

# 「IoT제품 보안 취약점 분석서비스」 사업 지원기업 모집 공고문

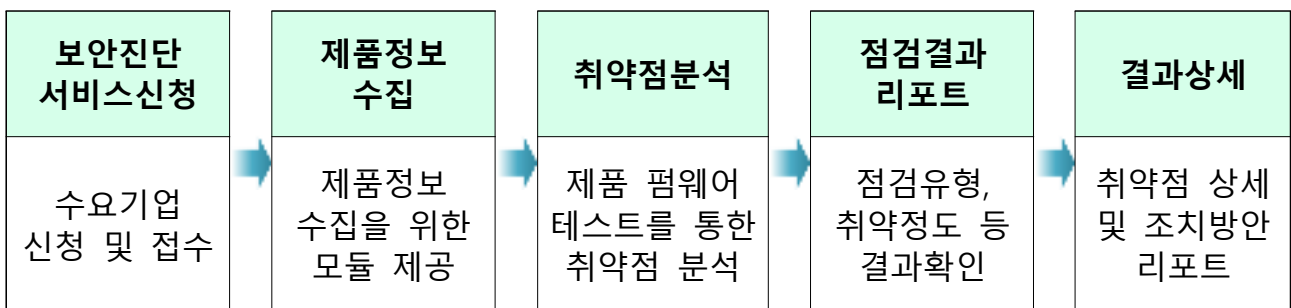
국내 가전기업의 보안 수준 향상을 위하여 IoT제품 보안 취약점 진단  
모집 공고를 다음과 같이 게재하오니 참여를 원하시는 기업의 많은 관  
심과 참여 부탁드립니다.

2025년 7월 30일

한국전자정보통신산업진흥회장

## □ 개요

- 목적 : 물리적, 기술적 해킹 방지를 위해 IoT제품의 보안 위협 시스템  
취약점을 진단하고 대응책을 마련함으로써 기업의 보안수준 향상
- 기간 : 2025. 8. ~ 11월(4개월)
- 규모 : IoT제품을 보유한 국내 가전·전자 기업 3개사 선정  
※ 지원 규모 및 프로그램은 기업 수요에 따라 일부 변경될 수 있음
- 내용 : IoT제품 보안 취약점 분석 및 취약점 대응방안 제시



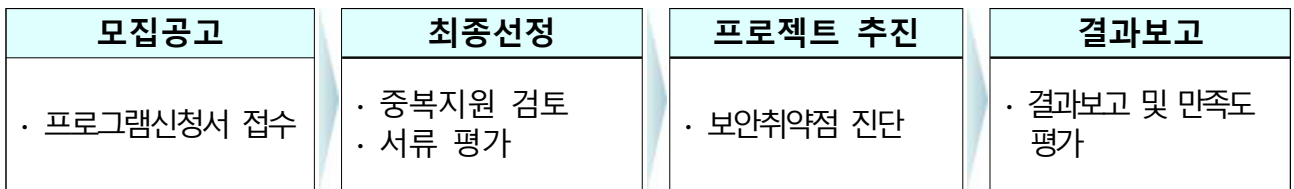
<IoT제품 보안점검 프로세스>

□ 사업신청

- (신청기간) 2025년 8월 5일(화) ~ 8월 19일(화) 18시까지
- (신청대상) ① IoT제품을 보유한 국내 가전·전자 기업  
② 지원 기간 내에 프로젝트 수행이 가능한 기업에 한함
- (제출서류) ① 신청서, ② 개인정보 수집 동의서, ③ 사업자등록증
- (신청방법) 이메일 접수([sjahn@gokea.org](mailto:sjahn@gokea.org))

□ 선정 및 지원절차

- 서류심사를 통해 최종기업 선정 및 프로젝트 추진



\* 프로그램 신청서 참조

□ 추진일정

모집공고	선정평가	기업선정	사업추진	사업종료
'25.8.5~8.19	'25.8.21~8.26	'25.8.27	'25.9.1~	'25.11.30
서류접수	서면평가	선정발표	취약점 진단	결과보고

□ 유의사항

- 동일 개발 내용으로 정부 지원(지자체 포함)을 받은 경우 제외
- 채무불이행, 국세·납세 체납된 자 또는 기업의 경우 신청 제외
- 제출된 서류 및 사업계획서가 허위, 위조·변조, 그 밖에 부정하게 작성되었을 경우 선정 취소 및 협약 해약 등 불이익 조치함
- 제출된 서류는 일체 반환하지 않음

□ 문의처 : 한국전자정보통신산업진흥회 디지털혁신실 안수진 대리

☎ 02-6388-6115, ✉ [sjahn@gokea.org](mailto:sjahn@gokea.org)

□ 총 4개 영역, 15개 분야, 30개 항목

구분	상세구분	진단항목	진단 코드	영향도
H/W 영역	가. 인터페이스 보호	외부 인터페이스 노출	V-01	중
		내부 인터페이스 노출	V-02	상
	나. 비휘발성 메모리 보호	비휘발성 메모리 추출 및 판독	V-03	상
F/W 영역	가. 취약한 패스워드	취약한 패스워드 사용	V-04	상
	나. 인증서 보안	인증서 만료 여부 확인	V-05	중
		취약한 알고리즘 사용	V-06	상
		개인키 관리 미흡	V-07	중
	다. 오픈소스 취약점	취약한 운영체제 사용	V-08	상
		취약한 소프트웨어 버전 사용	V-09	상
	라. 바이너리 취약점	바이너리 보안 설정 미흡	V-10	중
		취약한 함수 사용	V-11	상
	마. 보안 설정 점검	취약한 원격 포트 사용	V-12	상
		방화벽 구성 오류	V-13	상
		취약한 uPnP 설정	V-14	상
		SUID, SGID 설정	V-15	중
		Shadow 파일의 권한 설정	V-16	중
N/W 영역	가. 취약한 인증	인증 및 세션 처리 미흡	V-17	상
	나. 취약한 암호화 설정	전송 구간 암호화 설정 미흡	V-18	상
	다. 민감한 정보 노출	개인정보 / 중요 정보 노출	V-19	상
	라. 입력 값 검증	SQL Injection	V-20	상
		파일 업로드/ 다운로드	V-21	상
		XSS	V-22	중
	마. 보안 설정 미흡	부적절한 에러 처리	V-23	하
		불필요한 포트 오픈	V-24	중
패스워드 정책 적용 미흡		V-25	중	
App 영역	가. 취약한 인증 및 권한 설정	Activity 강제 실행을 통한 권한 우회	V-26	중
		불필요한 권한 설정	V-27	하
	나. 역공학 분석 방지	루팅 탐지 미흡	V-28	상
		난독화 미흡	V-29	중
	다. 민감한 정보 노출	민감한 정보 노출	V-30	중