관계부처합동 | 보도참고자료 | 국민이 만든 회복과 도약, 모두의 1년 대전환의 길

보도시점 2026.5.29.(금) 12:00 (2026.5.30.(토) 조간) 배포 2026.5.28.(목) 18:00

해커수준의 AI 사이버위협, 민관이 함께 대응

과기정통부, 「AI 기반 사이버위협 대응 민간 정보보호추진계획 발표」

- 민관이 합심하여 AI 사이버위협에 대응하고, AI 보안주권 확립에 총력
- 과기정통부를 중심으로 민간분야 소관 부처 상황 대응체계 운영
- 주요기업은 보안대비태세 강화, 중소기업은 보안기본기 확립 만전

【관련 국정과제】 23-4. AI 시대를 지탱하는 견고한 디지털 보안 안전체계 구축

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')는 5월 29일(금), **제9회 과학기술관계장관회의에서 「AI 기반 사이버위협에 대응하기 위한 민간 정보보호 추진계획(안)」을 발표**하였다.

최근 美 빅테크는 보안전문가 수준의 사이버보안 역량을 가진 AI 모델을 제한된 기업에만 제공하는 프로젝트를 가동하여 화두가 되고 있다. 실제로, 앤트로픽 글래스윙 프로젝트 1차 보고서(5.23)에 따르면, 참여사 SW 및 오픈소스에서 1.6만 건 이상의 취약점이 발견되었다고 발표한 바 있다.

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

향후 이런 고성능 AI를 통한 취약점 대량 발굴 일상화가 예상되는 가운데, 실제 보안조직에는 상당한 부담도 우려된다. 특히, 발굴된 취약점이 사이버 공격에도 활용될 가능성이 있어 '개인·기업·기관' 모두가 AI 위협 영향권에 있다는 것이 전문가들의 지적이다.

이에 과기정통부는 이번 계획을 통해 민간분야에서 AI 보안 위협에 대비하기 위한 긴급조치와, 우리 사회 전반의 정보보호 체계를 AI 기반으로 전환하기 위한 중장기 방향성을 제시하기로 하였다. 주요 내용은 다음과 같다.

▲ **(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

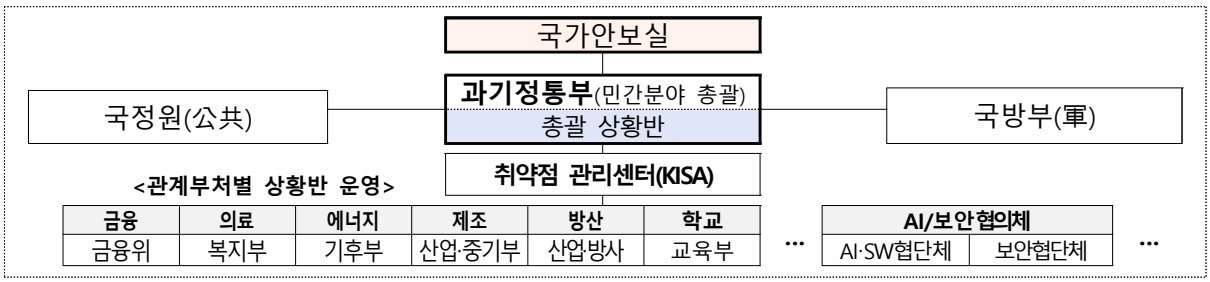
▲ **(보호대상별 대응)** 기반시설·산업인프라 등 주요기업은 **강도 높은 점검과 대비태세강화를** 독려하고, **일반인·중소기업**에는 적극적인 **정부지원과 홍보 추진**

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

1 AI 취약점 공개에 대응하기 위한 민관합동 대응체계 마련

우선 정부는 청와대 국가안보실을 중심으로 AI 취약점 공개 및 패치, 위협상황 등을 신속 공유·전파하고, 침해사고(정황) 발생시 합동대응 가능한 긴급체계를 구축하는 한편, 과기정통부 내에는 총괄상황반을, 민간 분야는 소관 부처별 상황반을 가동하기로 하였다.

<AI 취약점 대응 민관협력체계 구성도(안)>



2 취약점 관리센터 중심 취약점·패치 관리 일원화 및 긴급대응 준비

한편, 한국인터넷진흥원(이하 'KISA') 내 취약점 관리센터를 설치하여 취약점·패치 관리를 일원화하고, 관계부처 및 기업 기술지원을 추진한다.

특히, KISA 취약점 정보포털(KNVD)을 중심으로 대내외 공개 및 신고, 유관기관 공유 등을 통해 취약점과 패치를 광범위하게 수집 및 분석하는 한편, 이를 보안공지, 기업 정보보호최고책임자(CISO, 약 2.8만개社), 민간 협력채널(C-TAS, ISAC), 부처별 상황반·관군 전체에 신속 공유 및 조치 권고하는 긴급 대응체계를 구성한다.

또한, 과기정통부가 국제협력을 통해 확보한 최신·고성능 AI 모델을 위와 같은 취약점·패치 업무 및 기업지원 전반에 시범 적용도 추진한다.

※ ▲(**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 주요기업은 보안대비태세 강화, 중소기업은 보안기본기 확립 만전

AI 보안위협 관련 피해 파급력이 큰 주요기업에 대해서는 보안대비태세 강화를 위해 각 소관부처의 주관 하에 자산관리 및 취약점 점검, 패치 대응 등을 자체 추진하도록 하고, 정부는 분야별 이행점검을 추진한다.

※ (**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**

중소기업은 보안 관리의 출발점인 자산 관리체계 확립을 위해 스스로 IT 자산식별·現 보안수준을 진단하고, 이에 기반한 보안투자 가이드 및 조치실행을 추천해주는 웹 도구를 배포하는 한편, AI가 악용하기 쉬운 오픈소스 취약점을 선제 식별·조치할 수 있도록 SW구성명세서 생성·분석 기술지원도 추진한다.

아울러 공격 표면점검 및 전문가 상담을 제공하여 혹시 모를 사이버공격 범위 축소에 만전을 기하고, 과기정통부가 접근권을 확보한 고성능 AI 모델을 활용하여 중소기업 제품(SW)의 취약점 점검 등 인프라를 제공하여 AI 위협에도 쉽게 흔들리지 않는 디지털 산업환경 조성을 유도한다.

4 AI 기반 사이버 위협 선제 대응 체계 확립

AI 보안위협에 빠르게 대응하기 위해 전 세계 도메인(약 3.5억건/일)을 상시 모니터링하는 한편, AI 기반 악성행위(공격준비)와 도메인을 생성 즉시 탐지하고 대응한다. 또한 AI 서비스 관련 침해사고(정황·의심) 발생시, 「침해사고조사심의위원회」를 즉각 가동하여 신속한 침해사고 조사 및 피해확산 차단을 도모하기로 하였다.

5 국제협력을 통한 글로벌 수준의 AI 보안생태계 구축

오픈 AI의 정부·기관용 신뢰기반 접근프로그램(GTAC) 확보를 시작으로, 글로벌 빅테크와 AI 보안 프로젝트 참여 및 정보획득을 위한 협력을 지속하는 한편, 우방국 사이버보안 기관과 AI 기반 위협대응 및 정보공유 등 협력 강화도 추진한다.

6 대국민 등 홍보 및 대응요령 전파

뿐만 아니라 취약점 발견부터 패치까지 전 단계에 걸친 주체별(제조사, 기업·기관·일반인) 대응요령을 마련해 전파하고, 보안투자 확대를 위한 홍보도 지속 추진할 예정이다.

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

7 AI 보안위협은 AI 보안역량 강화로 대응

마지막으로, 향후 고성능 AI의 보안 활용 일상화, 공격무기화에 대비하여 '27년부터는 국내 정보보호 체계를 독자 AI 기술 기반으로 대전환 하고, AI 보안주권을 확립하기 위한 다양한 프로젝트를 기획하여 과감히 실행할 예정이다.

배경훈 부총리는 "최고 수준의 해커와 견줄 정도로 사이버보안 분야의 AI 발전 속도가 빠른 상황으로, 우리나라도 AI 시대에 걸맞은 보안 체계와 글로벌 협력을 갖추지 못한다면 AI 3대 강국 도약도 흔들릴 수밖에 없다"라며, "이번 대책을 통해 AI 발 대규모 취약점 공개에 대응하기 위한 긴급체계를 마련하고, 우리의 기술과 모델을 기반으로 한 AI 보안주권 확립도 속도감 있게 추진해 나가겠다" 라고 밝혔다.

담당 부서	정보보호네트워크정책실 정보보호산업과	책임자 담당자	과 장 사무관	이종혁 박세진	(044-202-6450) (044-202-6455)