공개

의안번호	제 4 호
보 고 연 월 일	2026. 5. 29. (제 9 회)

보고사항

AI 기반 사이버위협에 대응하기 위한
민간 정보보호 추진계획(안)

과학기술관계장관회의

제 출 자	과 학 기 술 정 보 통 신 부 장 관	배 경 훈
제출 연월일	2026. 5. 29.	

AI 기반 사이버위협에 대응하기 위한 민간 정보보호 추진계획(안)(요약)

Ⅰ. 보고주문

○ 「AI 기반 사이버위협에 대응하기 위한 민간 정보보호 추진계획(안)」을 별지와 같이 보고함

Ⅱ. 제안이유

○ 고성능·고위험 AI 보안위협에 대응할 단기대책과, 우리 사회 전반의 정보보호 체계를 AI 기반으로 전환하기 위한 중장기 방향성을 제시

Ⅲ. 주요 내용

1 추진배경 및 현황

□ 美 빅테크는 해커 수준의 사이버보안 역량을 가진 AI 모델을 제한된 기업에만 제공하는 프로젝트 가동, 사이버보안 분야에 화두

○ 동 AI 모델들은 뛰어난 코딩·연산능력으로 빠른 SW취약점 탐지, 해킹툴 자동 생성·실행이 가능하며, 향후 성능 향상 가속화도 예측

※ 전문기관(KISA)이 공개된 AI 모델로 보안솔루션이 없는 기업의 동의를 받아 모의침투한 결과, 실제 취약점 발굴을 통해 기업 내부 네트워크 침입 가능성을 확인

□ 실제로, 앤트로픽 글래스윙 프로젝트 1차 보고서에 따르면 참여사 SW 및 오픈소스에서 1.6만 건 이상의 취약점이 발견되었다고 발표(5.23)

- 또한, 빅테크 AI 모델 공개 경쟁으로 향후 취약점 대량 발굴의 일상화도 우려

< **정부의 대응** > AI 보안 위협에 대한 **리스크 점검과 긴급대응**을 **추진** 중

▲CISO **대비태세 강화요청**(4.14), ▲**CISO·CEO 가이드 및 행동요령 배포**(4.30) ▲주요기업·민간 전문가 등 **5차례 긴급현안점검회의**(~5.8), ▲앤트로픽·오픈AI·구글 등과 **국제협력**(~5.28)
▲글래스윙 1차보고서 취약점 공개(88건) 후 **국내영향 2건 보안공지** 및 **민관군 공유**(5.24)

⇒ **전문가 주요 의견**: ▲**민관군 긴급대응체계** 마련, ▲**취약점 점검·패치·전파의 신속·통합화** ▲기업의 **보안기본기 확립** ▲ AI 보안주권 확립 위한 **특화모델 개발, 보안체계 AI 개편** 등

2 추진 방향

□ 민간분야에서 AI 보안 위협에 대응할 단기과제와, 우리 사회전반의 정보보호 체계를 AI 기반으로 전환하기 위한 중장기 방향성을 제시

▲ **(체계마련)** 범정부 **거버넌스와 협력체계, 민간분야 대응조직** 마련

▲ **(취약점·패치 등 긴급대응)** AI **취약점 및 패치정보를 일원화하여 관리**하고, **민관군에 신속공유 및 전파**하는 한편, 기업·부처에 기술지원 등 추진

▲ **(보호대상별 대응)** 기반시설·산업인프라 등 주요기업은 **강도 높은 점검과 대비태세강화를** 독려하고, **일반인·중소기업**에는 적극적인 **정부지원과 홍보 추진**

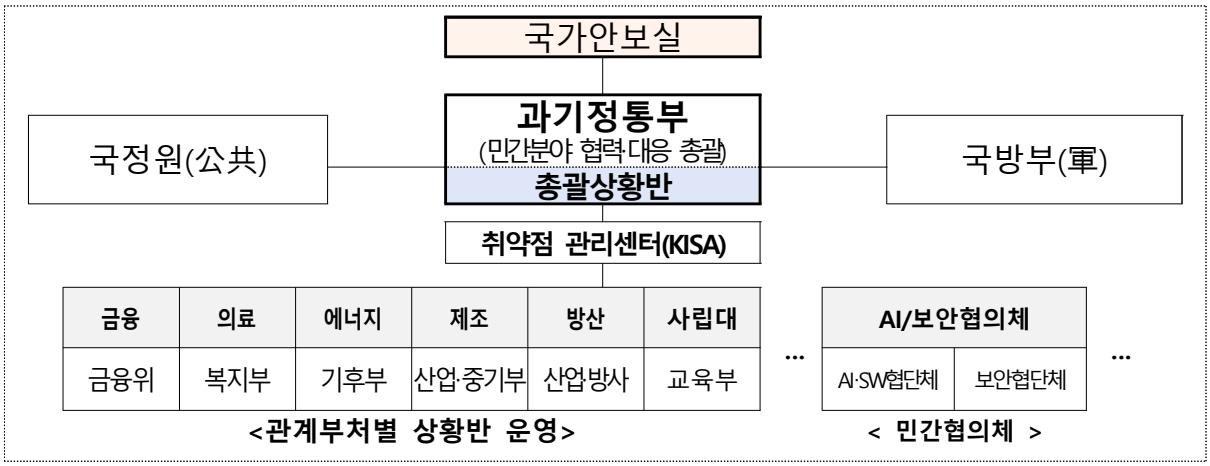
▲ **(AI 보안주권 확립)** 고성능 **AI의 보안 활용 일상화**, **공격무기화에 대비**하여 국내 정보보호 체계를 **독자 AI 기술 기반으로 대전환** 하기 위한 **중장기 방향성 제시**

3 단기 대응과제 ['26.6월~]

1 AI 취약점 공개에 대응하기 위한 민관합동 대응체계 마련

○ (범부처 협력체계) AI 취약점 공개 및 패치, 위협상황 등을 신속 공유·전파하고, 침해사고(정황) 발생시 합동대응 가능한 임시체계 구축

<AI 취약점 대응 범부처 민관협력체계 구성도(안)>



○ (총괄상황반) 과기정통부 內 총괄상황반을 구성하여 상황관리 총괄

- 민간 분야는 소관부처별 상황반(안보실 협조·지원)을 가동하고, KISA 내 취약점 관리센터를 설치하여 기술지원 및 AI 보안위협 대응반(BH) 실무지원 추진

2 취약점 관리센터 중심 취약점·패치 관리 일원화 및 긴급대응 준비

- (취약점 수집·탐지) KISA 취약점 정보포털(KNVD)을 중심으로 대내외 공개 및 신고, 내부입수(AI 활용), 유관기관 공유 등을 통해 취약점 수집
- (취약점 분석 및 분류) 수집된 취약점을 국제 표준(CVSS)에 따라 분류하고, 위험도와 피해파급도 등에 따른 대응 우선순위 도출
- (패치관리) 공유·전파된 취약점에 대한 개발사 등 패치 입수·전파
- (전파·공유) ①보안공지, ②CISO(2.8만개社), ③민간 협력채널(C-TAS, ISAC), ④부처별 상황반·관군 전체에 취약점·패치 공유 및 조치 권고

※ 대규모 사이버 피해 예상시 예경보 발령 등 비상·안정성 보호조치 적용 등 검토

< 취약점 정보포털 (KNVD) 개요 >

- (고성능AI 시범적용) 국제협력을 통해 확보한 최신·고성능 AI 모델을 취약점·패치 업무 및 기업지원 전반에 시범 적용하고 검증(~12월)

※ ▲(**업무적용례**) 오픈소스 취약점 수집/검증 → 자동분석 및 분류 → 패치 생성 및 검증
▲(**기업지원례**) 개인정보(DB)가 포함되지 않은 SW(소스코드) 등 대상 → 수요기업 동의 기반 취약점 발굴 → 조치 방법에 대해서도 AI를 활용해 결과 도출 후 안내 → 기업별 조치

3 피해 파급력이 큰 주요기업 대상 보안 점검 등 추진

각 산업·인프라 등 주요기업은 소관부처의 주관 하에 자산관리 및 AI 기반 취약점 점검을 자체 추진하고, 정부는 이행점검

※ (**대상**) **약 1,200개社**(중복포함) / 피해 파급력이 높은 **정보통신기반시설 및 ISMS 의무기업을 비롯한** 금융, 의료, 에너지 등 **분야별 대형기업 및 상급종합병원·주요 사립대 등**

ㅇ (기반시설) AI 위협 대응을 위해 기존 이행점검에 더해 자산관리·공급망·AI 취약점 점검 집중추진(6월~)

ㅇ (ISMS) 인증기업 대상 '26년 사후(현장) 심사 시 취약점 관리·조치 체계구축 여부, KNVD에서 전파받은 취약점 조치 여부 등 점검(6월~)

4 여건이 부족한 중소기업 대상 보안기본기 확립 집중 지원

자산관리·식별, 공격표면 축소 등 보안기본기 향상을 중점지원하여 AI 위협에도 쉽게 흔들리지 않는 디지털 산업 환경 조성

※ **(대상) '26년** ICT 기반 보유 **중소기업 2,900개사 목표**(과기정통부 예산 활용)

ㅇ (자산식별·관리) 보안 관리의 출발점인 정보자산 관리체계 확립을 위해 미관리·미승인 IT자산 식별을 위한 사례집 배포와 지원 추진

- (가이드) 중기 스스로 IT자산식별·現 보안수준을 진단하고, 보안투자 가이드 및 조치실행 추천 사항으로 구성된 웹도구 배포(6월)

※ 중소기업 대상 보안 컨설팅 및 솔루션 보급(100개사), SECaaS 보급(500개사)도 병행

- (오픈소스 식별·관리) AI가 악용하기 쉬운 오픈소스 취약점을 선제 식별·조치할 수 있도록 SBOM 생성·분석 등 기술지원(8월~, 약 100개사)

ㅇ (공격표면 축소) 여건·역량이 부족한 중소기업 대상 공격표면점검(무상) 및 AI 보안위협 대응을 위한 전문가 상담 제공(16개 지역센터, 2,000개사 목표)

ㅇ (AI 점검인프라 구축) 고성능 AI 모델을 활용한 중소기업 제품(SW) 대상 취약점 점검 등 인프라 제공 및 지원(8월~, 약 200개사)

5 AI 기반 사이버 위협 선제 대응 체계 확립

ㅇ (위협 선제탐지·대응) 전 세계 도메인(약 3.5억건/일)을 상시 모니터링, AI 기반 악성행위(공격준비)와 도메인을 생성 즉시 탐지·대응

○ (침해대응) AI 서비스 관련 침해사고(정황·의심) 발생시, 「침해사고 조사심의위원회」 가동, 신속한 침해사고 조사 및 피해확산 차단(10월~)

6 국제협력을 통한 글로벌 수준의 AI 보안생태계 구축

○ 글로벌 빅테크와 프로젝트 참여 및 정보획득을 위한 협력을 지속하고, AI 안전연구소 네트워크를 통해 프론티어 AI 모델 공동 대응체계 강화

※ 美歐日 등 우방국 사이버보안 기관과 AI 기반 위협대응 및 정보공유 등 협력 강화도 지속 추진

7 대국민 등 홍보 및 대응요령 전파

○ 취약점 발견부터 패치까지 전 단계에 걸쳐 주체별(제조사, 기업·기관·일반인) 대응요령을 마련해 홍보하고, 진단도구 개발 및 배포 등 집중 지원(연중)

※ 보안투자 확대를 위해 주요 산업군 CEO 등 대상 정부 행동요령 기반 릴레이 간담회도 검토

4 중장기 대응과제('27년~): 「AI 보안위협은 AI 보안역량 강화로 대응」

1 독자적 AI 보안생태계 조성

○ (AI 보안주권 확립) 과기정통부가 지원 중인 독자 AI 모델의 경쟁력 향상 등 다양한 수단을 검토해 AI 보안 기술의 자립화를 유도

※ 특히, 취약점 관리센터 및 주요기업 점검을 통해 수집·분석된 취약점 등 데이터는 국내 AI 보안모델 개발 등에 적극 활용될 수 있도록 제도화 검토

○ (보안운영 재설계) 사람 중심의 SW 취약점 탐지 및 수동대응(패치) 등 경직된 프로세스를 AI 중심 자율체계로 전환하기 위한 로드맵 마련

※ 정부 가이드라인, 국내 AI 기반 보안 에이전트 보급 및 실증, 지원사업 등 검토

2 AI 시대 정보보호 체질 개선을 위한 기초체력 확보

○ (제로트러스트 확산) 정부 가이드 및 주요 분야 실증 결과 기반으로 全 사회 제로트러스트 확산을 위한 제도화 검토 및 전환사업 지속 추진

○ (양자내성 원천방어체계) AI-양자 기술발전으로 고조된 암호체계 무력화 위협에 대응하여 PQC 전환을 통해 데이터 해독 공격 대응력 혁신

○ (인력양성) AI 개발·활용 전주기 보안인재로 보안 인력양성 정책 초점을 전환하고, 新 과정 및 인재 플랫폼 구축방향 등 검토

3 AI 자율형 침해대응 및 지원체계 확립

○ (AI 기반 침해대응) 신고·분석, 재발방지, 이행점검, 정보공유 등 KISA 침해대응 체계를 AI 기반 대응체계로 단계적 전환

○ (민간 보안체계) 침해사고 피해기업의 공격표면과 노출된 자산을 AI 에이전트로 진단·검증·조치하는 지능형 위협노출 관리체계 구축

4 주요 정보보호 제도 AI 중심개편

○ 기존 보안체계 기반 주요 정보보호제도·정책(기반시설, 보안평가·인증, ZT, 정보보호 공시, 인력양성 등)을 AI 시대에 걸맞게 재검토 및 개편

5 협조사항 및 향후계획

○ (협조사항) 동 계획 실행을 위해 관계부처 및 기업 등의 적극적인 협조 필요

▲ 민관군 취약점 관리 일원화 및 정보공유 등(**국방부, 국정원**) ▲ 소요예산 검토(**기획처**)
▲ 관계부처 상황반 운영 및 기업 지원(**금융위·복지부·기후부·산업부·중기부·교육부 등**)
▲ 언론 및 대국민 홍보 협조(**문체부**) ▲ 주요기업별 자체점검 및 정부이행점검 협조

○ (향후계획) AI 보안위협 상황을 예의주시하며, 동 계획 지속 점검·보완

과학기술관계장관회의	
회　　차	2026 - 5 (4호)

AI 기반 사이버위협에 대응하기 위한
민간 정보보호 추진계획(안)

2026. 5. 29.

과학기술정보통신부

목 차

1. 추진배경 및 현황 1

2. 주요 환경변화와 국내 영향 1

3. 추진방향 3

4. 단기 대응과제('26.6월~) 3

5. 중장기 대응과제('27년~) 9

6. 협조사항 및 향후계획 11

1 추진배경 및 현황

□ **(배경)** 美 빅테크는 해커 수준의 사이버보안 역량을 가진 AI 모델을 제한된 기업에만 제공하는 프로젝트 가동, 사이버보안 분야에 화두

> **<비공개>** '**미토스**' 기반 앤트로픽 **글래스윙 프로젝트**('26.4.): **공격가능성 및 위험성**을 이유로 MS·구글·리눅스재단 등 **52개 주요 기관·기업만 90일 간 제한 공개**
>
> **<공개>** ▲(앤트로픽) 방어능력이 동일한 **Opus 4.7, Claude Security**는 **신뢰기반 공개**
> ▲(OpenAI) **GPT-5.5 및 GPT-5.5-Cyber는 방어목적 TAC**(Trusted Access For Cyber) 프로그램 운영

□ **(현황)** 동 AI 모델들은 뛰어난 코딩·연산능력으로 빠른 SW취약점 탐지, 해킹툴 자동 생성·실행이 가능하며, 향후 성능 향상 가속화도 예측

※ 전문기관(KISA)이 공개된 AI 모델로 보안솔루션이 없는 기업의 동의를 받아 모의침투한 결과, 실제 취약점 발굴을 통해 기업 내부 네트워크 침입 가능성을 확인

○ 이런 AI 역량이 공·방 양쪽에 이식되면, AI 활용 자율·대규모 공격, 능동형 방어 체계 등 사이버보안 분야 전반의 급격한 변화 예상

> ◇ **정부의 대응**: AI 보안 위협에 대한 **리스크 점검과 긴급대응**을 **추진** 중
> ▲CISO **대비태세 강화요청**(4.14), ▲**CISO·CEO 가이드 및 행동요령 배포**(4.30) ▲주요기업·민간전문가 등 **5차례 긴급현안점검회의**(~5.8), ▲앤트로픽·오픈AI·구글 등과 **국제협력**(~5.28)
> ⇒ **전문가 주요 의견**: ▲**민관군 긴급대응체계** 마련, ▲**취약점 점검·패치·전파의 신속·통합화**
> ▲기업의 **보안기본기 확립** ▲ AI 보안주권 확립 위한 **특화모델 개발, 보안체계 AI 개편** 등

2 주요 환경변화와 국내 영향

□ **(보안체계 변화)** 고성능 AI 모델은 해킹에 필요한 전문 지식과 소요 시간을 크게 단축시키는 동시에, 필요한 인적·물적 자원까지 축소

○ AI 기반의 초 단위 공격과 실시간 새로운 공격 패턴 생성·확산으로 기존 사람 중심의 위협 대응체계는 한계 봉착 예상

□ (취약점 리스크) 앤트로픽 글래스윙 1차 보고서에 따르면 참여사 SW 및 오픈소스에서 1.6만 건 이상의 취약점이 발견되었다고 발표(5.23)

※ 향후 글래스윙 프로젝트 전체 공개(7월 예정)시 알려지지 않은 취약점이 단기간에 더욱 확대 발굴·공유될 가능성

⇒ 정부의 대응: ▲공개된 취약점(88건) 분석, **국내영향 2건에 대해 보안공지**(5.24) 및 **민관군 공유**, ▲전국 CISO(약 2.8만개사) **대비태세 강화요청**(5.25) 등

- 또한, 빅테크의 AI 모델 공개 경쟁으로 향후 취약점 대량 발굴의 일상화도 우려

※ **美 표준기술연구소(NIST)**는 취약점 목록 증가를 감당 불가, **핵심 위험도 기반**(▲실 공격 악용, ▲연방정부사용SW ▲운영체제·브라우저·방화벽 등 안보핵심 SW 취약점 등) **선별 관리체계로 전환**(4.15)

< 국내 환경과 문제점 >

▲(**시스템 환경**) Cloud가 일반적인 해외와 달리, 국내는 망분리와 온프레미스 환경, SI 기반 개별 SW 설치 및 커스터마이징 보편화로 대량·신속 패치 애로

▲(**개발 환경**) SW 개발시 보안이 검증되지 않은 오픈소스 활용이 많아 공급망 취약성과 피해 파급효과도 높은 상황

※ CISO/보안전문가 등 참여한 긴급현안점검회의(5회)에서 전문가들은 **중국 등 여타 국가의 AI 모델 출시 가능성**을 이유로 **금년 말까지를 대응의 골든타임으로 지적**

□ (보안격차 발생) 역량이 부족한 중소기업 대상 공격 집중 가능성과 함께 보안투자 여력 부족으로 인한 'AI 보안 불평등' 가속화도 우려

□ (보안산업 재편) 사이버 공격·방어가 AI를 기반으로 전환됨에 따라 경쟁력 있는 AI 빅테크 기업 중심의 보안산업 재편 전망

※ 세계 보안시장 50% 이상을 차지하는 美 사이버보안 기업이 AI 빅테크 기업과 협력하여 자율 보안 체계까지 구축할 경우 기술 종속 및 국내 보안산업 경쟁력 저하 우려

o 취약점 탐지·분석 및 보안패치 생성 전주기에 AI를 활용할 경우 국내 보안인력의 AI 대체 가속화, 고수준 AI 역량 전문가 수요 증가도 예상

◇ 전문가들은 AI로 인한 기존 보안 체계의 무력화 가능성을 지적하며, 국내 '정보보호 패러다임 전환'이 필요한 시기에 진입했다고 평가

☞ AI가 SW 취약점을 단시간에 대량 발굴하고, 공격 활용 가능성이 있어 '개인·기업·기관' 모두가 AI 사이버 위협 영향권, 대상별 맞춤형 대응 필요

3 추진 방향

□ 민간분야에서 AI 보안 위협에 대응할 단기과제와, 우리 사회전반의 정보보호 체계를 AI 기반으로 전환하기 위한 중장기 방향성을 제시

▲ **(체계마련)** 범정부 **거버넌스와 협력체계, 민간분야 대응조직** 마련

▲ **(취약점·패치 등 긴급대응)** AI **취약점 및 패치정보를 일원화하여 관리**하고, **민관군에 신속공유 및 전파**하는 한편, 기업·부처에 기술지원 등 추진

▲ **(보호대상별 대응)** 기반시설·산업인프라 등 주요기업은 **강도 높은 점검과 대비태세강화를** 독려하고, **일반인·중소기업**에는 적극적인 **정부지원과 홍보 추진**

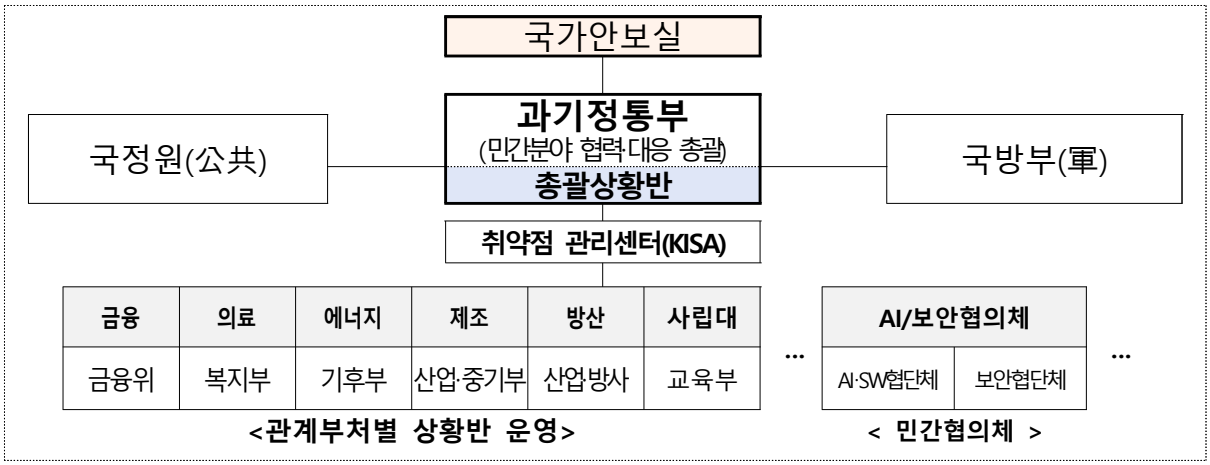
▲ **(AI 보안주권 확립)** 고성능 **AI의 보안 활용 일상화**, **공격무기화에 대비**하여 국내 정보보호 체계를 **독자 AI 기술 기반으로 대전환** 하기 위한 **중장기 방향성 제시**

4 단기 대응과제 ['26.6월~]

1 AI 취약점 공개에 대응하기 위한 민관합동 대응체계 마련

○ (범부처 협력체계) AI 취약점 공개 및 패치, 위협상황 등을 신속 공유·전파하고, 침해사고(정황) 발생시 합동대응 가능한 임시체계 구축

<AI 취약점 대응 범부처 민관협력체계 구성도(안)>



○ (총괄상황반) 과기정통부 內 총괄상황반을 임시구성하여 상황관리 총괄

※ ▲**(구성)** 1개팀(과장1, 사(주)무관 4인, 기존인력 우선활용) ▲**(임무)** 상황관리(취약점수집/패치/피해상황 등), 관계부처별 상황반 핫라인 운영, 국제협력 및 민간협의체 운영, 언론 대응 등

- **(부처별 상황반) 금융·의료 등 주요 분야는 소관부처별 상황반을 가동해 위협상황 관리·공유하도록 협조요청, 필요시 KISA 기업·기술지원 추진**

<**참고: Y2K 사례**> 13대 중점분야 선정, 소관기관 매칭을 통해 실태조사, 예방활동 집중 점검

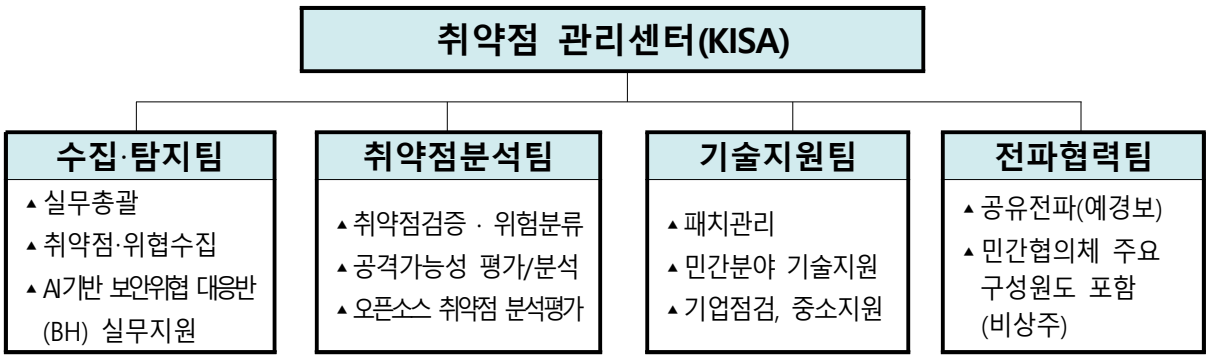
- 전력·에너지(건설교통부·산업자원부) • 원전(과학기술부) • 통신(정보통신부)• 수자원(건설교통부·환경부)
- 운송(건설교통부·철도청·경찰청) • 해운항만(해양수산부) • 금융(행정자치부·한국은행) • 환경(환경부)
- 의료(보건복지부·식품의약품안전청) • 국방(국방부) • 중소기업(중소기업청) •산업자동화설비(산업자원부) •중앙과 지방행정기관(행정자치부)

⇒ 초동대응을 위해 일단 기존 조직·인력을 최대한 활용하되, 취약점 대규모 공개 등으로 인한 긴급상황 발생시 관계부처 추가 협의

ㅇ (취약점관리센터) KISA 內 취약점 및 패치정보를 통합관리·공유·전파하고 기업 및 유관기관 기술지원, AI 보안위협 대응반(BH) 실무지원

※ ▲**(구성)** 1개 단 40명 수준 기존인력 구성, 기관 인력 상황을 고려 보안기업 등 민간전문가 포함

▲**(임무)** ①취약점 모니터링·탐지 → ②분석(평가) → ③조치 및 민간분야 기술지원 → ④공유·협력·전파(필요시 경보·비상중단) → ⑤정책 대응 건의 등 전주기 취약점 관리대응 실무



※ 국정원, 국방부 등 협조를 통해 민관군 취약점, 패치정보의 즉각적인 공유/전파 추진

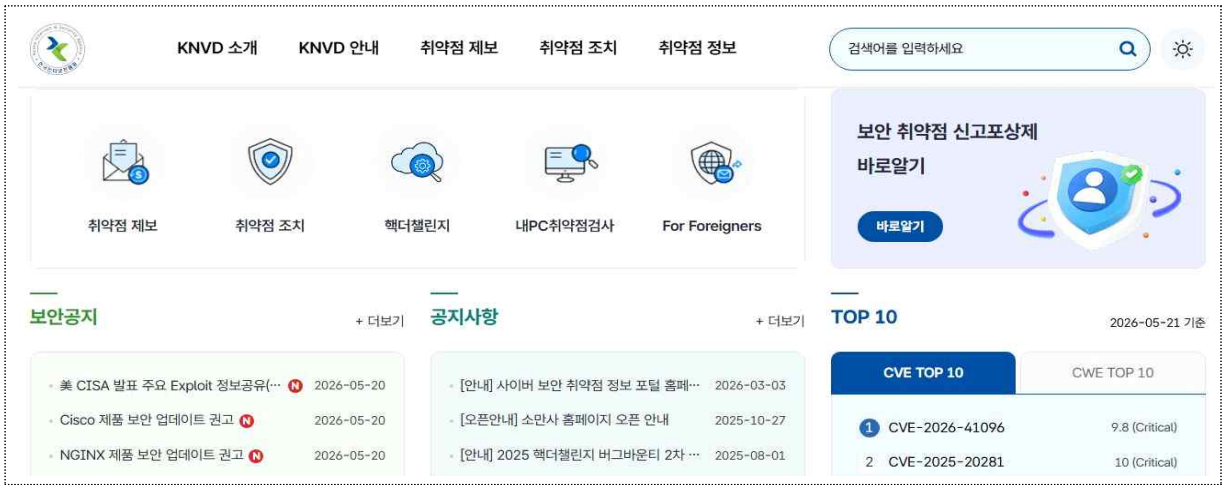
ㅇ (민간협의체) AI 및 보안기업·협단체 등이 참여하는 통합협의체를 구성하여 AI 위협 및 취약점 공유 및 전파, 공동대응 등 협력 추진

※ ▲(보안협의체) AI 취약점 평가·위험등급·우선순위 공동평가 및 전문가 자문

▲(AI협의체) 제조사(임시)패치에 대한 검증 및 안정성, 환경 테스트 지원 및 자문

2 취약점 관리센터 중심 취약점·패치 관리 일원화 및 긴급대응 준비

< 취약점 정보포털 (KNVD) 개요 >



① (취약점 수집·탐지) KISA 취약점 정보포털(KNVD)을 중심으로 대내외 공개 및 신고, 내부입수(AI 활용), 유관기관 공유 등을 통해 취약점 수집

② (취약점 분석 및 분류) 수집된 취약점을 국제 표준(CVSS)에 따라 분류하고, 위험도와 피해파급도 등에 따른 대응 우선순위 도출

※ (오픈소스) 최신 AI 모델을 활용, 주요 오픈소스 취약점을 정기점검 후 결과와 조치사항을 민관군 등에 전파하기 위한 시범 검증체계 운영(~12월)

③ (패치관리) 공유·전파된 취약점에 대한 개발사 등 패치 입수·전파

- (긴급알림) 취약점 클리닝 서비스(C-clean)를 통한 취약 SW 제거 안내 및 최신 보안 패치 적용 안내, 보안 공지 및 긴급 알림서비스 추진

※ 공격 가능성 및 위험도가 높은 취약점은 패치 배포 전까지 대체 SW 사용 권고, 특정 기능 비활성화 등 긴급조치 방안을 마련하여 신속 전파

- (기술지원) KISA는 민간 전문가와 함께 기업 취약점 점검 및 패치 적용 과정의 기술지원 및 상담, 관계부처 요청에 따른 지원추진

④ (전파·공유) ①보안공지, ②CISO(약 2.8만개社), ③민간 협력채널(C-TAS, ISAC), ④ 부처별 상황반·관군 전체에 취약점·패치 공유 및 조치 권고

- 위험도가 높은 취약점은 기업·기관이 즉시 파악·대응하기 위해 보안 공지 API 제공 및 디지털자산 위협 징후 즉시 알림서비스* 제공

* (예시) A 기업 보유 SW: Apache 2.5 → Apache 2.5 취약점 발견 시 A기업에 즉각 통지

- 대규모 사이버 피해가 예상되는 경우 예·경보 발령 등 비상·안정성 보호조치 적용 등 검토

○ (고성능AI 시범적용) 국제협력을 통해 확보한 최신·고성능 AI 모델을 취약점·패치 업무 및 기업지원 전반에 시범 적용하고 검증(~12월)

※ ▲(**업무적용례**) 오픈소스 취약점 수집/검증 → 자동 분석 및 분류 → 패치 생성 및 검증
▲(**기업지원례**) 개인정보(DB)가 포함되지 않은 SW(소스코드) 등 대상 → 수요기업 동의 기반 취약점 발굴 → 조치 방법에 대해서도 AI를 활용해 결과 도출 후 안내 → 기업별 조치

○ (국제협력) 국제협력 기반의 취약점 정보 공유 및 공동대응체계 운영

- 글로벌 CERT·CSIRT 및 국제 협의체(FIRST, APCERT), MITRE, 보안기업 등과 위협정보 공유, 국제 공동 대응 및 기술 협력 추진

3 피해 파급력이 큰 주요기업 대상 보안점검 등 추진

▲(대상) 주요기업 약 1,200개社(중복포함)
※ 피해 파급력이 높은 **정보통신기반시설 및 ISMS 의무기업을 비롯한** 금융, 의료, 에너지 등 **분야별 대형기업 및 상급종합병원·주요 사립대학 등**

⇒ 각 산업·인프라 등 주요기업은 소관부처 주관 하 자산관리 및 취약점 점검을 자체 추진하고, 정부는 이행점검

① (기반시설) AI 위협 대응을 위해 기존 이행점검에 더해 자산관리·공급망·AI 취약점 점검 집중추진(6월~)

② (ISMS) 인증기업 대상 '26년 사후(현장) 심사 시 취약점 관리·조치 체계구축 여부, KNVD에서 전파받은 취약점 조치 여부 등 점검(6월~)

4 여건이 부족한 중소기업 대상 보안기본기 확립 집중 지원

자산관리·식별, 공격표면 축소 등 보안기본기 향상을 중점지원하여 AI 위협에도 쉽게 흔들리지 않는 디지털 산업 환경 조성

▲**(대상) 중소기업 약 10만개社*** **내외 ⇒ '26년 2,900개社 목표**(과기정통부 예산활용)

* ICT 기반 보유 **중소기업 18만개社 중,** 자력대응 가능기업(매출 50억↑등) 제외시 규모

ㅇ (자산식별·관리) 보안 관리의 출발점인 정보자산 관리체계 확립을 위해 미관리·미승인 IT자산 식별을 위한 사례집 배포와 지원 추진

- (가이드) 중소기업 스스로 IT자산식별·現 보안수준을 진단하고, 보안투자 가이드 및 조치실행 추천 사항으로 구성된 웹도구 배포(6월)

※ 중소기업 대상 보안 컨설팅 및 솔루션 보급(100개사), SECaas 보급(500개사)도 병행

ㅇ (공격표면 축소) 여건·역량이 부족한 중소기업 대상 공격표면점검(무상) 및 AI 보안위협 대응을 위한 전문가 상담 제공(16개 지역센터, 2,000개사 목표)

ㅇ (오픈소스 식별·관리) AI가 악용하기 쉬운 오픈소스 취약점을 선제 식별·조치할 수 있도록 SBOM 생성·분석 등 기술지원(8월~, 약 200개사)

ㅇ (AI 점검인프라 구축) 고성능 AI 모델을 활용한 중소기업 제품(SW) 대상 취약점 점검 인프라 제공, 전문가 조치 지원(8월~, 약 100개사)

5 AI 기반 사이버 위협 선제 대응 체계 확립

ㅇ (위협 선제탐지·대응) 전 세계 도메인(약 3.5억건/일)을 상시 모니터링, AI 기반 악성행위(공격준비)와 도메인을 생성 즉시 탐지·대응

(예시) ① **AI로 생성 가능한 악성행위의 특징정보를 AI에 학습**시켜 사이버 공격 준비 단계에서 **위협을 사전 탐지·차단 수행**

② **국민 다수 이용 서비스를 사칭한 악성도메인**이 AI에 의해 대량 생성되더라도 즉시 탐지·대응 가능한 **AI 모니터링 체계 운영**

○ (침해대응) AI 서비스 관련 침해사고(정황·의심) 발생시, 「침해사고 조사심의위원회」 가동, 신속한 침해사고 조사 및 피해확산 차단(10월~)

6 국제협력을 통한 글로벌 수준의 AI 보안생태계 구축

○ (AI 협력확대) 공공·외교·민간 채널 등 가용수단을 총동원하여 글로벌 AI 기업 프로젝트 관련 정보공유 및 AI 모델 접근권 확보

- 글로벌 AI 선도기업과 협력체계를 구축하고, AI 안전성 평가 등 AI 위험에 공동 대응 추진

※ ▲(**앤트로픽**) 실무회의(아시아총괄, 4.21), 고위급 면담(제2차관-글로벌총괄, 5.11)
▲(**오픈AI**) TAC 워크숍(국가안보정책총괄, 관계부처 등 참여, 5.18), 고위급 면담(제2차관-CSO, 5.26)
▲(**구글**) 실무회의(과기정통부-아태 AI보안정책담당 등 5.28)

○ (AI 안전네트워크) 英(의장국)·美·日·EU 등 10개국이 참여하는 AI 안전 연구소 네트워크를 통해 프론티어 AI 모델 공동 대응체계 강화

※ 美歐日 등 우방국 사이버보안 기관과 AI 기반 위협대응 및 정보공유 등 협력 강화도 지속 추진

7 대국민 등 홍보 및 대응요령 전파

○ (기업문화 혁신) 자산관리·공격표면 축소, 사이버 복원력 대비 등 보안 기본기 확립을 경영 최우선 목표로, CEO 등 고위급의 관심과 투자 유도

※ AI 위협 파급력이 큰 주요 산업군 CEO 등 대상 정부 행동요령 기반 릴레이 현장간담회 검토

○ (대응요령) 취약점 발견부터 패치까지 전 단계에 걸쳐 대응요령을 마련하고, 주체별(제조사, 기업·기관·일반인) 가용 채널을 확보하여 신속 홍보

○ (인식전환·홍보) 제15회 정보보호의 날(7.8)을 계기로 사회 전반의 AI 보안패러다임 전환 공감대 확산과 관심 유도

※ AI 보안 全 영역을 다루는 글로벌 해킹방어대회(AI Cyber Defense Contest) 개최를 통해 AI 보안위협과 취약점을 선제 발굴하고, 세계 수준의 AI 화이트햇 선발(12월)

5 중장기 대응과제('27년~): 「AI 보안위협은 AI 보안역량 강화로 대응」

1 독자적 AI 보안생태계 조성

○ (AI 보안주권 확립) 과기정통부가 지원 중인 독자 AI 모델의 경쟁력 향상 등 다양한 수단을 검토해 AI 보안 기술의 자립화를 유도

- 특히, 취약점 관리센터 및 주요기업 점검을 통해 수집·분석된 취약점 등 데이터는 국내 AI 모델 경쟁력 향상 등에 적극 활용되도록 제도화 검토

○ (AI 보안기술 확보) 신종 AI 보안위협에 대응할 핵심기술 개발 추진

- AI 해커의 다단계 공격에 대비, 위협 인지-방어 재구성-안전상태 복구 등을 AI가 자율적으로 수행하는 핵심기술* 확보

* **탐지**(AI 해커 공격징후 감지·모니터링) → **방어**(공격 탐지시 네트워크 차단, 상위 보안 모델 전환 등 자율 판단 방어) → **복구**(강화학습 기반의 AI 자가 복구, 복원, 롤백 등)

- AI 보안 풀스택(데이터-엔진-에이전트-거버넌스)을 기반으로 국내외 전방위 해킹위협을 실시간 탐지 및 선제 예측하는 'AI 사이버 쉴드 돔' 기술개발

2 AI 자율형 침해대응 및 지원체계 확립

○ (AI 기반 침해대응) 신고·분석, 재발방지, 이행점검, 정보공유 등 KISA 침해대응 체계를 AI 기반 대응체계로 단계적 전환

※ (예) 민간분야 침해사고 대응 업무절차에 AI 도입하여, 침해사고 신고 시 사고원인 분석 및 재발방지 대책 수립 등 효율화 기대

○ (민간 보안체계) 침해사고 피해기업의 공격표면과 노출된 자산을 AI 에이전트로 진단·검증·조치하는 지능형 위협노출 관리체계 구축

※ **CTEM 체계**(Continuous Threat Exposure Management) ① 위협표면 자율 진단 → ② 심층 분석·교차검증 → ③ 최적 조치방안 자율 수립·판단 → ④ 조치 플레이북 자동생성·조치 → ∞

3 AI 시대 국가 정보보호 체질 개선을 위한 기초체력 확보

○ (제로트러스트 확산) 정부 가이드 및 주요 분야 실증 결과 기반으로 全 사회 제로트러스트 확산을 위한 제도화 검토* 및 전환사업 지속 추진

* (예) 제로트러스트 성숙도 진단·등급제 신설, ISMS-P / 정보보호수준평가 / 정보보호공시 內 ZT 성숙도 심사(공개)항목 신설 등 검토

- (주요분야 대전환) 보안사고 발생 시 국민에게 직접적인 피해가 발생하는 분야(금융, 통신, 의료 등)를 우선 선정하여 집중 전환 지원

< 제로트러스트 도입가속화을 위한 절차 >

① 보안현황 진단	② 보안모델 개발	③ 연동 및 통합	④ 실사용망 도입	⑤ 단계적 확산
시스템 접근 대상에 대한 분석 및 가시화	제로트러스트 아키텍처 신규 설계 및 도입 방안 수립	기존 보안체계와 신규 아키텍처의 보안 정책 연계	실제 솔루션 및 플랫폼 구성 후 업무망 전반에 구현	고위험 업무 영역부터 적용하여 전사 확산 추진

○ (보안운영 재설계) 사람 중심의 SW 취약점 탐지 및 수동대응(패치) 등 경직된 프로세스를 AI 중심 자율체계로 전환하기 위한 로드맵 마련

○ (양자내성 원천방어체계) AI-양자 기술발전*으로 고조된 암호체계 무력화 위협에 대응하여 PQC 전환을 통해 데이터 해독 공격 대응력 혁신**

* 양자컴 상용화 한계를 보완하는 세계 최초 오픈소스 양자 AI 모델 발표(NVIDIA 아이징, 4.14.) 등

** 現 암호화된 데이터를 미리 수집·저장 후, 향후 상용화된 양자컴으로 데이터를 해독하는 HNDL(Harvest Now Decrypt Later) 공격 등에 대해 PQC는 데이터가 탈취되더라도 해독을 방지

○ (인력양성) AI 개발·활용 전주기 보안인재로 보안 인력양성 정책 초점을 전환하고, 新 과정 및 인재 플랫폼 구축 방향 등 검토

4 주요 정보보호 제도의 AI 중심 개편

○ 기존 보안체계 기반 주요 정보보호제도·정책(기반시설, 보안평가·인증, ZT, 정보보호 공시, 인력양성 등)을 AI 시대에 걸맞게 재검토 및 개편

- 주요 제도의 기반 개편방향 모색을 위한 정책연구 추진

6 협조사항 및 향후계획

○ (협조사항) 동 계획 실행을 위해 관계부처 및 기업 등의 적극적인 협조 필요

▲ 민관군 취약점 관리 일원화 및 정보공유 등(**국방부, 국정원**) ▲ 소요예산 검토(**기획처**)
▲ 관계부처 상황반 운영 및 기업 지원(**금융위·복지부·기후부·산업부·중기부·교육부 등**)
▲ 언론 및 대국민 홍보 협조(**문체부**) ▲ 주요기업별 자체점검 및 정부이행점검 협조

○ (향후계획) AI 보안위협 상황을 예의주시하며, 동 계획 지속 점검·보완

과학기술정보통신부 정보보호네트워크정책실 정보보호네트워크정책관 정보보호산업과	
담당자	박세진 사무관
연락처	전 화 : 044-202-6455 E-mail : parksejin0622@korea.kr