

5 미국, 'AI 혁신 및 안보 증진' 행정명령 및 AI 국가안보각서 발표

➔ 미국 트럼프 대통령은 사이버보안과 국가안보 분야 각각에서 AI를 핵심 수단으로 활용하기 위한 지침과 이행방안을 담은 행정명령*과 국가안보각서**에 서명(26.6)

* Executive Order: Promoting Advanced Artificial Intelligence Innovation and Security

** National Security Presidential Memorandum/NSPM-11

- (개요) 트럼프 행정부는 AI 패권 전략의 연장선상에서 AI를 사이버보안 및 국가안보에 신속히 적용하기 위해 새로운 행정명령과 대통령 국가안보각서를 발표
 - (행정명령) '첨단 AI 혁신 및 안보 증진' 행정명령은 미국의 AI 산업 리더십을 유지하는 동시에, AI가 제기하는 새로운 안보 위협 속에서 급속히 발전하는 AI의 사이버 역량을 국가 방어 체계에 적극 활용하는 것을 목표로 마련
 - AI 규제를 최소화하면서도 국가안보와 주요 기반시설 방어력을 강화할 수 있도록 정부와 민간이 협력하는 체계를 구축하는 데에 초점을 설정
 - (안보각서) AI 국가안보각서(NSPM-11)는 미군 및 정보기관에 AI 기술을 신속히 배치하고, AI 시스템의 제어 가능성과 책임성을 강화하는 것이 핵심
 - AI가 미국 역사상 국가안보에 가장 혁신적인 변화를 가져올 기술 중 하나가 될 것이라고 강조하면서, 미군 및 정보공동체(Intelligence Community)가 최신 AI 기술을 사용할 수 있도록 보장하는 체계를 새로이 구축할 것을 지시
- (행정명령) 관련 부처·기관들에 ▲첨단 AI 기반 보안 체계 구축 ▲프론티어 AI 모델 대상 국가 관리 체계 도입 ▲사이버 범죄 단속 강화 등을 지시

1. AI 기반 보안 체계 구축

- 주요 연방기관들에 행정명령이 내려진 날로부터 30일 이내에 AI 기반 보안 체계를 구축하는 작업에 착수할 것을 명시

〈 AI 기반 보안 체계 구축 관련 주요 지시 사항 〉

기관별 이행 과제

- 국가안보체계위원회(CNSS)는 국가안보 시스템의 사이버 방어를 최우선 과제로 지정하고 신속한 조치에 착수
- 전쟁부는 부처 정보시스템 사이버 방어를 우선시하며 적절하고 신속한 조치에 착수
- 국토안보부 산하 사이버보안·인프라보안국(CISA)은 관리예산국(OMB), 국가사이버국장(National Cyber Director) 등과 협력해 다음 내용을 포함하는 운영 지침을 마련해 발표
 - 정부 산하 기관들의 방어력 강화
 - AI 기반 방어 도구 도입 확대
 - 지방정부, 농촌 병원, 지역 은행, 주요 기반시설 운영기관들에서 최첨단 사이버보안 도구·서비스(프론티어 모델 등) 활용 지원

- 또한 재무부 주도로 정부 기관들과 민간 AI 기업이 함께 참여하는 ‘AI 사이버 보안 클리어링하우스’^{*}를 설립해 소프트웨어 취약점 발견·검증 및 패치 배포 등에서 정부·민간 공동 대응 체제를 구축할 것을 촉구

^{*} AI Cybersecurity Clearinghouse: 소프트웨어 취약점 스캐닝 작업 조정 및 중복 탐지 방지, 발견된 취약점 검증 및 우선순위 부여, 취약점에 대한 패치 개발 및 배포 조율 등을 수행할 허브 기관

2. 프론티어 AI 모델 국가 관리 체계 도입

- 국가안보 및 주요 기반시설에 위협을 초래할 수 있는 고성능 AI 시스템에 대해 연방 정부의 검토·관리 체계를 구축을 지시
- ‘대상 프론티어 모델’^{*} 개념을 적용해 고위험 프론티어 AI 모델을 국가 관리 체계 내에서 식별·평가할 수 있는 기반 마련

^{*} Covered Frontier Model: 고도화된 사이버 공격 또는 방어 능력을 보유한 최첨단 AI 모델을 의미

- 국가안보국(NSA) 등을 중심으로 특정 AI 모델이 ‘대상 프론티어 모델’에 해당 하는지 평가할 수 있는 비공개 벤치마킹 체계^{*} 구축을 지시

^{*} 모델 개발 기업이 정부와 자발적으로 협력하여 프론티어 모델 해당 여부를 사전 협의하고, 공개 30일 전 정부에 사전 접근 권한을 제공하는 협력 프레임워크

- 이를 통해 정부가 모델 공개 전 보안 위협을 사전 검토하고, 주요 기반시설 운영기관 및 신뢰할 수 있는 보안 파트너의 조기 접근을 지원하는 것이 목적
- 다만 해당 체계가 신규 AI 모델의 개발·배포·공개에 대한 허가제 또는 사전 승인제를 의미하지 않으며, 규제보다 자율적 협력 중심의 관리 기조임을 강조

3. 사이버 범죄 단속 강화

- 법무부에 컴퓨터 시스템에 대한 무단 침입, 데이터 침해, AI를 활용한 기타 불법 접근 및 범죄 행위에 관한 연방법 집행을 우선 과제로 추진할 것을 촉구
- 특히 AI 에이전트를 이용해 시스템에 무단 접근하거나 탈취한 정보를 범죄 목적으로 활용하는 행위 등에 적극적으로 대처하도록 지시

- (AI 안보각서) 관련 부처·기관들에 안보 분야에서 AI 활용을 위한 ▲정책 원칙 준수 ▲정책·지침 업데이트 ▲안보 역량 강화 ▲AI 도입 역량 구축 조치를 지시

- (정책 원칙) AI 개발 및 활용에 대한 행정부의 정책 원칙으로 ①도입 가속화, ②임무 환경에 맞게 상용·오픈소스 기술 적용, ③AI 기술의 신뢰성·견고성·조종 가능성·제어 가능성 보장, ④책임 있는 활용을 강조

〈 국가안보 분야 AI 개발·활용을 위한 4가지 정책 필라(Pillar) 〉

구분	주요 내용
AI 도입 가속화 (Adaptation)	• AI가 작전 효율을 향상시킬 수 있는 임무 영역을 파악하고, 신속한 도입을 가로막는 불필요한 장벽을 제거함으로써 AI 도입을 가속화 • 국가안보 체제(국가안보 정책 관련 모든 정부기관·조직 등)는 산업계와의 긴밀한 협력 관계를 통해 최첨단 모델을 안보 전문가들에게 신속하게 제공하고, 기술 우위를 확보하는 동시에 잠재적 응용 분야 전반에 걸쳐 신속한 실험·검증을 추진
임무 환경에 맞게 상용·오픈소스 기술 적용 (Adaptation)	• 국가안보 체제는 상용·오픈소스 AI 기술을 적용하고, 다양한 공급업체를 활용하며, 선정된 AI 기술이 임무에 맞게 최적화되도록 보장 • 보안 또는 임무상의 제약으로 상용 솔루션 사용이 적절하지 않은 경우, 자체적으로 AI 기술을 개발하거나 개발한 AI 기술 배포도 가능
AI 기술의 신뢰성·견고성·조종가능성 ·제어가능성 보장 (Assurance)	• 국가안보 체제는 도입된 AI 기술이 신뢰성·견고성·조종 가능성·제어 가능성을 갖도록 설계되었는지, 관련 법률·정책·지침에 따라 운영되는지를 보증 • 국가안보 체제는 상업 기업을 포함한 어떤 외부 기관도 사전 승인 없이 미국 전투원이 임무 수행에 사용하는 AI 시스템의 사용을 방해하거나, 성능을 저하시키거나, 변경할 수 없도록 보장 • 국가안보 체제 전반에 걸쳐 AI 시스템의 기밀성, 무결성, 신뢰성, 가용성, 상호운용성 보장을 위한 시험·평가·검증 등 엄격한 보안·기능 조치 시행
책임 있는 활용 (Accountability)	• 표현의 자유 검열이나 이념적 편향 주입, 미국 국민에 대한 불법 감시 등을 위한 AI 기술 개발 및 활용 금지 • 모든 지휘 단계에서 책임 있는 AI 활용 보장

- **(정책·지침 업데이트)** 국가안보 정책 및 지침을 정책 원칙에 맞게 정비할 것을 요구하면서, 새로운 국가안보각서가 바이든 행정부 시절의 AI 국가안보 각서(NSM-25)* 및 관련 지침을 폐지·대체함을 명시

* National Security Memorandum-25: 바이든 행정부에서 발표된 국가안보 분야 AI 활용 지침으로 국가안보 관련 조직들이 AI를 개발·도입·운용할 때 따라야 할 원칙과 절차를 규정

- **(안보 역량 강화)** 국가안보 역량 강화를 위해 여러 공급업체로부터 최첨단 AI 모델을 신속하게 도입하고, 차세대 AI 시스템을 대규모로 운영할 수 있는 고보안 AI 컴퓨팅 시설을 구축하며, 민간 기업과 협력할 것을 강조
- **(AI 도입 역량 구축)** 연방 정부 내 AI 인재 채용을 가속화하는 동시에, 민간 AI 전문가로 구성된 'AI 국가안보 전략 예비군(AI National Security Strategic Reserve)'을 설립할 것을 지시

〈 국가안보 분야 AI 개발·활용을 위한 주요 지시 사항 〉

구분	주요 내용
정책·지침 업데이트	• AI 무기 체계와 관련해 자율 무기체계 정책을 개정하고, 매년 재검토 실시 • 정책 원칙에서 벗어난 행태를 반복하는 기업과의 조달 계약 해지 • 국가안보체계위원회(CNSS) 등은 국가안보 체계 AI 사용 거버넌스 정책 발표 • 정책 원칙에 맞게 모든 안보 관련 정책·지침 업데이트 및 매년 재검토 • NSM-25는 폐지
국가안보 역량 강화	• 전쟁부 및 정보기관들은 최첨단 AI 모델의 신속한 도입을 위해 국방 조달 절차를 검토·업데이트 • 대통령 과학기술보좌관(APST)과 OMB는 국가안보 체제의 모든 요소가 최첨단 컴퓨팅 자원에 충분히 접근할 수 있도록 보장하는 로드맵을 개발 (차세대 AI 시스템의 대규모 운영을 지원하는 고보안 AI 컴퓨팅 시설 구축 계획 등 포함) • 전쟁부 등은 미국의 AI 기술을 보호하기 위해 민간 기업과 파트너십 구축 • 에너지부는 AI 기반 과학연구 이니셔티브인 ‘제네시스 미션(Genesis Mission)’을 통해 관련 기관과 협력하며 AI를 국가안보 임무에 적용하기 위한 역량 개발 • 외국의 AI 기술, AI 응용 프로그램 및 활용, AI 거버넌스·정책에 대한 정보 수집 및 분석 실시 • 국가정보국, 전쟁부, 에너지부 등은 공동 AI 데이터 및 모델 교환 실시
AI 도입 역량 구축	• 연방 정부에 AI 기술 인재 채용 가속화 • 인사관리처는 민간 AI 전문가로 구성된 ‘AI 국가안보 전략 예비군’ 설립해 필요 시 AI 국가안보 문제 해결에서 연방 정부를 지원하도록 보장 • 국가정보국은 국가안보를 위한 AI 교육과정을 개발·시행 • AI의 신뢰성, 견고성, 조종 가능성, 제어 가능성에 대한 연구개발 우선시 • AI 시스템의 기밀성, 무결성 및 가용성을 보장하기 위한 AI 위험관리 및 보증에 대한 공동 전략과 구현 지침 개발 • 국가안보 분야 AI에 대한 표준화된 테스트·평가·검증 방법론 개발

출처 : 미국 백악관 (2026.6.2.)

<https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>

<https://www.whitehouse.gov/presidential-actions/2026/06/national-security-presidential-memorandum-nspm-11/>

<https://www.whitehouse.gov/fact-sheets/2026/06/fact-sheet-president-donald-j-trump-signs-historic-directive-on-ai-in-the-national-security-enterprise/>