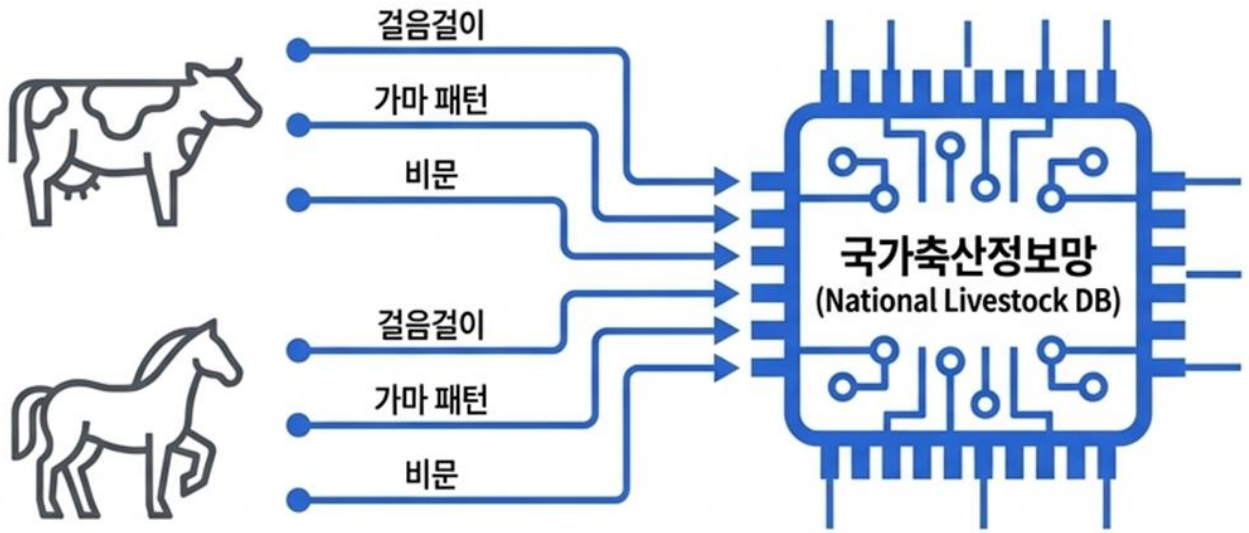
- (국내) KITSTA(DB 구축 가이드) 및 TTA PG505(데이터 포맷 및 저장 구조 표준화) 동시 가동.
- (국제) ITU-T SG17 Q10(텔레바이오인식)에서 X.1095 후속 국제표준화 확장.

04. 중점 표준화 항목별 추진 전략

[중점항목 6-2] 생체인식 기반 가축동물 개체식별 관리지침

주요 이슈

- 귀표(RFID) 탈락 및 위조, 마필 탐지 부정확성으로 인한 방역·경마 보안사고 빈발.
- 자동 인식이 가능한 생체정보(비문, 안면, 가마 패턴, 걸음걸이) 수집·관리 통합 지침 부재.
- 국가 가축방역 시스템 및 이력관리 시스템과의 대규모 상호운용성 시급.



추진 전략

- (국내) 신기술 선점 전략(병행). KITSTA(수집·품질 기준) 및 아이싸이랩 등 민간 협력을 통한 알고리즘 및 방역망 연계 인터페이스 개발.

04. 중점 표준화 항목별 추진 전략

[중점항목 7-1] 개방형 영상보안 통합 프레임워크 표준

주요 이슈

- 제조사 고유 OS 종속으로 인해 자율적인 AI 및 보안 기능 탑재가 원천 불가.
- 안드로이드 OS 탑재 시 Attack Surface 급증으로 영상 유출 등 보안 취약성 극대화.
- 폐쇄적 생태계에서 개방형 협업 프레임워크로의 전환 필요.



추진 전략

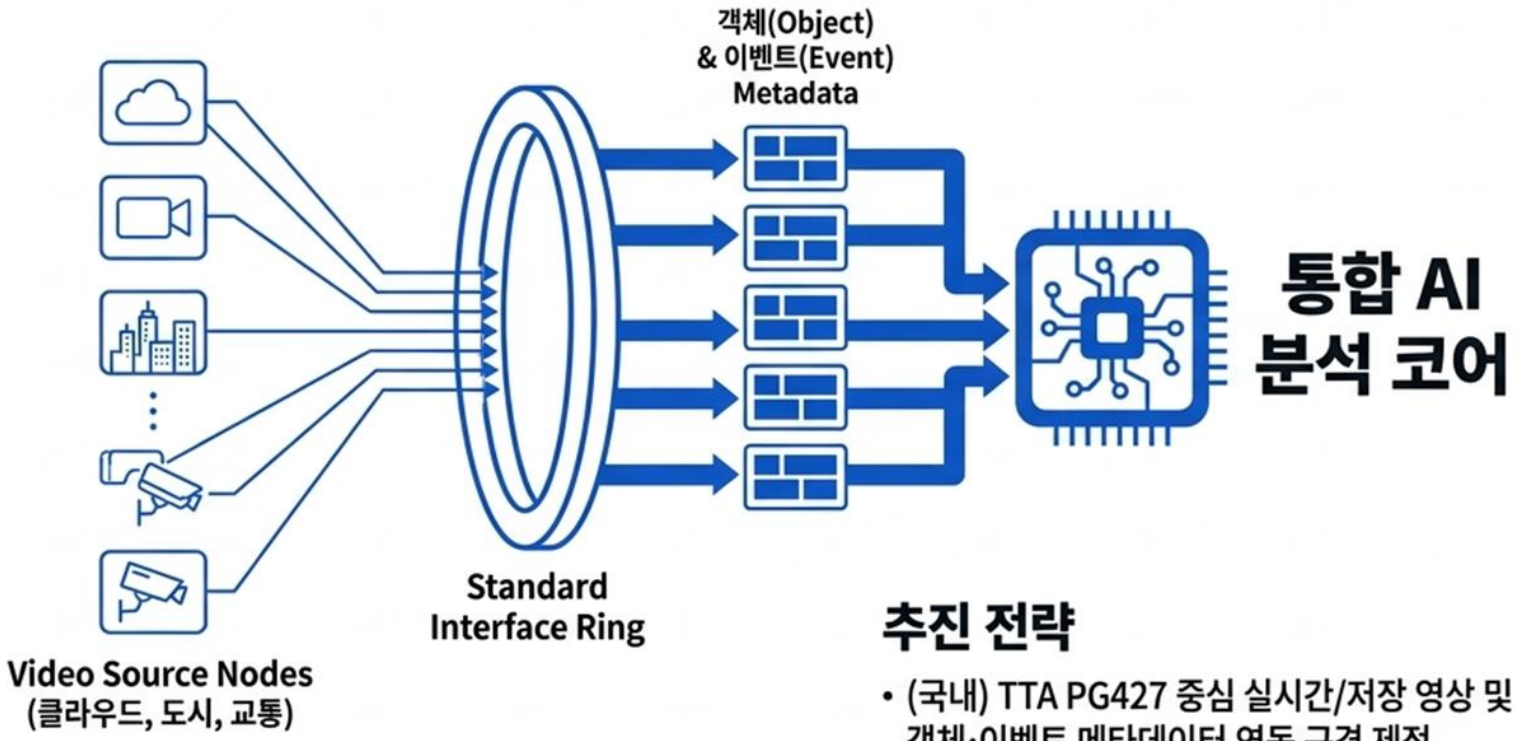
- (국내) TTA PG427 중심 개방형 프레임워크 제정. OSSA 표준 4건(보안, 카메라, 앱, 연동 규격) 국내 표준화('25~'27).
- (국제) 신기술 선점 전략(병행). 국내 제정 표준을 글로벌 Onvif OSSA 표준으로 억제안 및 개정 추진.

04. 중점 표준화 항목별 추진 전략

[중점항목 7-2] 대규모 영상 플랫폼 간 연동 표준

주요 이슈

- 영상 플랫폼 간 메타데이터 구조 및 해석 기준 불일치로 복합 AI 분석 및 객체 연계 불가.
- 클라우드 관제, 도시 통합관제 확산에 따라 표준화된 교환 인터페이스 수요 폭증.



추진 전략

- (국내) TTA PG427 중심 실시간/저장 영상 및 객체·이벤트 메타데이터 연동 규격 제정.
- (국제) IEC TC79 위원회를 통한 대규모 영상 플랫폼 연동 규격 국제표준 제정 추진.

10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

감사합니다.

권대성 연구위원, ETRI 부설연구소

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA kista ETRI