2026 정보보호산업계 R&D간담회 개최 계획(안)

('26. 7. 22. (수), KISIA 산업진흥팀)

□ 개요

o (일시) '26. 8. 7.(금) 14:00 ~ 16:00

o (장소) 한국정보보호산업협회 16층 세미나실

※ 서울특별시 송파구 중대로 135 IT벤처타워 서관

o (참석자) IITP 정보보안 PM(신규), KISIA 회원사 등

o (구성) 산업현장 문제해결과 정보보호산업 경쟁력 강화를 위한 R&D 발굴

- (인사 말씀) 정보보호산업계와 IITP 정보보안 PM의 교류 인사
- ① (IITP발표, 약 10분) IITP R&D기술수요조사 설명
- ② (토의, 최대 80분) 산업계에 필요한 R&D지원 방향과 기술수요 논의

※ 각 참석자들은 R&D수요제기 및 기술수요 아이템에 대한 의견 준비 필요
(▲ 필요성 ▲ 연구아이템 등 포함하여 참석자 한 분씩 구두로 발제)

< R&D 기술 분야 : IITP 공고내용 발췌 >

기술분야	세부 기술분야(관련 대분류-중분류)	기술분야	세부 기술분야(관련 대분류-중분류)
①인공지능	•**인공지능** (지능학습AI, 신뢰산업AI, 빅데이터)	⑥정보보안	•**사이버보안**(공통보안, 디지털취약점 분석·시스템 보안, 네트워크·클라우드 보안, 융합보안, 물리보안)
②AI 반도체	•**스마트디바이스**(지능형반도체)		
③양자	•**양자**(양자통신, 양자센싱, 양자컴퓨팅, 양자활성화기술)	⑦미디어 콘텐츠	•**방송콘텐츠** (방송·미디어,콘텐츠, 서비스인프라) •**디지털융합**(메타버스)
④통신 전파위성	•**차세대통신** (이동통신, 네트워크, 전파, 위성통신)	⑧AX융합	•**디지털융합** (블록체인, ESG/탄소중립, 산업융합) * 국방ICT *사회문제해결
⑤소프트웨어	•**소프트웨어** (기반SW, 컴퓨팅시스템, 클라우드, SDx)	⑨피지컬AI	•**스마트디바이스**(자율주행·행동기술, 지능디바이스) •**디지털융합**(디지털 트윈)

특정사업분야	세부 사업분야	특정사업분야	세부 사업분야
⑩국제공동연구	•ICT국제공동연구	⑪표준개발	•ICT표준화

붙임 **정보보호 분야 R&D 투자방향 안내**

《 2027년 정부연구개발투자 방향 및 기준 관련 내용》

◈ 핵심 인프라 보호기술, 양자내성암호(PQC) 등 첨단 정보보호기술 확보를 통해 금융·통신 등 사회 전 분야 사이버침해 대응역량 제고

□ (인프라 보호 기술) 신종 사이버위협 대응을 위해 국가·공공인프라 보호 및 양자내성암호(PQC) 전환 등 국가적 차원 보안 역량 강화

ㅇ 데이터·네트워크·클라우드 등 국가·공공 인프라 보호기술 및 위성, 자율주행차 등 신산업 확산에 따른 신규 위협 대응 기술 개발

- 제로트러스트, 사이버복원력 확보 등 네트워크 보호 기술, 정보보안 표준 기술 개발 등
- 전기자동차, 영상보안플랫폼, 무인이동체 제어시스템 및 인공위성 데이터 보호 기술 등

□ (AI 보안기술) AI 전면 확산에 따른 AI에 대한, AI에 의한 사이버침해 대응, AI 활용 자율 보안 관제 및 블록체인 융합 기술 확보

ㅇ AI 모델·데이터 등 AI 시스템 핵심자산 보호 및 악성코드 생성, 사기 콘텐츠 제작 등 AI 활용 사이버 침해의 사전 억제 기술개발

□ 정보보호 R&D 추진방향

◈ **(정보보호핵심원천기술개발)** ICT 환경변화에 따른 새로운 사이버 위협에 맞서, 정보보호 핵심기술을 개발하며, 데이터 및 네트워크 보호기술, 디지털취약점 분석 및 대응 기술, ICT와 산업 간 융합 보호 기술 등 정보보호 전 기술 영역 포괄

◈ **(AI 사이버 쉴드돔)** 보안 인프라의 全 구간을 보안특화 AI로 유기적으로 결집하여, 국내·외 전방위 위협에 대응하여 위협 전처리부터 자율 방어까지 하나의 시스템처럼 통합 대응하는 기술 개발

◈ **(피지컬AI보안)** 휴머노이드·로보틱스 기반 피지컬 AI의 전체 구조(인식-계획-실행)와 시스템, 거버넌스까지 전주기적 보안을 담보하는 기술개발

◈ **(AI생태계보안내재화)** Agentic AI의 급격한 진화로 AI 모델·서비스·에이전트 전반의 공격 표면이 확대됨에 따라 데이터·모델·외부도구·운영환경이 복합 결합된 AI 서비스 특성을 고려하여 예상되는 모든 취약 지점의 보안성 강화 기술개발

◈ **(범국가양자내성암호전환)** 기존 ICT 인프라 암호체계를 양자컴퓨터의 위협을 막는 '양자내성암호(PQC)' 체계로 전환하기 위한 핵심기술 개발

※ '27년 예산 사정에 따라 상기 내용은 변경 될 수 있습니다.

□ 정보보호 사업별 중점 추진 방향

◈ 정보보호핵심원천기술개발

※ (참고) '27년 사업 방향(안)

① (공모방식 다양화) 현장의 기술 수요와 새로운 시장의 기회를 기업·연구자가 직접 발굴하고 기획하여, 시장 주도로 구조적 전환을 위한 **자유공모** 및

② 기술적 정답이 불확실한 고난이도 주제에 대해 복수의 주체가 제안하고, 단계평가를 통해 검증하여 우수과제 지속 추진하는 **경쟁형** R&D 시범추진

③ (대형·플랫폼화) 보안 기술을 결합하여 단독으로는 불가능한 플랫폼형 보안기술을 발굴하도록 대형 과제 추진

※ 공통적으로 문제를 해결하고, 산업에 실제 적용되어 확산할 수 있는 구조 마련

④ AI·양자 등 혁신 기술에 의한 보안 위협과 데이터 침해 위험 심화에 따라 국내 독자적 암호화·키관리·접근통제 등 기초·원천연구 추진

- ㅇ AI·클라우드 확산으로 민감 데이터의 외부 유출 위험이 급증하는 가운데, 데이터의 기밀성을 유지하면서 분석·활용을 가능하게 하는 프라이버시 보존 기술의 실용화, 금융·의료 등 분야별 데이터 기밀 보장 기술

- ㅇ 6G 기술 규격 설계단계에서 보안 요구사항을 체계적으로 반영하기 위한 6G 보안 아키텍처·프로토콜 등 선행 보안 연구 수행 및 표준화 연계 연구

- ㅇ N2SF 적용에 대응한 등급별 클라우드 보안 체계 및 프라이버시 보존형 데이터 보호 기술 개발 등 변화되는 보안 체계 대응을 위한 기술개발

- ㅇ SBOM 자동 생성 탐지율 고도화, 자산 종속 관계 해결 등 산업에 SBOM 실제 이행을 위한 기술적 한계 돌파를 위한 연구

- ㅇ AI를 공격 도구로 활용한 자동화 침해에 대비하여 레거시 시스템에 대한 AI 기반 자율 탐지·패치 자동화 기술 연구

- ㅇ 실시간 제어·안전 기능이 요구되는 OT·모빌리티 등 신산업 융합 환경에서 실시간 제어·가용성 보장을 위한 사이버 복원력 기술 연구

※ 상기 내용은 기술개발 주제 예시로, 기술수요조사서·예산서·최근 기술동향을 고려하여 과제기획위원회를 통해 과제 기획 예정('26. 12월)

◈ AI 사이버 쉴드돔 기술개발

(개요) 보안 데이터-모델-에이전트-거버넌스로 이어지는 'AI 보안 풀스택 '기반 위협 전처리부터 자율 방어까지 일체화된 소버린 방어체계 실현을 위해 '27년 신규사업으로 추진 중

○ (보안 데이터) 보안 패브릭 구현을 위한 데이터 정제·정합 등 전처리 기술 개발

- 내부 자산과 외부 공급망 연계 자산의 보안 속성 및 정책 정보를 통합 정제하고, 제로트러스트 기반의 동적 가시성을 확보하는 기술 개발
- 초고속·저지연 보장 비복호화 기반 트래픽 분석을 위한 시스템과 암복호화 등 보안 기능을 강화한 시스템 개발

○ (모델) 위협 추론을 위한 LLM 기반 소버린 보안 엔진 기술 개발

- 비복호화 트래픽 분석(ETA), 자산 데이터, 다크웹 등 외부 CTI 등을 기반으로 단일 데이터만으로 식별 불가한 복합 위협을 추론하는 기술 개발
- 자산 가치와 공격 가능성 위협 행위 등을 결합하여 대응 우선순위 판단을 위한 정량적 리스크 관리 지수 산출 기술 개발
- AI 자체에 대한 공격으로부터 시스템을 보호하는 기술 개발

○ (에이전트) 자율방어를 위한 에이전틱AI 기반 위협 대응 기술 개발

- 위협 상황별 최적 방어전략을 수립·실행하고 공격 전개양상과 위험맥락에 따라 보안 정책을 동적으로 생성·최적화하는 지능형 자율 제어 기술 개발
- 침해·취약점 발생 시 스스로 복구·패치하여 복원력을 확보하는 기술 개발

○ (거버넌스) 연합·군집 방어를 위한 협력형 사이버 쉴드 돔 구현 기술 개발

- 개별 기관의 Agentic AI를 유기적으로 제어하는 오케스트레이션 관제와 검증을 수행하는 기술 개발
- 개별 기관에서 탐지된 신종 위협 정보를 연결된 모든 기관에 실시간 전파하고 군집 협업을 기반으로 지능형 조기 예보하는 기술 개발

◈ 피지컬AI보안

(개요) 휴머노이드·로보틱스 분야 피지컬 AI의 전주기적 보안을 담보하는 AI 내재형 자율 예측·복원·제어 보안 기술 확보를 위해 '27년 신규사업으로 추진중

- 피지컬 AI의 데이터·모델·에이전트·제어 전 주기에 대한 융합보안 기술을 개발하여 데이터 유출, 에이전트 오동작 등 보안 위협에 대응

ㅇ 피지컬 AI를 구성하는 HW, 운영체제, 신뢰 인프라 및 통신 프로토콜 전반의 보안 위협에 대응하기 위한 시스템 보안 기술개발

ㅇ 제조 기업의 핵심 자산인 공정 데이터의 생성을 위해 물리 환경을 인식하는 센서(카메라 등) 해킹 대응 및 데이터 신뢰성 보장 기술 등 개발

ㅇ 물리적 제어를 의사결정하는 피지컬 AI 모델 대상 탈옥 및 증류 공격을 통한 역설계(제조 공정 추출) 탐지·대응 등 모델 안전성 확보 기술 개발

ㅇ 제조 AI 에이전트의 오동작 방지가 가능하도록 실시간 관제 및 긴급정지 기술, 설명 가능한 AI 에이전트 감시 기술 등 개발

ㅇ 피지컬 AI 풀스택 생태계에 대한 보안 거버넌스 정립을 위해 보안성 평가·인증, 테스트베드 및 모의훈련, 레드티밍 기술 등 개발

◈ AI생태계보안내재화핵심기술개발

AI 위협 환경의 변동성이 급격히 높아짐에 따라 시의성 있는 현안에 신속 대응할 수 있는 단기 집중 패스트트랙 및 핵심 기술 축적을 위한 중기 전략 과제 지원 예정

ㅇ **(AI 모델·데이터 보호)** AI 시스템의 핵심 자산인 AI 모델과 학습 데이터를 대상으로 하는 탈취·복제·오염 등 외부 위협으로부터 안전하게 보호하기 위한 기술

ㅇ **(AI 응용시스템 보안)** 자율적 판단·외부 도구 호출·다중 에이전트 협업 등 Agentic AI 환경에서 발생하는 새로운 보안 위협에 대응하여 AI 응용시스템의 안전성을 확보하기 위한 기술

ㅇ **(AI 생태계 보안성 평가)** AI 모델의 개발·배포·운영에 디르는 전주기에 걸쳐 보안성을 객관적으로 측정·검증할 수 있는 평가 체계 마련 및 공급망 무결성 확보 기술

◈ 범국가양자내성암호전환핵심기술개발

'35년까지 범국가 PQC 체계 완비를 목표로 하는 「PQC 전환 마스터플랜(과기정통부·국정원)」의 달성을 위한 기술 확보를 위한 과제 추진

○ **('26년 중점 추진)** 기존 취약 암호를 PQC 체계로 안전하게 전환하기 위한 핵심 기술과 PQC 구현 적합성 검증을 위한 기술개발 과제 추진중으로,

○ **('27년 중점 추진)** 양자내성암호 전환 후 주요 도메인과 플랫폼 등 실제 환경에서 올바르게 동작되기 위한 운용·관리·평가 기술 추진 필요

- PQC전환 후 실 환경에서의 취약점 탐색 및 운영 환경에 대한 보안 검증
- PQC를 도입하거나 전환하고자 하는 산·학·연에게 필요한 시험환경 기술
- PQC전환 후 운용 및 관리 시 안전성을 위한 필요 기술 등