3 EU 집행위원회, '사이버 보안 및 AI 액션플랜' 발표

유럽연합집행위원회(EC)는 최첨단 AI가 초래하는 사이버 보안 리스크에 대응하기 위해 EC·회원국·EU기관*·산업계가 이행할 조치를 담은 액션플랜**을 발표('26.7)

* EU 사이버보안청(ENISA), EC 산하 공동연구센터(JRC), 유럽사이버보안역량센터(ECCC) 등

** Action plan on Cybersecurity and Artificial Intelligence

- **(배경)** 최첨단 AI 모델 도입으로 사이버 보안 환경이 급격히 변화함에 따라, 고성능 AI가 사이버 보안 생태계에 미치는 영향에 대비해야 할 필요성이 고조
  - 프론티어 AI 모델은 사이버 보안 준비 태세를 강화하고, 위협 탐지·대응을 개선해 사이버 복원력을 크게 높일 수 있는 잠재적 기회를 제공
  - 그러나 다른 한편으로는 사이버 공격을 자동화·정교화할 뿐만 아니라 공격의 규모와 속도를 전례 없는 수준으로 끌어올릴 위험이 존재
  - 현재는 소수의 AI 모델·시스템만이 프론티어 수준의 역량을 보유하고 있으나 오픈소스 모델들이 꾸준히 개선되면서 기술 격차가 좁아지는 양상이 포착
  - 결과적으로 향후 프론티어 수준의 AI 역량에 접근하기는 점점 더 쉬워지고, 악의적인 행위자들도 이를 악용해 더 복잡한 공격을 실행할 것으로 예상
- **(개요)** EC는 AI 시대를 맞아 변화하는 사이버 보안 패러다임에 대응하기 위해 AI와 사이버 보안을 연계한 액션플랜을 마련해 공개
  - AI 기술로 인한 사이버 보안 리스크에 대응하는 동시에 AI를 활용해 사이버 방어 역량을 강화하고 AI의 안전하고 책임 있는 사용을 지원하는 것이 목적
  - 액션플랜은 그 자체로 법적 구속력은 없으나 EU의 기존 AI 및 사이버 보안 관련 법적·제도적 기반*을 보완하고 관련 시행을 뒷받침할 전망

    * EU의 AI법(AI Act), NIS2 지침(NIS2 Directive), 사이버복원력법(Cyber Resilience Act) 등
- **(주요 내용)** ▲프론티어 AI의 안전성·접근성·배포용이성 ▲AI 시대를 준비하는 EU 사이버 생태계 ▲사이버 보안을 위한 유럽의 AI 역량이라는 3가지 필라를 중심으로 EC·회원국·EU기관·산업계가 협력해 이행할 9가지 핵심 조치들을 제시
  - **(AI 모델 평가)** 프론티어 AI 모델이 배포되기 전에 안전성을 평가할 수 있는 기관 대부분이 역외에 있는 문제를 극복하기 위해 EU 자체의 AI 검증 역량을 갖추는 것을 가장 중요한 조치 중 하나로 명시
  - 이를 위해 EC는 AI법 시행*과 연계해 제3자 평가기관에 대한 기준을 정립하는 등 관련 제도와 생태계를 정비·육성하고, 사이버 보안 분야를 포괄해 EU의 모델 평가 역량을 구축하기 위한 특별 공모전도 진행할 방침

    * EU AI법('26.8.2. 시행)은 최첨단 AI 모델에 대한 사전 평가 의무를 도입

- **(AI 모델 접근성)** 또한 공공·민간이 고성능 AI 보안 시스템에 안전하게 접근할 수 있는 구조적 방법을 규정·제시하는 청사진을 마련해 발표할 예정
- **(AI 모델의 배포 용이성)** 국가 주요 인프라 운영기관들을 위해 AI 모델의 보안 성능을 모의 테스트할 수 있는 가상 플랫폼도 제공할 계획
- **(사이버 보안을 위한 AI 역량)** 이에 더해 AI 기반 사이버 보안 솔루션 개발을 촉진하는 경진대회도 운영할 예정

〈 3대 필라와 9가지 핵심 조치 〉

필라	핵심 조치
유럽의 사이버 보안을 위한 프론티어 AI의 안전성·접근성·배포 용이성 확보	① 사이버 보안 기능을 포함해 AI 모델에 대한 EU 차원의 평가 역량 구축('27년, EC) – 제3자 평가기관에 대한 기준 제안, 특별 공모전 개최 등 ② 사이버 보안 목적의 고성능 AI 역량에 대한 구조화된 접근방법을 규정·제시하는 EU 차원의 청사진 마련('26년 4분기, EC·ENISA) – 이로써 EU 조직들이 고급 AI 기반의 사이버 보안 역량에 안전하고 적시에 접근할 수 있도록 지원 ③ 고성능 사이버 보안 역량을 갖춘 AI를 안전하게 테스트할 수 있는 플랫폼 개발('26년 4분기, ENISA·JRC) – 이를 통해 사이버 보안 분야에서 AI의 신속하고 안전한 배포 촉진
AI 시대를 위한 EU 사이버 생태계 정비	④ AI 기반 위협에 대한 보호를 강화하고, 사이버 보안 작업에 AI를 안전하게 통합하기 위한 지침·권고·자문·모범사례 등을 발표('26년 3분기 현재부터, ENISA 등) ⑤ 기존 취약점 관리 관행·도구를 AI 시대에 맞게 개선·정비('26년 3분기 현재부터, EC·회원국·ENISA·산업계) ⑥ 주요 오픈소스 프로젝트의 심각한 취약점을 파악하기 위한 '중요 오픈소스 복원력 캠페인(Critical Open Source Resilience Campaign)' 시범 실시('26년 4분기, ENISA 등) – 캠페인에서 AI를 활용한 취약점 패치 가속화 방안도 검토
사이버 보안을 위한 유럽의 AI 역량 확대	⑦ AI 기반 사이버 보안 솔루션의 개발·확산을 촉진하기 위한 대회(EU Grand Challenge on AI for cybersecurity) 개최('26년 4분기, EC·ECCC·ENISA) – 기업·연구원·기관들에 AI 기반 사이버 보안 솔루션을 개발하는 장 제공 ⑧ 복원력 강화 목적으로 이용 가능한 고성능·프론티어 AI 모델이 주권적 컴퓨팅 인프라에서 테스트·훈련·배포될 수 있도록 AI 팩토리의 컴퓨팅 역량에 대한 접근권을 제공하는 데 주력(EC·회원국) ⑨ 사이버 보안 전문가가 AI를 사이버 보안 목적으로 활용하는데 필요한 역량을 키울 수 있도록 AI 활용 교육 모듈 개발('26년 4분기, EC·회원국·산업계)

출처 : 유럽연합집행위원회 (2026.7.7.)
https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence