과학기술정보통신부 공고 제2024-0521호

2024년 AI 보안 제품 및 서비스 확산 지원사업 참가기업 모집 공모

AI 보안 시장규모가 확대됨에 따라 경쟁력 있는 AI 보안 제품·서비스가 개발되고 있으나 공공·민간시장에 레퍼런스를 쌓을 수 있는 실증기회 확보에 어려움을 겪고 있습니다. 이에 우수한 AI 보안 제품·서비스를 보유한 기업의 실증지원을 통해 실데이터 활용을 통한 제품·서비스 고도화 및 공공·민간 시장의 AI 기반 보안 신기술 활용도를 제고하기 위해 AI 보안 제품 및 서비스 확산 지원사업 참여기업을 모집 공고하오니 많은 참여를 바랍니다.

2024년 5월 13일
과학기술정보통신부장관
한국인터넷진흥원장

□ 사업 목적

○ 유망한 AI 보안 제품·서비스의 실증 지원을 통해 기술경쟁력을 확보하여 공공·민간 시장의 AI 보안 제품·서비스 확산 유도

□ 사업 개요

○ 사업명 : 2024년 AI 보안 제품 및 서비스 확산 지원사업

○ 사업기간 : 협약체결일 ~ 2024년 12월 20일(약 7개월)

○ 사업예산 : 총 4억원(총 2개 과제, 과제 당 최대 2억원 지원)

○ 신청분야 : ’24년 AI 보안 제품 및 서비스 확산 지원사업 수요기관/기업 모집공고를 통해 총 2개 지원분야 선정(’24.2~3월)

구분	수요기관/기업명	제안 사업명	지원규모	
			정부지원금	지원기업수
① 공공	병무청	· AI 기반 실시간 유해사이트 분석 및 검증 기술 실증	2억원	1개社
② 민간	쓰리에이로직스	· AI 기반 암호화 트래픽 내 위협패킷 탐지 및 분류 기술 실증	2억원	1개社

※ 1차 평가에서 분야 별 3배수 이내 선정 → 2차 평가에서 최종 1개 기업 선발

○ 지원방법 : 단독 또는 컨소시엄 형태로 참여하며, 2개 이상의 기업이 참여하는 경우에는 주관기관, 참여기관으로 구분

※ 컨소시엄 참여비율은 주관기업 60% 이상, 참여기업은 10% 이상으로 구성해야하며 최대 3개 기업까지 컨소시엄 구성 가능(주관 및 참여기관은 1개 과제에만 지원 가능)

□ 사업수행 세부내용

① AI 기반 실시간 유해사이트 분석 및 검증 기술 실증(병무청)

○ **(성능 고도화)** AI 기반 실시간 유해사이트 분석 및 탐지의 정확도 향상을 위한 내·외부 데이터 수집 및 AI 모델 학습

○ **(커스터마이징)** AI 기반 실시간 유해사이트 분석 및 탐지 기술을 수요기관 환경에 맞춤형으로 적용하기 위한 커스터마이징

※ 수요기관의 네트워크 구성, 운영 중인 보안솔루션 등을 고려하여 커스터마이징을 수행해야 함

[주요 필요기능]

구분	주요내용
유해사이트 분석·탐지	- 수요기관 내부 인터넷망을 대상으로 자동화된 웹사이트 분석을 통해 웹사이트 유해 여부를 실시간으로 분석하고 결과의 가시화 기능 제공 - 웹사이트에 유해성에 대한 판단 기준 수립 및 제시가 필요하며, 웹사이트의 JS(Java Scirpt), JSP(Java Server Page), 웹사이트 호출기능(문서편집, 파일전송 등) 등의 웹사이트 구성요소를 다양하게 고려해야 함 ※ 유해사이트 판별기준 및 오탐·미탐 수준의 적정성은 KISA, 수요기관과 협의하여 결정
모니터링	- AI 모델의 웹사이트 분석을 통한 유해사이트 적중유무를 실시간으로 모니터링 - 웹사이트의 위험도 분석·평가 결과를 기반으로 임계치를 설정하여 실시간 탐지·알림 기능 제공(요일, 시간별 임계치 자동 조정 프로세스 구현)
통계/분석	- 월별, 일별, 유해사이트 판별·적중 상황 별 발생 통계 데이터 제공

※ 주요 필요기능에 대한 세부사항은 추후 KISA, 수요기관과 협의를 통해 최종 확정 예정

○ **(실증·기능개선)** AI 기반 실시간 유해사이트 분석 및 탐지를 위해 실제 운영 중인 수요기관 환경에 해당 기능을 적용하고 피드백을 통한 기능 개선

※ 사업종료 후 실증 완료된 제품의 운영을 위한 계약 등은 수요기관과 별도로 추진

[유의사항]

구분	주요내용
기능 수준	- 학습기반으로 동작하여 오탐·미탐 분류를 통한 정확도 향상이 가능해야 함 - 유해사이트의 경우 웹사이트 구성요소를 유지한 채 URL, 도메인만 변경하는 케이스 등을 고려하여 유해성 판단기준 수립 및 탐지·분석 기능이 필요함
실증 환경	- 수요기관에서 운영 중인 보안관제환경(빅데이터분석시스템, 인공지능시스템 등)과 연동 및 커스터마이징 필요 - 수요기관 내부의 지정한 장소에 On-premise 형태로 실증을 진행해야 함 - 외부 인터넷망과 연결되지 않은 내부망 운영 방안 마련 필요 - 이기종 보안장비(악성코드차단시스템, 유해사이트차단시스템 등)와 호환 필요
보안	- 실증 시 정보보안관련 법령 및 내부규정, 외주 용역사업 보안관리 지침 등을 준수하여야 함 - 실증 관련 데이터는 원칙적으로 외부반출이 불가하며, 수요기관에서 제공한 장소를 활용해 기능 고도화·최적화 및 실증 추진

② AI 기반 암호화 트래픽 내 위협패킷 탐지 및 분류 기술 실증(쓰리에이로직스)

○ **(AI 모델 고도화)** AI 기반 암호화 트래픽 내 위협패킷 탐지 및 분류 정확도 향상을 위한 암호화 트래픽, 악성 데이터셋 등 유형별 데이터 수집 및 학습

○ **(커스터마이징)** AI 기반 암호화 트래픽 내 위협패킷 탐지 및 분류 기술을 수요기업 네트워크 환경에 맞춤형으로 적용하기 위한 커스터마이징

[주요 필요기능]

구분	주요내용
탐지·차단	- 최신 웹 보안 프로토콜(TLS v1.3 등)을 사용하여 전송되는 암호화 트래픽에 대해 복호화 없이 주요위협* 트래픽 신속탐지 및 차단 * 스피어피싱, ○WASP 상위 10대 위험 등 주요 사이버위협 공격
모니터링	- 탐지 분류된 악성 공격위협에 대한 모니터링을 위한 분류 정보 출력 (json 호환) ※ 악성 공격 위협을 탐지하는 기준과 출력되는 분류 정보에 대한 내용 제시 필요 ※ 악성 공격 위협 탐지 기준의 적정성은 수요기업, KISA와 협의하여 결정
통계/분석	- 월별, 일별, 악성 공격위협 상황 별 발생 통계 데이터 제공

※ 주요 필요기능에 대한 세부사항은 추후 KISA와 수요기업과 협의를 통해 최종 확정 예정

○ **(실증·기능개선)** 암호화된 트래픽 기반 공격 방지를 위해 실제 운영 중인 수요기업 환경에 해당 기능을 적용하고 피드백을 통한 기능 개선

※ 사업종료 후 실증 완료된 제품의 운영을 위한 계약 등은 수요기업과 별도로 추진

[유의사항]

구분	주요내용
기능 수준	- 학습기반으로 동작하여 오탐·미탐 분류를 통한 정확도 향상이 가능해야 함 ※ 적절한 오탐·미탐 수준에 대해서는 실증처·KISA와 협의하여 결정
실증 환경	- 수요기업에서 실 운영중인 네트워크 환경에 대해서 실제 트래픽 기반 암호화 위협을 탐지·차단 및 분류할 수 있는 테스트 계획 수립 실시 - 수요기업에서 운영 중인 UTM(Unified Threat Management) /방화벽 장비와 미러링 연계를 통해 외부 네트워크 트래픽 중 암호화 트래픽 위협에 대한 탐지·차단 및 분류 처리 ※ 실증 환경에 대한 구체적인 사항은 KISA, 수요기업과 협의하여 결정
보안	- 실증 시 각종 정보보안관련 법령 및 규정, 정보시스템 개발 가이드라인, 각종 표준지침 등을 준수하여야 함

□ 지원 대상

○ **(대상)** AI 기술을 활용한 실시간 유해사이트 분석·탐지 또는 암호화 트래픽 내 위협패킷 탐지·분류 기술을 보유하고, 이를 실증하고자 하는 기업

- 사업자 규모 제한 없음(중소, 중견 및 대기업 참여 가능)

※ 본 사업은 "중소기업제품 구매촉진 및 판로지원에 관한 법률 시행령" 제2조의 3(중소기업자와의 우선조달계약에 대한 예외) 제4호에 의거 AI 보안이라는 특정한 보안기술의 개발과 이를 적용하여 산업을 확산하기 위한 사업임

- 비영리기관이 본 지원사업에 공모 시 컨소시엄을 구성하여 참여기관으로 공모 가능(단독 공모 및 주관기관 불가)

- 제안 기업은 <u>기술성숙도 7단계 이상</u>인 기술만 지원 가능

※ 선정 평가 시 평가위원회를 통해 기술성숙도 단계를 판단하며, 7단계 미만인 것으로 확인 시 지원 대상에서 제외 가능

□ 지원 내용

○ **(예산지원)** 지원금 상한액(과제당 최대 2억원) 이내에서 제안 가능

- 제안기업은 현금 또는 현물(인건비, 기자재 등)을 통해 총 사업비의 25% 이상 부담(중견·대기업의 경우 각각 30%, 50% 이상 부담)

※ 지원금으로 사업비 편성 시 본 지원사업의 공고문, 별첨 서식, 과학기술정보통신부 고시 제2023-49호 '국가연구개발사업 연구개발비 사용기준' 등을 참고·준용하여 사업비 편성

○ **(실증 환경 지원)** 수요기관·기업의 인프라, 데이터 등 실증 환경 제공

○ **(기업 역량강화)** 실증할 제품·서비스의 고도화·최적화 및 기업 성장(사업화, 마케팅 등), 투자유치를 위한 전문가 컨설팅 제공

※ 제안기업의 기업진단, 제품·서비스 기술 분석, 요구사항 등을 전반적으로 고려하여 적합한 전문가를 매칭할 예정이며, 기업 당 최소 3회 이상 지원 예정(변동 가능)

○ **(확산 지원)** 실증 완료된 제품·서비스의 이용 확산을 위해 인증 취득, 판로개척 및 제품·서비스 홍보 지원

- **(인증 지원)** 제안기업의 제품·서비스에 대한 성능 평가와 우수성을 인증하기 위해 관련된 인증 취득 지원

※ 제안기업은 우수 정보보호 기술 지정, 신기술 및 융·복합 정보보호제품 신속확인제 조건·대상에 부합하는 경우 인증절차 신청을 권고함

- **(판로개척)** 대기업·공공기관 등과 참여기업 간 구매상담 및 협력의 장 마련을 위한 구매상담회 및 네트워킹 데이 개최

- **(홍보 지원)** 제안기업 우수 사례의 적극 홍보를 위한 성과 공유회, 데모데이 개최 및 홍보 리플렛 제작 등 대내외 제품·서비스 홍보 지원

□ 지원 조건

○ <u>정부지원금 상한액(최대 2억원) 이내에서 제안</u> 가능

- 각 기업 규모에 따라, 총 사업비는 정부 지원금, 민간 부담금 매칭 펀드 비율에 따라 산정 필요

※ 과학기술정보통신부 고시 제2023-29호「정보통신·방송 연구개발 관리규정」상의 '[별표 4] '정부지원연구개발비 지원기준 및 기관부담연구개발비 기준'에 따라, 총 사업비 대비 민간부담금 최소 비율 이상을 현금·현물로 부담

※ 각 기업 규모별로 민간부담금 중 현금 부담 비율은 대기업 15%, 중견기업 13%, 중소기업 10% 이상 현금 부담

- 선정된 기관의 제안금액을 대상으로 원가산정 등을 통해 적정규모를 평가 후 최종 지원금을 확정

※ 부가세는 지원금에 포함되지 않으며, 참여 기관에서 부담

○ KISA, 정부 및 타 기관으로부터 지원금을 받아 동일 또는 유사한 사업의 형태로 수행하는 경우 지원 신청할 수 없음

※ 선정 평가 시 평가위원회를 통해 중복여부를 판단하며, 중복 확인 시 지원 대상에서 제외 가능

○ 정부지원금은 사업 착수 시 70%를 지급하고, 중간평가 후 30%를 지급

□ 신청서 접수

○ 접수기간 : 2024. 5. 13.(월) ~ 2024. 5. 31(금) 14:00까지

○ 접수마감일 : 2024. 5. 31(금), 14:00까지 (※ 제출기한(14:00) 이후 접수 불가)

※ 접수 마감시간 임박 시 원활하게 전자계약시스템에 접속되지 않을 수 있으니, 최소 마감시간 2시간 전에 신청 완료할 것을 권장함

○ 신청서 및 제출자료 작성 : 소정 양식(공모안내서 붙임자료 및 첨부파일 참조)

○ 접수방법 : KISA 전자계약시스템을 통한 온라인 접수

- 온라인 접수 경로 : https://cont.kisa.or.kr - 위탁과제/지원 – 공고현황

○ 문의처 : 박경호 주임(061-820-1357)

과학기술정보통신부 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

****

본 입찰은 KISA전자계약시스템을 이용한 전자입찰 대상으로 전자입찰서는 반드시 KISA 전자계약시스템(https://cont.kisa.or.kr)에 접속하여 인터넷으로 제출하여야 하며, 전자계약을 실시합니다.

접수마감 기한 경과 시 전자계약시스템이 자동마감 되며, 마감시간에 임박하여 접수할 경우 시스템 사용 미숙에 따른 오류, **입찰등록 집중으로 인한 시스템 장애 등이 발생할 수 있으니 가급적 1~2일 전부터 여유를 갖고 접수하시기 바랍니다.**

****