개인정보보호위원회 | 보도자료 | 국민이 만든 대전환의 길

보도시점 2026. 6. 9.(화) 12:00 배포 2026. 6. 9.(화) 07:30

인공지능 시대, 개인정보 전주기 보호체계를 담은 기술 연구개발 로드맵 나왔다

- 11대 핵심기술과 인재양성을 아우르는 개인정보 기술 생태계 구축 목표
- 기존의 기술 연구개발(R&D)·표준화 로드맵을 통합·연계하고, 인공지능 환경을 고려한 조기 개정

인공지능 시대에 **개인정보**를 **안전하게 활용**하기 위한 **기술혁신**의 **청사진**이 제시된다.

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 인공지능·데이터 중심 사회에서 개인정보 보호와 안전한 활용을 지원하고, 인공지능 시대에 부합하는 신뢰 환경을 조성하기 위해 「**개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵(2026~2030)**」(이하 '로드맵')을 **수립**하여 **공개***했다.

* '개인정보위 홈페이지(정책·법령>기업정책), 개인정보 포털(자료>정책자료)'에서 내려받기 가능

이번 로드맵은 기존 각기 운영 중이던 기술 연구개발(R&D)과 표준화 로드맵*을 **통합·연계**하여 조기 개정한 것으로, 개인정보 기술 연구개발(R&D)과 표준화 간 **연속성**을 **높이**고 **인공지능 시대의 개인정보 분야 기술** 변화에 **선제적으로 대응**하기 위해 마련됐다.

* 개인정보 보호·활용 기술 R&D 로드맵('22~'26), 개인정보 보호·활용 기술 표준화 로드맵('23~'27)

특히, 최근 에이전틱·피지컬 인공지능(AI) 등 신기술 확산으로 개인정보 처리 환경이 급변하면서 **개인정보 유·노출, 인공지능 학습데이터의 노출·재식별 등**에 대한 **우려**도 증가하고 있어, **현 기술 발전상황을 반영**해 개인정보의 생성·수집부터 파기까지 **생애 전주기**별 연구가 필요한 **보호·활용 기술**과 **표준화 대상**을 **재정비**했다.

또한, 국내·외 **최신 기술 및 표준화 동향** 등을 고려해 개인정보 전주기 보호·활용 기술 분류체계를 정의하였고, **▲개인정보 주권보장, ▲유·노출 위험경감, ▲신뢰기반 안전활용, ▲인공지능(AI) 대응 기술개발 등 4대 분야 11대 핵심기술**을 선정했다.

< 최종 선정된 11대 핵심기술>

분야 (중분류)	연번	핵심기술 (세분류)	주요 세부 기술 및 표준
1 개인정보 주권 보장 (1)	1	**정책준수 증명결과 열람**	검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제증명(Forget-by-Design) 기술 등 3건
2 유·노출 위험 경감 (3)	2	**딥페이크·합성 검증·레이블링**	딥페이크 사전 예방을 위한 데이터 변환 기술('26년 예산 반영) 및 관련 표준 등 4건
	3	**엣지 디바이스 개인정보보호**	온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술·표준 등 3건
	4	**다크웹·표면웹 유출 탐지**	다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술, 연계 표준 등 5건
3 신뢰기반 안전활용 (3)	5	**재식별 위험도 평가·검증**	가명·익명정보 재식별 검증 기술('26년 예산 반영) 및 평가 방법론 표준 등 5건
	6	**합성데이터 등 PET 기반 비식별화(단일·하이브리드)**	개인정보 보유 제한 관련 시계열 합성데이터 생성 및 검증 기술('26년 예산 반영), 평가 표준 등 3건
	7	**마이데이터 동의·위임 통합 자동화 플랫폼**	마이데이터·공공 서비스 연계를 위한 신원(SSI) 기반 개인정보 지갑 운영·보안 검증 기술 등 2건
4 AI 대응 기술개발 (4)	8	**AI 모델 안전성 평가**	생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제 기술('26년 예산 반영), 파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술('25년, 2건 예산 반영) 및 시험방법 표준 등 6건
	9	**에이전트·도구·로봇 실행 보안**	에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험예측·보호조치 기술, 연계 표준 등 6건
	10	**피지컬 AI 실시간 프라이버시 제어**	피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술 등 4건
	11	**AI 기반 비정형데이터 비식별화(영상, 텍스트, 음성 등)**	멀티모달형 AI 기반 개인정보 탐지·추적 및 비식별화 기술('25년 예산 반영), 관련 표준 등 4건

1. **(정책 준수 증명 결과 열람)** 개인정보 처리·삭제 이행 여부를 자동 분석·증명
2. **(딥페이크/합성 검증·레이블링)** 합성콘텐츠 여부를 자동 판별하고 검증 정보를 제공
3. **(엣지 디바이스 개인정보보호)** 모바일·IoT 단말의 개인정보 관련 이상행위를 탐지·차단
4. **(다크웹·표면웹 유출 탐지)** 다크웹 상 개인정보 불법유통 및 노출 여부를 탐지
5. **(재식별 위험도 평가·검증)** 가명·비식별 데이터의 재식별 가능성을 검증
6. **(합성데이터 등 PET 기반 비식별화)** PET 기반의 안전한 데이터 활용 지원
7. **(마이데이터 동의·위임 통합 자동화 플랫폼)** 정보주체 동의·위임 등 통합 관리 플랫폼
8. **(AI 모델 안전성 평가)** 생성형 AI 모델의 개인정보 노출·민감정보 추론 위험 등 방지 및 평가
9. **(에이전트·도구·로봇 실행 보안)** AI 에이전트의 개인정보 접근·실행 권한의 안전한 통제
10. **(피지컬 AI 실시간 프라이버시 제어)** 로봇·IoT 환경의 개인정보 수집 범위를 제어
11. **(AI 기반 비정형데이터 개인정보 탐지·비식별화)** 텍스트·영상·음성 내 개인정보를 탐지·비식별화

11대 핵심기술 내에는 **인공지능(AI) 모델 학습·추론 과정**에서 발생할 수 있는 개인정보 유·노출 위험 등 **안전성 평가**, **에이전틱·피지컬 인공지능(AI) 환경**에서 **개인정보 오·남용을 방지**하기 위한 **기술** 등 인공지능 환경에 **적시 대응 가능한 기술 요소**들을 **신규 반영**하였다.

또한, **개인정보보호 강화 기술(PET)***과 인공지능이 융합된 **AI-PET 기술**, 비정형데이터 등의 **비식별화 기술 연구** 등을 통해 다양한 신기술이 등장하는 환경 속에서도 **개인정보 보호**와 **안전한 활용**의 **균형**을 갖춘 **실용적**이고 효능감 있는 **기술 연구개발(R&D) 및 표준화**를 **추진**해 나갈 계획이다.

* PET(Privacy Enhancing Technology) : 가명·익명처리 기술, 합성데이터, 동형암호 등 다양한 개인정보 보호 강화 기술을 통칭

아울러, **개인정보 분야에 특화된 전문가를 양성**하기 위한 향후 **10년간**의 **인력양성 방향***을 **신규**로 **마련**했다. '**개인정보 보호·활용, 유출사고 예방·대응 등**'의 **역량을 갖춘 전문 인재를 확보**하기 위하여 **단계적으로 추진**할 예정이다.

* 로드맵 내 「개인정보 분야 전문인력 양성 로드맵('26~'35)」을 [별첨]으로 구성

송경희 개인정보위 위원장은 “**인공지능 기술 발전**과 함께 **새로운 프라이버시 위험이 증가**하고 있는 만큼, 이를 **사전에 예방하기 위한 기술 연구개발의 중요성이 더욱 커지고 있다**”면서, “개정된 로드맵을 기반으로 **현장의 수요를 반영한 상용화 가능한 개인정보 보호·활용 기술을 개발**하고, 이를 **국내·외 표준화, 전문가 양성과 유기적**으로 **연계**하여 **인공지능 시대에 필요한 개인정보 보호·활용 기술 생태계를 구축**해 나가겠다”고 밝혔다.

붙임 「개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵」 1부.

담당 부서	개인정보보호정책국 신기술개인정보과	책임자	과 장	원세연 (02-2100-3071)
		담당자	사무관	최재민 (02-2100-3068)
			주무관	김성현 (02-2100-3069)

참고1 **개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵 개요**

1. 개인정보 전주기 보호·활용 기술 분류 체계 재구조화*

* 기술 R&D와 표준화 로드맵을 통합·연계하고, 세분류(59개)로 신 분류체계 정의

(종전) 기술 R&D 로드맵	
중분류(3)	소분류(14)
Ⅰ 정보주체 권리보장	Ⅰ-1 정보주체 동의 실질화
	Ⅰ-2 정보주체 통제권
	Ⅰ-3 정보주체 신원인증 정보 관리
	Ⅰ-4 개인정보 접해동등
Ⅱ 유·노출 최소화	Ⅱ-1 PbD 원칙을 적용한 기획·설계
	Ⅱ-2 수집시 개인정보 탐지
	Ⅱ-3 이용·제공시 개인정보 관리·강화
	Ⅱ-4 개인정보 파기
	Ⅱ-5 개인정보 안전성 확보
Ⅲ 안전한 활용	Ⅲ-1 인간활동 기반기술
	Ⅲ-2 서비스 응용
	Ⅲ-3 데이터에이터 기반기술
	Ⅲ-4 융합 프라이버시 보호
	Ⅲ-5 인공지능 프라이버시

(종전) 표준화 로드맵	
중분류(3)	소분류(17)
Ⅰ 정보주체 권리보장	Ⅰ-1 정보주체 권리보장 체계
	Ⅰ-2 정보주체 동의
	Ⅰ-3 정보주체 통제권
	Ⅰ-4 정보주체 신원인증 정보관리
	Ⅰ-5 개인정보 접해제공
Ⅱ 처리단계별 보호 강화	Ⅱ-1 개인정보 처리단계 체계
	Ⅱ-2 PbD 원칙을 적용한 기획·설계
	Ⅱ-3 수집
	Ⅱ-4 이용·제공
	Ⅱ-5 파기
	Ⅱ-6 안전성확보
Ⅲ 안전한 활용	Ⅲ-1 안전한 활용 체계
	Ⅲ-2 기반기술
	Ⅲ-3 서비스 응용
	Ⅲ-4 아이에이터 개인정보 보호
	Ⅲ-5 융합 프라이버시 보호
	Ⅲ-6 인공지능 서비스 프라이버시 보호

(개정) 기술 R&D 및 표준화 로드맵		
중분류(4)	소분류(15)	세분류(59)
Ⅰ 개인정보 주권 보장	Ⅰ-1 정보주체 동의의 실질화	동적 동의 관리
	Ⅰ-2 정보주체 통제권	정책 준수 증명 결과 설명
	Ⅰ-3 정보주체 신원인증 정보 관리	개인정보 지갑
Ⅱ 유·노출 위협 최소	Ⅱ-1 수집 시 개인정보 탐지	실시간 비식별화엔진/온디바이스 필) 등 2개
	Ⅱ-2 개인정보 파기	자동화된 파기 등 2개
	Ⅱ-3 개인정보 안전성 확보	플랫폼 무결성/신뢰실행환경(TEE) 등 7개
	Ⅱ-4 외부 유출 모니터링 탐지	디크랩 표면랩 유출 탐지 등 4개
Ⅲ 신뢰기반 안전활용	Ⅲ-1 인간활용 기반기술	데이터 정제·전처리, 비식별/변환 등 11개
	Ⅲ-2 서비스 응용	합성 영상데이터, 합성 통계데이터 등 7개
	Ⅲ-3 데이터에이터 기반 기술	데이터 클린룸·데이터 스페이스 연계 PET 등 3개
Ⅳ AI 대응 기술개발	Ⅳ-1 AI 모델 학습단계 프라이버시	언러닝(Unlearning) 등 4개
	Ⅳ-2 AI 모델 프라이버시 공격 방어 및 안전성 평가	AI 모델 안전성 평가 등 5개
	Ⅳ-3 AI 콘텐츠 신뢰성 플랫	생성 합성콘텐츠 탐지 표시 등 2개
	Ⅳ-4 AI 에이전트 보안	에이전트 도구 로봇 실행 보안 등 3개
	Ⅳ-5 AI 기반 개인정보 탐지·비식별화	피지컬 AI/로보 센싱 프라이버시 등 6개

2. 핵심기술 별 세부기술 및 표준

중분류	소분류	핵심 기술(세분류)	개념 및 주요 세부 기술·표준	비고
Ⅰ 개인정보 주권 보장	Ⅰ-2 정보주체 통제권	① 정책 준수 증명 결과 열람	· (개념) 개인정보 처리·관리행사 이력을 위변조 방지 기술로 관리하고, 검색/열람/삭제 요청 이행 여부를 정책·법규 기준으로 자동 분석·증명해 정보주체에게 제공하는 기술 · (세부 기술) - 개인정보 활용 현황을 모니터링하고 통제권 실행을 보장하는 기술 - 검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제증명(Forget-by-Design) 기술 · (관련 표준) - [국제표준] 소비자 권리 보호를 위한 PbD(Privacy by Design) 관련 국제표준	
Ⅱ 유·노출 위험 경감	Ⅱ-1 수집 시 개인정보 탐지	② 딥페이크/합성 검증·레이블링	· (개념) 이미지·영상·음성의 딥페이크/합성 여부를 자동 판별해 메타데이터 및 화면 표시로 라벨링하는 기술 · (세부 기술) - 딥페이크 사전 예방을 위한 데이터 변환 기술* - 저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술 · (관련 표준) - [국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준 - [국내표준] 유관 기관·서비스 간 딥페이크/합성콘텐츠 진위검사 결과를 안전하게 공유하기 위한 인터페이스·프로토콜 국내표준	* '26. 예산 반영
	Ⅱ-3 개인정보 안전성 확보	③ 엣지 디바이스 개인정보보호	· (개념) PC·모바일·IoT 등 엣지 단말에서 앱·프로세스 행위를 모니터링하고 격리/통제를 통해 단말 수준에서 개인정보 유출·오남용을 예방하기 위한 기술 · (세부 기술) - 온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술 · (관련 표준) - [국제표준] 엣지·모바일 단말 환경에서 개인정보 보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준 - [국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내표준	
	Ⅱ-4 역추 유출 모니터링·탐지	④ 다크웹·표면웹 유출 탐지	· (개념) 다크웹·표면웹에서 수집한 정보를 분석해 개인정보 불법 유출 및 거래 정황을 탐지·추적하는 기술 · (세부 기술) - 다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술 - 도메인명·IP 주소 범위를 기반으로 한 노출 자산 네트워크 스캐닝 및 취약점 식별 기술 - 유출 탐지 시스템의 성능 평가 지표·시험방법 및 보고서 템플릿 설계·검증 기술 · (관련 표준) - [국제표준] 다크웹·표면웹 인텔리전스(OSINT) 수집·교환 포맷 및 기관 간 연계 인터페이스 국제표준 - [국내표준] 개인정보 유출 탐지·분류·신고를 위한 공통 데이터 모델 및 API 국내표준 규격	

중분류	소분류	핵심 기술(세부분류)	개념 및 주요 세부 기술·표준	비고
8 신뢰기반 안전활용	8-1 안전활용 기반기술	⑦ 재식별 위험도 평가·검증	· (개념) 가명 비식별 데이터의 재식별 가능성을 정량 산정하고 안전성 기준 충족 여부를 검증하는 기술 · (세부 기술) - 비정형 합성데이터의 안전성 검증 및 유용성 평가 기술* - 가명 의명정보 재식별 검증 기술* - PC·모바일의 기기식별자 등 융합 현황 분석 및 랜스크래핑 상황의 개인정보 재식별 위협 판단, 개인정보 통제 기술 · (관련 표준) - [국내표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국가표준(KS) - [국내표준] 비식별 데이터의 안전성 등급 분류 및 재식별 위험 검증 절차 보고서 형식 국내표준	* 고시 예산 반영
		⑧ 합성데이터 등 PET 기반 비식별화단일 하이브리드	· (개념) 합성데이터 등 각종 프라이버시 강화 기술(PET)들을 단일 혹은 조합하여 활용도는 유지하면서 재식별 위험을 허용 수준 이하로 낮추는 비식별화 기술 · (세부 기술) - 개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술* · (관련 표준) - [국제표준] 학습·분석용 합성데이터의 품질 프라이버시 유용성 평가 기준 및 시험방법 국제표준 - [국내표준] 합성데이터·차분 프라이버시·가명처리 등 PET 연계 비식별 처리 프로파일·참조모델 국내 표준	* '26 예산 반영
	8-3 마이데이터 기반기술	① 마이데이터 등의 위임 통합 자동화 플랫폼	· (개념) 마이데이터 환경에서 정보주체의 동의 위임·철회·상태 이동 전을 통합 관리하고, 본산신원(DID)과 자기주권신원(SSI) 기반 지갑과 연계하여 신원·자격 개인정보 제공 철회 조를을 통합 자동화하는 플랫폼 기술 · (세부 기술) - 마이데이터 검증 서비스 연계를 위한 SSI 기반 개인정보 지갑 레퍼런스 구현 및 운영 보안 검증 기술 · (관련 표준) - [국제표준] 마이데이터 서비스의 정보주체 관리 및 통제권 보장을 위한 국제표준	

중분류	스몰톱	핵심 기술(세분류)	개념 및 주요 세부 기술 요소	비고
라 AI 대응 기술개발	라-3 AI 모델 공격·방어 /안전성	② AI 모델 안전성 평가	- (개념) AI 모델에 대한 행버십 속성추론·모버전 프롬프트 공격을 방어하고, 개인정보 노출 편향·취약성을 지표와 시험 시나리오로 평가/인증하는 기술 - (세부 기술) - 파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술* - 파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술* - 행정형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제 (성능 저하 최소화) 기술* - 선택적 언러닝 및 검증 가능한 모델 수준 개인정보 삭제 확인 기술 - (관련 표준) - [국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가 원화 가이드라인 및 요구사항 국제표준 - [국제표준] 개인정보 편향 보안을 포함한 AI 모델 안전성 평가 지표·벤치마크 및 시험방법 국제표준	* '25, '26 예산 반영
	라-4 AI 에이전트 보안	① 에이전트-도구-로봇 실행 보안	- (개념) AI 에이전트의 도구 API 호출 시 사용자 신원·역할 동의와 연계된 권한과 실행 조건을 제어해 개인정보 오남용과 침해를 방지하는 기술 - (세부 기술) - 에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험제로 보호조치 기술 - 멀티모달 맥락 인식 기반 개인용 프라이버시 코파일럿·트랜스포머 AI에이전트를 활용한 다맥락 개인정보 유출 탐검·삭제 자동화 기술 개발 - PET 조합 기반 에이전틱/피지컬 AI 행동정책 설계·검증 및 프라이버시 보존 실행환경 기술 - 에이전트 계정·키값(SSI/DID 등)과 연계된 사용자 신원·권한 동의 관리를 통한 안전한 실행 통제 기술 - (관련 표준) - [국제표준] AI 에이전트 권한·정책 언어 및 정책 집행 신원 연계 인터페이스 국제표준 - [국내표준] 에이전트-도구/플러그인 연계 시 보안 프라이버시 요구사항 및 권한·동의 위임 모델 국내표준	
	라-4 AI 에이전트 보안	③ 피지컬 AI 실시간 프라이버시 제어	- (개념) 로봇·IoT·스마트기기의 센싱·전송·저장 과정에서 수집 범위·해상도·보존기간 등을 제어해 실시간 프라이버시를 보호하는 기술 - (세부 기술) - 피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술 - 로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술 - (관련 표준) - [국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준 - [국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA) 위험등급 분류 및 인증 기준 국내표준	
	라-5 AI 기반 개인정보 탐지·비식별화	① AI 기반 비정형데이터 개인정보 탐지·비식별화	- (개념) 텍스트·영상·이미지·음성 등 멀티모달 환경에서 트랜스포머 등 AI 모델을 활용한 이름·주소·얼굴·번호 등 다양한 개인정보를 문맥 기반으로 탐지·비식별하는 기술 - (세부 기술) - 멀티모달형 AI 기반 개인정보 탐지·추적 및 비식별화 기술* - 트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 파운데이션 모델 오픈소스 라이브러리 개발 기술 - (관련 표준) - [국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크 기초 시험방법 국제표준 - [국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스 국내표준	* '26 예산 반영

3. 핵심기술 별 세부기술 및 표준

【 1단계 - 전문인력 양성(석·박사급) 】

● 개인정보 분야 전문가 양성 로드맵('26~'31, 총 640명 양성)

양성분야	지원대상	2026	2027	2028	2029	2030	2031
개인정보 분야 석·박사 전문인력 양성	보호·활용 전문가 2개교 (160명)	개인정보 학과(정공) 및 차별화된 커리큘럼 개발					
			개인정보 보호·활용 관련 신기술 연구·개발				
			산·학 협력체계 구성				
			현장중심형 전문가, 기술 등 인프라 확보				
				글로벌 역량 확보(해외 교육기관 협력 등)			
	예방·대응 전문가 6개교 (480명)		개인정보 유출사고 예방·대응 커리큘럼 개발				
				개인정보 사고조사 전용기술 연구·개발			
					AI 기반의 유출사고 예방·대응 실습환경 마련		
						산업계 취업 연계 지원	

※ '27년 등 신규 예산확보 여건에 따라 추진시점과 양성 규모가 일부 변경가능

【 2단계 - 선도기술 연구인재 양성(석·박사급 연구자 등) 】

● 개인정보 분야 선도기술 연구인재 양성 로드맵('31~'35, 총 300명 양성)

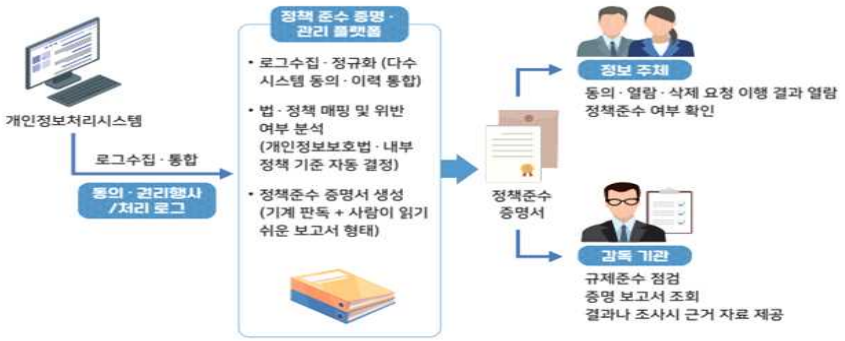
양성분야	지원대상	2031	2032	2033	2034	2035
개인정보 선도기술 연구인재 양성	차세대 개인정보 기술인재 3개교 (180명)	능동형 AI 프라이버시 제어기술 연구				
			신종 AI 융합 서비스 관련 실시간 위협저감 기술 연구			
			개인정보 전주기 별 보호방안 연구			
				다중 AI 플랫폼의 네트워킹 보호기술 연구		
	개인정보 융합인재 2개교 (120명)		개인정보 침해·유출 사전예방 기술 연구			
				사고 원인·분석 자동화 연구		
				PbD 기반, 프라이버시 융합모델 연구		
					개인정보 추적·관리 기술 연구	

※ 신규 예산확보 여건에 따라 추진시점과 양성 규모가 일부 변경가능

참고2 | **11대 핵심기술 별 주요 내용**

1. 정책 준수 증명 결과 열람

개인정보 처리·삭제 이행 여부를 자동 분석 및 증명 가능한 기술

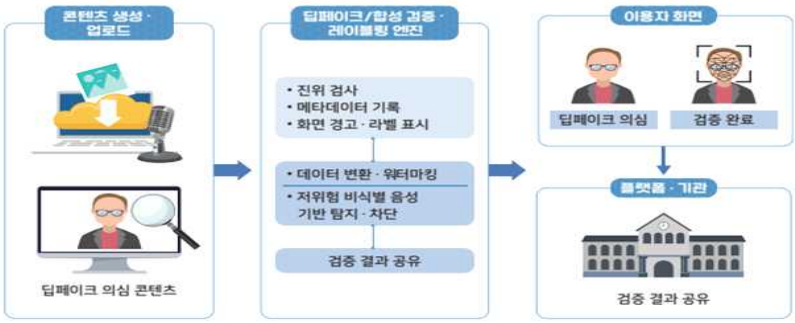


: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
정책 준수 증명 결과 열람		개인정보 활용 현황을 모니터링하고 통제권 실행을 보장하는 기술			
		검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제증명 (Forget-by-Design) 기술			
	[국제표준] 소비자 권리 보호를 위한 PbD 관련 표준				

2.딥페이크/합성 검증 · 레이블링

합성콘텐츠 여부를 자동 판별하고 검증 정보를 제공하는 기술

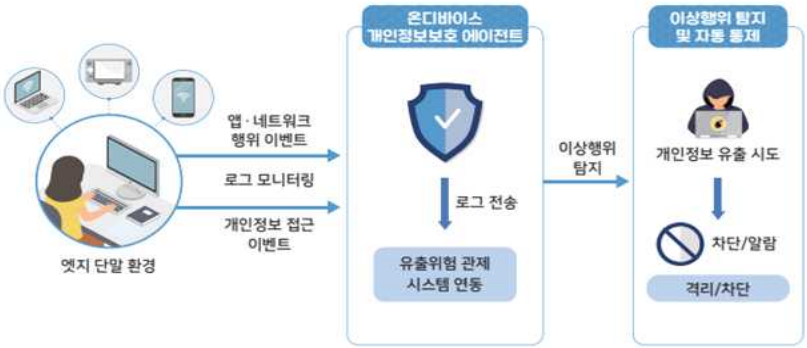


: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
딥페이크/합성 검증·레이블링	딥페이크 사전 예방을 위한 데이터 변환 기술				
		저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술			
		[국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준			
		[국내표준] 유관 기관·서비스 간 딥페이크/합성콘텐츠 진위검사 결과를 안전하게 공유하기 위한 인터페이스·프로토콜 국내표준			

3. 엣지 디바이스 개인정보보호

모바일·IoT 단말의 개인정보 관련 이상행위를 탐지 및 차단하는 기술



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
엣지 디바이스 개인정보보호		온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술			
			[국제표준] 엣지·모바일 단말 환경에서 개인정보 보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준		
			[국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내표준		

4. 다크웹 · 표면웹 유출 탐지

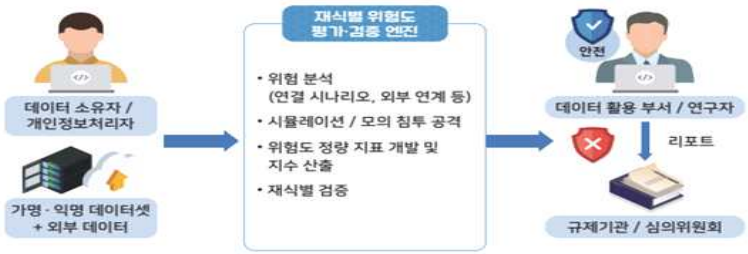
다크웹 상 개인정보 불법유통 및 노출 여부를 탐지하는 기술

: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
다크웹·표면웹 유출 탐지		다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술 개발			
			도메인명·IP 주소 범위를 기반으로 한 노출 자산 네트워크 스캐닝 및 취약점 식별 기술		
			유출 탐지 시스템의 성능 평가 지표·시험방법 및 보고서 템플릿 설계·검증 기술		
			[국제표준] 다크웹·표면웹 인텔리전스(OSINT) 수집·교환 포맷 및 기관 간 연계 인터페이스 국제표준		
			[국내표준] 개인정보 유출 탐지·분류·신고를 위한 공통 데이터 모델 및 API 국내 표준 규격		

5. 재식별 위험도 평가·검증

가명·비식별 데이터의 재식별 가능성을 검증하는 기술

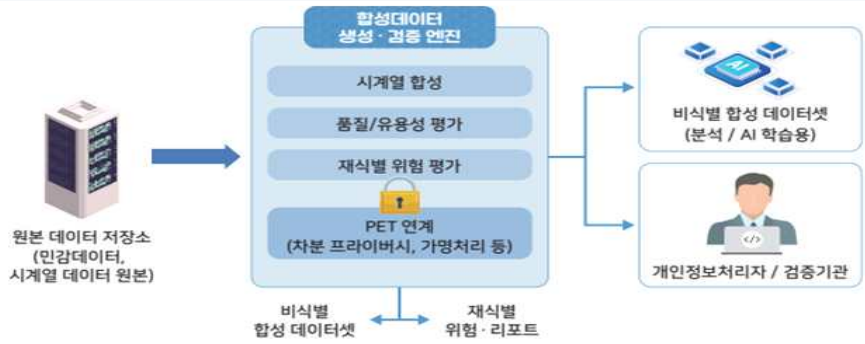


: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
재식별 위험도 평가·검증	비정형 합성데이터의 안전성 검증 및 유용성 평가 기술				
	가명 익명정보 재식별 검증 기술				
			PC·모바일의 기기식별자 등 운용 현황 분석 및 웹스크래핑 상황의 개인정보 재식별 위험 판단, 개인정보 통제 기술 개발		
			[국내표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국가표준		
			[국내표준] 비식별 데이터의 안전성 등급 분류 및 재식별 위험 검증 절차·보고서 형식 표준		

6. 합성데이터 등 PET 기반 비식별화 (단일 · 하이브리드)

개인정보보호 강화 기술(PET) 기반의 안전한 데이터 활용 지원 기술

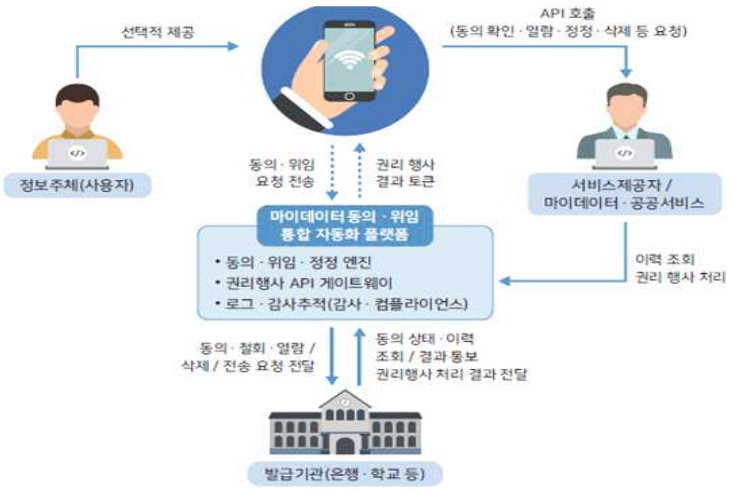


: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술				
			[국제표준] 학습·분석용 합성데이터의 품질·프라이버시·유용성 평가 기준 및 시험방법 국제표준		
			[국내표준] 합성데이터·차분 프라이버시·가명처리 등 PET 연계 비식별 처리 프로파일·참조모델 국내표준		

7. 마이데이터 동의 · 위임 통합 자동화 플랫폼

정보주체의 동의·위임 등을 통합 관리하는 자동화된 플랫폼 기술



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
마이데이터 동의·위임 통합 자동화 플랫폼			마이데이터·공공 서비스 연계를 위한 SSI 기반 개인정보 지갑 레퍼런스 구현 및 운영 보안 검증 기술		
		[국제표준] 마이데이터 서비스의 정보주체 권리 및 통제권 보장을 위한 국제표준			

8. AI 모델 안전성 평가

생성형 AI 모델의 개인정보 노출·추론 위험 등을 방지 및 평가하는 기술

: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
AI 모델 안전성 평가	파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술				
	파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술				
	생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제(성능 저하 최소화) 기술				
		선택적 언러닝 및 검증 가능한 모델에서의 개인정보 삭제·폐기 기술 개발			
			[국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 가이드라인 및 요구사항 국제표준		
			[국제표준] 개인정보·편향·보안을 포함한 AI 모델 안전성 평가 지표·벤치마크 및 시험방법 국제표준		

9. 에이전트 · 도구 · 로봇 실행 보안

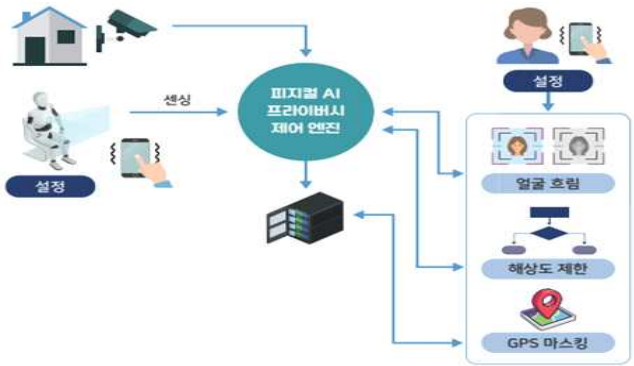
AI 에이전트의 개인정보 접근·실행 권한을 안전하게 통제하는 기술

: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
에이전트·도구·로봇 실행 보안		에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험 예측·보호조치 기술			
		멀티모달 맥락 인식 기반 개인용 프라이버시 코파일럿: 트랜스포머·AI 에이전트를 활용한 다채널 개인정보 유출 점검·상담 자동화 기술			
		PET 조합 기반 Agentic/Physical AI 행동정책 설계·검증 및 프라이버시 보존 실행엔진 기술			
			에이전트 계정·지갑(SSI·DID 등)과 연계된 사용자 신원·권한·동의 관리를 통한 안전한 실행 통제 기술		
		[국제표준] AI 에이전트 권한·정책 언어 및 정책 집행·신원 연계 인터페이스 국제표준			
		[국내표준] 에이전트-도구/플러그인 연계 시 보안·프라이버시 요구사항 및 권한·동의 위임 모델 국내 표준			

10. 피지컬 AI 실시간 프라이버시 제어

로봇·IoT 환경의 개인정보 수집 범위를 제어하는 기술

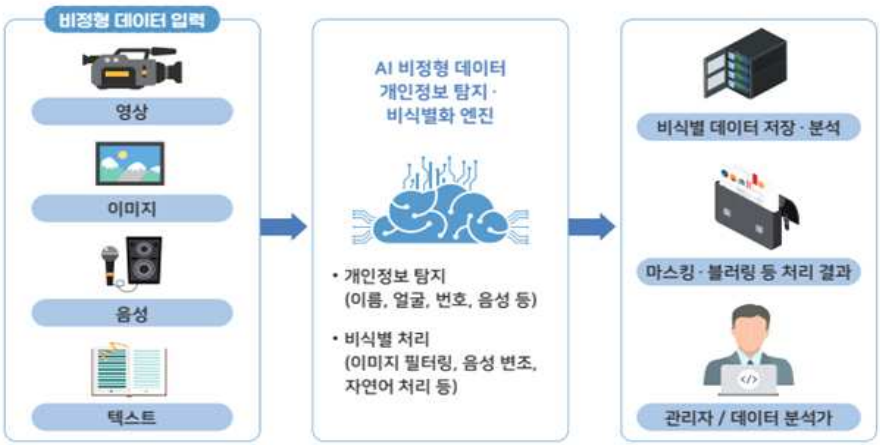


: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
피지컬 AI 실시간 프라이버시 제어		피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술			
			로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술		
			[국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준		
			[국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급 분류 및 인증 기준 국내표준		

11. AI 기반 비정형데이터 개인정보 탐지 · 비식별화

텍스트, 음성·영상 내에서 개인정보를 탐지 및 비식별화하는 기술



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
AI기반 비정형데이터 (영상, 텍스트, 음성 등) 비식별화	멀티모달형 AI 기반 개인정보 탐지 추적 및 비식별화 기술				
			트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 개인정보 탐지용 파운데이션 모델·오픈소스 라이브러리 개발 기술		
			[국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크·지표·시험방법 국제표준		
			[국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스 국내 표준		