교육부 보도자료

배포 2026. 4. 22.(수) 08:30 보도시점 (인터넷)2026. 4. 22.(수) 12:00
(지 면)2026. 4. 23.(목) 조간

교육부 인공지능(AI) 기반 사이버 보안관제로 안전한 인공지능(AI) 활용 교수·학습을 지원한다

- 지능화·조직화된 사이버침해 위협에, 자체 개발하여 특허 등록한 '사이버침해 인공지능(AI) 자동 판별 및 자동 통보' 시스템으로 대응
- 고도화된 인공지능(AI) 보안관제 시스템을 활용하여 고위험 악성코드 사이버 공격에 집중 대응하는 등 더 세밀한 보안관제 실시
- '인공지능(AI) 사이버안전센터' 개소(4.23.), 민간 클라우드 서비스까지 보안관제 영역 확대를 통해 교육기관에 더욱 특화된 인공지능(AI) 보안관제 모델로 고도화 추진

교육부(장관 최교진)와 한국교육학술정보원(원장 정제영)은 지능화되어 증가하는 사이버 공격에 대응하고자 자체 개발 및 특허 등록한 '사이버침해 인공지능(AI) 자동 판별 및 자동 통보' 시스템을 세밀하게 고도화한다. 또한 교육기관들의 원활한 인공지능(AI) 교수학습을 위해 이용 중인 민간 클라우드 서비스까지 보안관제 범위를 확대한다고 밝혔다.

교육부는 435개 교육기관*의 24시간 365일 사이버 보안관제와 침해사고 대응을 위하여 한국교육학술정보원을 전담기관으로 지정해 "교육부 사이버안전센터"(ECSC : Ministry of Education, Cyber Security Center)를 운영 중이다. 사이버공격에 효율적으로 대응하고자 지난 2022년부터 '인공지능(AI) 기반 사이버침해 자동 판별'을 자체 개발하여 도입하였고, 2025년에는 '인공지능(AI) 기반 자동 통보' 기능을 추가하는 고도화를 통해 실질적인 '인공지능(AI) 기반 사이버 보안관제' 기반을 마련하였다.

* 교육부 및 소속기관(7), 대학(385), 공공기관(23), 유관기관(3), 시도교육청(17, 유·초·중등학교는 시도교육청 자체 관제)

< 인공지능(AI) 기반 사이버침해 자동 판별 및 통보 시스템 >

○ **(분석 모델)** 트랜스포머*(Transformer) 모델을 기반으로 DNN 등 여러 머신러닝 및 딥러닝 알고리즘을 결합한 앙상블 모델(CMAE, Convolutional Multi-Head-Attention Ensemble)
* 문장을 이해하고 처리하는 딥러닝 모델 구조로, GPT(OpenAI), LLaMA(Meta), BERT(구글)에서 활용

○ **(자동 판별)** 수집·표준화된 위협정보를 AI 탐지규칙에 학습시킨 후 자동 판별 적용, 침입시도·악성코드 감염·경유지 악용의 경우 90% 일치 시 자동 판별, AI 자동 판별 결과 이유 설명 기능(XAI, Explainable AI), 15만 건 사이버위협을 1분 만에 판별하고 정확도 최고 98.8%

○ **(자동 통보)** AI가 판별한 위협정보 중 정확도 99% 이상, 동일 IP 30건 이상의 침입시도 공격 유형의 경우 AI가 공유시스템에 자동 등록하고 해당 기관에 자동 통보하는 기능 수행

교육부 ‘인공지능(AI) 사이버 보안관제 시스템’은 정부부처 ‘보안관제종합시스템’ 중 최초의 인공지능(AI) 보안관제 적용이며, 국내 최초 인공지능(AI) 보안관제 특허 등록*을 마쳤다.

* 국내 최초 인공지능(AI) 보안관제 특허 등록, “네트워크에 대한 침해 공격을 탐지하는 장치, 방법 및 컴퓨터 프로그램”, 제10-2651655호, ’24.3.22. 한국교육학술정보원 등

< 교육부 사이버안전센터(ECSC) 인공지능(AI) 보안관제 체계 >

교육부는 ‘인공지능(AI) 사이버 보안관제’를 통하여 2025년 435개 교육기관에 설치한 탐지장비로 총 약 4.8억 건의 사이버침해 징후를 탐지하고, 이 중 약 8.6만 건을 사이버침해로 판별해 대응하였다. 인공지능(AI) 보안관제 고도화 전인 2024년 약 6.3만 건 대비 36% 증가한 성과이다. 이는 ▲주요 침해 의심 사고를 대상으로 실시하는 초동조사 및 심층점검을 대폭 강화, ▲대국민 공개된 교육기관 홈페이지 등에 대한 상시 점검에 공격표면관리(ASM)* 점검을 신규 추가, ▲최근 급증하는 랜섬웨어·가상화폐 채굴형 악성코드 대규모 침해 공격에 적극 대응하는 등 정밀한 보안관제의 결과이다.

* 외부 노출된 정보기술(IT) 자산이 자체적으로 갖는 취약점에 대해 점검하는 최신 보안 점검 기술로 2025년부터 보안관제에 도입, 435개 교육기관의 약 13만 개 보안 취약점 도출

아울러, 교육부와 한국교육학술정보원은 4월 23일(목) ‘교육부 인공지능(AI) 사이버안전센터’(이하, 인공지능(AI) 사이버안전센터)를 정식 개소한다고 밝혔다.

인공지능(AI) 사이버안전센터는 인공지능(AI)을 활용하여 교육기관의 사이버공격 데이터 수집·분석·대응과 민간 클라우드 서비스 이용 확대에 따른 실시간 보안관제 기능을 수행한다.

※ 교육기관 민간클라우드 서비스 이용 현황(’25.4월) : 435개 교육기관 중 158개 기관에서 477개 서비스 이용 중

교육부는 이를 위해 지난 2025년 7월부터 민간 클라우드 서비스 업체와 연계하여 교육부 사이버안전센터와 연동되는 탐지 장비를 민간 클라우드 서버에 설치하고, 탐지 규칙 및 탐지 결과의 안전한 송·수신을 시범 운영하였다.

※ ('25년) NAVER, NHN, KT 3개 사 연동 테스트 완료, ('26년) 7개 사 테스트 추진 예정

교육부와 한국교육학술정보원(KERIS)은 2026년도 12월까지 시도교육청별 보안·네트워크·서버 장비를 통해 수집된 접속기록(Log)을 '인공지능(AI) 사이버 보안관제 시스템'에 학습시켜 교육기관에 더욱 특화된 모델로 고도화할 예정이다.

2027년부터는 '교육부 사이버안전센터(ECSC)'에서 운영 중인 '인공지능(AI) 사이버 보안관제 시스템'을 시도교육청 보안관제에도 적용하여, 교육기관에 대한 사이버 침해 시도에 대해 공동의 데이터 수집·분석·대응할 수 있도록 추진할 계획이다.

이윤홍 인공지능인재지원국장은 "최근 인공지능(AI) 기술 확산으로 정보보호 환경이 급변함에 따라, 새로운 인공지능(AI) 사이버보안 대응체계를 빠르게 구축해야 한다."라고 말하며, "진화하는 사이버침해에 대응하기 위해 국가정보원과 긴밀한 협조체계를 구축하고, 교육부의 인공지능(AI) 기반 사이버 보안관제 시스템을 더욱 세밀화·고도화하여 학생, 교원, 학부모 모두가 신뢰할 수 있는 안전한 인공지능(AI) 교육환경을 조성하고자 최선을 다하겠다."라고 밝혔다.

정제영 한국교육학술정보원장은 "교육기관의 인공지능(AI) 사이버안전센터 운영을 통해 교육청과 대학의 사이버침해에 대응하는 동시에, 이용률이 점차 증가하고 있는 민간 클라우드 서비스에도 수준 높은 '인공지능(AI) 사이버 보안관제' 서비스를 제공하여 정보보호 사각지대를 해소하겠다."라고 밝혔다.

【붙임】 1. 교육부 AI 사이버안전센터 개소식 개요
2. 교육부 AI 사이버안전센터(ECSC) 현황

【참고】 보도자료 내 정보보안 용어 해설

담당 부서	인공지능인재지원국 정보보호팀	책임자	과장	이정석 (044-203-5502)
		담당자	사무관	이진구 (044-203-6519)
			주무관	김현동 (044-203-7064)
	한국교육학술정보원 정보보안부	책임자	본부장	안재호 (053-714-0496)
		담당자	부장	김동우 (053-714-0495)
			책임연구원	장지화 (044-203-7102)

붙임1 **교육부 AI 사이버안전센터 개소식 개요**

□ 개요

○ (일시/장소) ’26.4.23.(목) 10:30/정부세종청사 12동 402호

○ (주관) 교육부(정보보호팀), 한국교육학술정보원(정보보호본부)

○ (참석) 총 16명

- (교육부) **인공지능인재지원국장**, 정보보호팀장, 담당자 등
- (KERIS) **원장,** 정보보호본부장, 정보보안부장, 담당자 등
- (유관기관) **국가정보원 세종본부, 국가사이버위기관리단**
- (민간업체) ㈜**SK쉴더스 부사장**, 유지보수 업체 대표 등

○ (내용) AI 기반 사이버공격 자동 판별 및 침해위협 자동 통보시스템 소개, 최근 교육분야 사이버위협 대응상황 보고 등

□ 세부 일정(안)

일자	시간	내용	비고
4/23 (목)	10:30～11:00	현판식(기념촬영)	비공개
		개소식 참석자 소개 및 인사	
		환영사 (KERIS 정제영 원장)	
		축사 (교육부 인공지능인재지원국장)	
		축사 (국정원 세종본부장)·	
	11:00～11:40	교육부 AI 사이버안전센터 소개	
		. 중동 관련 교육분야 사이버위협 대응상황 . AI 기반 사이버공격 자동판별체계 현황	
	11:40～	정리 및 해산	

붙임2 교육부 AI 사이버안전센터(ECSC) 현황

< 교육부 AI 사이버안전센터(ECSC : Ministry of Education, AI Cyber Security Center) >

❖ 교육기관을 대상으로 정보시스템 보호를 위해 사이버 위협 정보를 수집·분석·대응할 수 있는 AI 보안관제 센터(전담기관 : 한국교육학술정보원)

○ 설립 근거

- 「국가사이버안전관리규정」(대통령령) 제316조
- 「교육부 사이버안전센터 운영규정」(교육부 훈령 제528호)

○ 주요 기능

- 보안관제 대상기관*의 24시간×365일 보안관제 실시

  * 435개 기관(교육부와 소속기관 7, 시도교육청 17, 대학 385, 공공기관 23, 유관기관 3)

- AI 기반 사이버위협 정보의 실시간 수집, 분석, 통보, 조치 등 대응
- 보안취약점 점검 및 침해요인 대응 관련 정보 제공
- 교육기관이 이용하는 민간 클라우드까지 사이버보안 관제 실시
- 클라우드 서비스 보안취약점 점검 및 침해요인 대응 관련 정보 제공 등
- 사이버안전 관련 매뉴얼 배포, 국내외 기술·연구 조사 및 간행물 발간

[교육기관 보안관제 체계]

○ **국가보안관제(국정원)**
- 국가·공공기관 보안관제

○ **부문보안관제센터(교육부)**
- 소속기관(6), 대학(385), 공공기관(23), 유관기관(3)

○ **단위보안관제센터**
- 17개 시도교육청(소속기관 및 각급 학교(초중등))
- 한국방송통신대학교
- AI 디지털 교육자료 통합보안관제센터

참고 **보도자료 내 정보보안 용어 해설**

순	용어	해설
1	사이버보안관제	네트워크, 서버 등 정보화(ICT) 자원을 대상으로 발생하는 교육기관 사이버 공격을 24시간 AI를 활용한 실시간 탐지·분석·대응하는 활동
2	클라우드 서비스 (Cloud Service)	인터넷을 통해 외부 민간 데이터센터의 ICT 자원(저장공간, SW 등)을 필요한 만큼 빌려 쓰는 방식
3	트랜스포머 (Transformer Open source Tool)	데이터 속 단어들 사이의 관계를 분석하여 복잡한 사이버공격 흐름을 전후 맥락까지 고려하여 판별하는 데 활용되는 오픈소스 ※ 챗GTP 핵심 기반 기술로 알려져 있음
4	DNN (Deep neural network)	인간의 뇌세포가 신호를 전달하는 구조를 본떠 만든 AI 기술로 사람이 일일이 지정하던 해킹 패턴을 스스로 파악하여 더 정밀하게 방어 가능
5	머신러닝 (Machine Learning)	AI가 데이터 규칙을 스스로 학습하여 일정한 패턴이나 규칙을 찾아내는 기술로 사이버공격 시 과거의 학습 데이터를 바탕으로 위험여부 판단 가능
6	딥러닝 (Deep Learning)	머신러닝의 한 종류로 AI가 인간의 뇌처럼 데이터를 스스로 분석하고 학습하는 기술로 데이터의 숨겨진 특징에서 아주 정교하고 지능적인 사이버공격까지 구별 가능
7	앙상블 모델 (CMAE*)	트랜스포머 모델을 기반으로 DNN 등 여러 머신러닝 및 딥러닝을 결합하여 단일 모델보다 더 정확한 분석 결과를 도출하는 기술 * Convolutional Multi-Head- Attention Ensemble
8	XAI (Explainable AI)	지능적인 사이버공격에 대한 AI의 위험여부 판단 근거를 사람이 이해할 수 있게 설명하여 보안 전문가의 신속한 대응과 신뢰도 상승을 돕는 기능
9	경유지 악용	해커가 추적을 피하려고 보안이 취약한 교육관련 기관의 서버를 공격 거점(경유지)으로 삼아 우회적 해킹에 활용하는 수법
10	랜섬웨어	해킹을 통해 사용자 데이터를 탈취한 후 암호화하여 열지 못하게 한 뒤 복구를 대가로 금전을 요구하는 악성코드
11	가상화폐 채굴형 악성코드	사용자 몰래 시스템 성능을 가상화폐 채굴에 동원하여 속도 저하를 일으키는 프로그램
12	접속기록(Log)	시스템 접속 시 활동 기록(5W1H 파악을 위한 최소한의 데이터 세트로 ID, 접속일시, 접속지 정보, 정보주체 정보, 수행업무)으로 해커의 이동 경로 추적 및 증거로 활용