국외출장 결과보고서

1. 출장개요

출장목적	고도화되는 사이버위협 및 AI를 활용한 공격의 증가로 글로벌 IT 기업의 방문을 통해 사이버 위협에 대한 대응 능력 제고			
출장기간	'26. 10. 20.(화) ~ 26. 10. 23.(금) / 3박 4일			
출장국가	일본(도쿄, 치바)			
출장자	소속	직급	성명	비고
	사이버보안부	3급	김OO	보안관제
	재정정보보호부	4급	조OO	개인정보
	사이버보안부	5급	박OO	취약점점검
	사이버보안부	5급	서OO	정보화

2. 출장일정

날짜	출발지	도착지	방문기관	업무수행내용	접촉예정인물 (직책포함)
10.20.(화)	서울	도쿄	-	일본/나리타 공항	현지 가이드
	도쿄	도쿄 (도쿄역)	한·일 기업 Business Day	IPA(일본 공공기관) - 일본 사이버보안 정책 세미나 참석	KISA 이OO 책임
10.21.(수)	도쿄	도쿄 (롯폰기)	CISCO Network 일본	일본 사이버보안 시장 동향 AI기반 보안 탐지모델 학습 Experience Center 견학	CISCO 선OO 프로 시OO 영업리더
10.22.(목)	도쿄	도쿄 (시부야)	Trellix 일본	EDR 전략, SCO 등 생성형 AI 보안 플랫폼 적용 사례 학습	Trellix 나OO 영업총괄 사OOO 매니저
	도쿄	치바	-	시부야→전시회장	-
	치바	치바 (마쿠하리 멧세)	2026 JAPAN IT WEEK Autumn	정보보호 Sector 견학 (전시회장, 세미나)	현지 가이드
	치바	도쿄	-	전시회장→숙소	-
10.23.(금)	도쿄	치바	-	숙소→전시회장	-
	치바	치바	2026 JAPAN IT WEEK Autumn	AI Sector 견학 (전시회장, 세미나)	현지 가이드
	치바	도쿄	-	전시회장→공항	-
	도쿄	서울	-	인천 국제공항	-

3. 업무수행내용

□ 최신 사이버보안 동향 파악

○ **AX*** **가속화** 및 '설계 내재화(Secure by Design)' 패러다임 정착

* AX(AI Transformation): 기존 업무 디지털화를 넘어 AI를 실무에 이식

○ **생성형 AI를 악용한 공격** 급증에 따른 **기존 방어 체계의 한계**

○ **섀도우 AI**** **확산**에 따른 사내 중요 정보 유출 위협 증대

** Shadow AI: 조직에서 인가되지 않은 AI를 업무에 활용하는 행위

□ 일본 동향 및 운영 사례

○ 국가사이버보안센터(NISC)의 국가사이버통괄실(NCO) 격상 및 DX/AX를 위해 디지털청(Digital Agency)을 신설하여 **중앙 통제**

○ 국가 규정에 따라, **온-프레미스/클라우드 영역***의 **이원화** 운영

* 온-프레미스: 국방성, 경찰, 정보기관 등 국가안보 부문에서 폐쇄망 고수
클라우드 영역: 교육, 공공, 금융 등 주요 산업망의 클라우드 전환 진행

○ 인터넷망뿐 아니라 **폐쇄망**에서도 데이터 흐름을 탐지하기 위해 국가 규정에 따라 **보안솔루션 적용을 의무화**하는 추세

□ 기업 및 세미나 방문을 통한 신기술 운영 사례 습득

○ (Business Day) KISA에서 주관하는 행사에서 IPA(일본 정보보호 기관)가 제공하는 일본 보안 정책 동향에 대한 정보보안 세미나 참석

○ **(시스코 네트워크)** 일본 사이버보안 동향 설명 및 네트워크, 제로트러스트 및 섀도우 AI 대응 등의 전체적인 보안대책 교육

○ **(트렐릭스)** AI, 클라우드 전환 과정에서 고도화된 위협 대응 EDR, NDR 및 AI를 활용한 SOC 방안에 대한 교육

○ **(Japan IT Week)** AI·DX 가속화에 따른 정보보안 이슈 및 솔루션 학습

4. 시사점 및 향후계획

□ AI의 활성·가속화는 피할 수 없는 세계적인 추세

○ 저출산으로 인한 고령화로 인한 기술 역량을 가진 엔지니어의 감소와 역량 강화를 위한 비용은 지속적으로 증가하고 있음

○ 글로벌 IT기업(Cisco, Trellix)를 방문 결과, AI 기반 자동화 공격으로 급증하는 대규모 보안 이벤트에 대해 기존 관제 인력 중심의 대응은 피로도 누적 및 초동 대응 한계가 주요 위험 요인으로 공통 지적됨

○ ARTEX 및 중국의 AI 해킹도구에 의한 공격이 증가하는 만큼 AI 공격은 같은 AI로 대응해야 한다는 것이 전문가 대다수의 의견

□ 무조건적 차단에서 안전한 가드레일 및 설계 내재화로의 전환 전략

○ 보안이 담보되지 않은 AX 전환은 사상누각이나, 현재 클라우드 및 생성형 AI 활용을 물리적으로 차단하는 것은 불가함

○ 기존 시그니처 기반 보안 체계는 점차 한계를 보이고 있으며, AI 기반의 실시간 탐지·분석·대응 체계 전환이 필요

□ 망분리 환경 맹신 탈피 및 내부 제로트러스트 가시성 확보 필요

○ 엄격한 망분리 환경을 유지하더라도 AI를 악용해 정상 사용자로 위장한 우회 침투, 내부자 위협, 이동형 매체 등을 통한 폐쇄망 타깃 공격이 고도화되고 있음.

○ 기존의 경계 중심 장비(방화벽, IPS)와 시그니처 백신만으로는 방어에 명확한 한계가 존재하므로, 내부망 및 원격 접점 전반에 식별자(Identity) 기반 지속 검증(Zero Trust)과 단말·네트워크 통합 가시성 확보가 필수적임

□ 현행 보안 환경 진단 및 차세대 방어 체계 도입에 대한 고민 필요

○ 망분리 환경을 유지하더라도 AI를 악용해 정상 사용자로 오인하게 만들어 공격할 경우 기존 장비는 그대로 통과시킬 위험이 존재

○ 네트워크 전 구간 트래픽 및 이기종 보안장비(방화벽, IPS, SIEM)이벤트를 통합 상관분석하는 NDR* 구축 도입 고려 필요

* NDR(Network Detection and Response): 인공지능과 머신러닝을 활용하여 네트워크 트래픽을 실시간 분석하고 보안위협을 탐지·대응하는 보안장비

○ 외부 인터넷 연결 없이 내부망에서 독자 구동되는 고성능의 행위 기반의 정보보안 탐지체계 구축 필요

○ AI를 활용한 보안취약점 점검 자동화 체계 도입을 고려하여, 사전에 잠재된 보안취약점을 찾아내어 기관 보안성 강화 필요

□ 향후 추진 계획

추진단계	추진과제	기대효과
단기 (1~3개월)	▪ 파일 내 신종·변종 악성코드를 자체 분석할 수 있는 관제 체계 구축	▪ 기획재정부문 연계기관 관제 범위 내 탐지 파일의 악성 여부·동작 내용 등 가시성 확보
중장기 (2027년)	▪ 네트워크 전 구간을 분석하여 탐지·대응하는 NDR 장비 도입 ▪ AI를 활용한 보안취약점 점검 자동화 체계 구축	▪ 기획재정부문 연계기관 관제 대역 내 NDR 도입으로 관제 사각지대 해소 ▪ AI를 통해 보안취약점 점검 품질 균일화 및 점검 속도 향상