'26년 AI·XR 얼라이언스 윤리제도분과 2차 회의 결과

('26.9.7.(월), MDIA 정책기획팀)

□ 회의 개요

○ (일시/장소) 9월 1일(화), 오후2시~4시 / MDIA 회의실

○ (참석자) : 총 13명(오프라인 9명/온라인 4명)

□ 논의 내용

○ (발제1) AI 시대의 사이버보안 위협과 중소기업 정보보호 지원 정책

○ (발제2) AI 시대 사이버보안 위협과 기업의 법적 책임 및 대응 방안

□ 세부 일정

시 간		세부내용	비고
14:00 ~ 14:10	10분	참석자 소개 및 회의 안내	사무국
14:10 ~ 14:40	30분	▸ AI 시대의 사이버보안 위협과 중소기업 정보보호 지원 정책 - 20분 강연 / 10분 질의응답	KISA 정현철 연구위원
14:40 ~ 14:50	10분	휴식	
14:50 ~ 15:20	30분	▸AI시대 사이버보안 위협과 기업의 법적 책임 및 대응 방안 - 20분 강연 / 10분 질의응답	김앤장 김도엽 변호사
15:20 ~ 15:40	20분	발제 관련 질의응답 및 자유토의	참여자 전원
15:40 ~ 16:00	20분	하반기 운영 논의 및 마무리	분과장 및 분과원

□ 회의 내용

○ AI 시대의 사이버보안 위협과 중소기업 정보보호 지원 정책 발제 (KISA 정현철 연구위원)

1. AI 기반 사이버공격의 고도화
- AI 확산으로 해킹 공격이 대중화·정교화·자동화되고 있으며, 취약점 탐색부터 공격 설계·익스플로이 체이닝까지 자율적으로 수행하는 수준으로 발전
- 공격 비용과 소요시간이 크게 감소하면서 인터넷에 노출된 중소기업도 공격 대상이 될 가능성이 높아짐
- 에이전트 AI 활용 확산에 따라 내부 시스템과 연결된 NHI 및 Shadow AI 관리 등 새로운 보안 과제 발생

2. 중소기업 보안의 구조적 한계
- 보안 전담인력이 부족하고 패치·탐지·차단 등 지속적인 보안 관리에 어려움이 있어 공격자와 방어자 간 비대칭적 위협에 노출
- 공급망을 통해 중소기업의 침해가 대기업·공공기관 등으로 확산될 수 있어 중소기업 보안 강화의 중요성이 높아지고 있음

3. 중소기업의 우선 대응방안
- 모든 보안체계를 한 번에 구축하기보다 ASM을 통한 인터넷 노출 자산 점검 및 불필요한 노출 차단, 취약점·패치 관리 등 기본적인 보안조치를 우선 강화할 필요
- 자체 인력 확보가 어려운 경우 클라우드·SaaS 기반 구독형 보안서비스를 활용하고 정부의 컨설팅·솔루션 지원사업을 적극 활용할 필요

4. AI 보안 기술 및 정책적 과제
- 에이전트 AI의 신원·권한 관리, Shadow AI 탐지·관리, NHI 생명주기 관리 등을 위한 AI 보안 기술개발 및 R&D·실증 지원 필요
- 기술개발과 함께 국제 표준화 논의에도 적극 참여해 국내 기술의 경쟁력 확보 필요
- 침해사고 신고가 처벌·과징금으로만 이어질 경우 기업의 신고 기피가 발생할 수 있으므로 면책·비밀보장·인센티브 등 신고 유인체계 마련 필요

○ AI 시대 사이버보안 위협과 기업의 법적 책임 및 대응 방안 발제
(김앤장 법률사무소 김도엽 변호사)

1. AI 에이전트의 자율성과 법적 쟁점
- AI 에이전트는 최소한의 인간 개입으로 의사결정·계획·행동을 수행하며, 기존 챗봇보다 높은 자율성을 보유
- 에이전트의 행위에 대해 운영자·공급자·이용자 중 누가 책임을 질 것인지 기존 법체계만으로 판단하기 어려워 새로운 기준 마련 필요

2. AI 에이전트의 권한 및 투명성 관리
- 에이전트의 데이터 접근에 대해 최소 권한·권한 차등 부여 및 자동 회수 등을 적용하고, 중요 의사결정에는 인간의 최종 승인 절차 마련 필요
- 사용자, 실행 시각, 도구 호출 등 에이전트의 활동 기록을 남겨 투명성과 책임성 확보 필요

3. 개인정보 및 기업정보 보호
- 에이전트의 메모리·학습 데이터 등에 개인정보가 잔존할 수 있어 보유기간 및 파기 기준을 명확히 설정할 필요
- 프롬프트에는 개인정보뿐 아니라 기업의 노하우·기밀정보가 포함될 수 있어 영업비밀 등 중요정보에 대한 관리체계 마련 필요
- 외부 AI 이용 시 개인정보 국외이전 등 관련 법적 의무와 함께 기술적 보호조치를 검토할 필요

4. 기업의 대응 방향
- AI 활용 단계에서부터 접근권한·접속기록·정보 파기 등을 반영하는 Privacy by Design 방식의 관리체계 구축 필요
- 에이전트의 자율성·데이터 민감도 등에 따라 위험도 기반의 권한 통제 및 가드레일을 적용하고, AI DLP·게이트웨이 등을 활용해 중요정보의 외부 전송을 차단할 필요

붙임 AI·XR 얼라이언스 윤리제도분과 2차 회의 참석 명단

□ 대상 인원 : 총 13명

구분	소속	성명	직급	비고
학계	법무법인 비트	송도영	변호사	분과장
	김앤장 법률사무소	김도엽	변호사	발제자
연구계	한국전자통신연구원	강신각	책임연구원	
	한국전자통신연구원	현욱	책임연구원	온라인
기관	정보통신산업진흥원	김성미	팀장	개방형참여자
	한국인터넷진흥원	정현철	연구위원	발제자
개방형 참여자	시흥산업진흥원	김정아	주임	온라인
	㈜스페이스에이디	최돈출	대표	온라인
	HTC 코리아	백승배	대표	온라인
정부	과기정통부	박선경	사무관	
간사	MDIA	김민관	팀장	
	MDIA	이혜민	과장	
	MDIA	박지수	대리	