

【NCS기반 직무기술서】

한국전자통신연구원		분 류 체 계	구분	연구원 자체 직무분석을 통해 도출
채용 분야	연구직 (일반연구)		대분류	국가 지능화
채용 예정 인원	1명		중분류	잠재적 사이버 위협을 원천 차단하는 지능형 사이버 보안 및 신뢰 인프라 기술 연구
			소분류	정교화·자동화 해킹을 원천 차단하는 지능형 정보보호 핵심 기술 개발
기관 소개		한국전자통신연구원은 정보, 통신, 전자, 방송 및 관련 융합기술 분야의 핵심·미래 기술을 연구개발하고, 성장동력 창출 및 성과확산을 통해 국가경제·사회 발전에 기여함		
전형 절차		서류전형 → 전공세미나(전공면접) → 종합면접(인성검사 포함) → 임용		
직무 수행 내용		○ (네트워크보안) 5G/6G 네트워크 취약점 분석 및 인공지능 기반 탐지·대응 기술 연구 ○ (클라우드보안) 클라우드 네이티브 환경 취약점 분석 및 사이버 공격 탐지·예방 기술 연구		
근무지		한국전자통신연구원 본원(대전광역시 유성구 가정로 218 한국전자통신연구원)		
일반 요건	연령, 성별	○ 연령: 무관 ○ 성별: 무관		
	논문, 특허	○ 아래의 연구실적 자격 중 하나에 해당하는 자(접수마감일 기준 최근 5년 이내) ① SCIE 논문 1건 이상 게재한 자(제1저자 또는 교신저자에 한함) ② 이에 준하는 국제학술대회 발표논문 실적 1건 이상 보유한 자(제1저자 또는 교신저자에 한함) ③ 국제특허 1건 이상 등록한 자		
	기타	○ 국가공무원법 제33조(결격사유)와 연구원 규정(인사규정 제10조)의 임용 결격사유가 없는 자로 해외여행에 결격사유가 없는 자 ○ 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」 제82조(비위면직자 등의 취업제한)에 해당하지 않는 자 ○ 병역의무 대상자(남성)는 군필자*, 면제자 또는 병역특례 대상자** * 군필자: 2025. 2. 28.까지 군 복무를 마칠 수 있는 자 ** 병역특례대상자: 병역법 및 동법 시행령에 따라 전문연구요원 전직 요건을 갖춘 자 지원 가능 ○ 국가연구개발사업 참여 제한이 없는 자 ○ 임용일부터 정상근무가 가능한 자		
교육 요건	학력	○ 석사 이상[2025년 2월 28일까지 국내·외 석사학위 취득(예정)자* 포함] * 학위증명서 수여일 기준 ※ 학위 취득예정자가 최종 합격 후 2025년 2월 28일까지 졸업증명서를 제출하지 못하는 경우 합격 취소		

	<p>관련 전공</p> <p>○ 정보보호, 컴퓨터공학, 통신공학 등 관련 전공</p>
<p>관련 경력</p>	<p>○ 국가연구개발 사업 참여 유경험자</p> <p>○ 네트워크(5G) 또는 클라우드 보안 관련 연구 유경험자</p> <p>○ 인공지능 기반 침해대응 관련 연구 유경험자</p>
<p>필요 지식</p>	<p>○ 컴퓨터통신, 정보보호, 인공지능 기술에 대한 종합지식</p> <p>○ 네트워크, 클라우드 및 AI 보안 기술에 대한 지식</p>
<p>필요 기술</p>	<p>○ (네트워크·클라우드보안) 유무선 네트워크 트래픽 분석기술, 클라우드 네이티브 기술, 리눅스 기반 시스템SW 기술</p> <p>○ (지능형 침해대응) 침해위험 분석·탐지를 위한 인공지능 관련 프레임워크 활용 기술</p>
<p>직무 수행 태도</p>	<p>○ 새로운 도전과 창의</p> <p>○ 선제적 변화 및 혁신 의지</p> <p>○ 연구협업을 위한 소통 및 협력</p>
<p>직업 기초 능력</p>	<p>○ 의사소통능력, 대인관계능력, 수리능력, 문제해결능력, 자기개발능력, 자원관리 능력, 조직이해능력, 정보능력, 기술능력, 직업윤리</p>
<p>기타</p>	<p>○ 본 채용공고는 「평등한 기회, 공정한 과정을 위한 공공기관 블라인드 채용 가이드라인」과 「과기정통부 소관 연구개발목적기관 채용 기준」을 준수합니다.</p> <p>- 모집분야별 전문성과 직무적합성을 확인·검증하기 위하여 관련 기준에 따라 연구 및 직무와 관련된 학위취득기관(학교명, 전공, 학위, 학점, 지도교수명 등) 및 연구수행기관(기관명, 직위, 직무수행내용 등) 경력에 대한 정보를 수집합니다.</p> <p>○ 상기 직무는 지원자가 입사 시 수행할 대표 전문 분야의 직무이며, 입사 후 해당 직무 외 관련된 타 직무도 수행할 수 있습니다.</p> <p>○ 참고사이트 : www.ncs.go.kr</p> <p>※ 위 내용은 NCS 미개발 직무로 한국전자통신연구원의 별도 직무분석을 통해 도출되었습니다. 향후 NCS 개발동향과 기관 주요사업 변경 등 내·외부 상황에 따라 변경될 수 있음을 양지하여 주시기 바랍니다.</p>

신규인력 요구사유(1개 이상 선택하여 기재)

[① R&R 추진계획 연계]

- R&R 핵심 역할(5-2-1. 정교화·자동화 해킹을 원천 차단하는 지능형 정보보호 핵심 기술 개발) 수행을 위한 신규인력 총원 필요

[② 중대형 전략중점 연구과제(ETRI연구개발지원사업 등) 연계]

- 국가전략기술인 “사이버보안”의 4대 중점기술(네트워크·클라우드 보안)에 대한 핵심 역량 확보를 위한 신규인력 필요

[③ 기타] 직전 미채용 인력 총원

신규인력 요구사유 상세

[① R&R 추진계획 연계]

- R&R 핵심 역할(5-2-1. 정교화·자동화 해킹을 원천 차단하는 지능형 정보보호 핵심 기술 개발)로서, 인공지능 기술 확산 등 고도화·지능화되는 사이버 공격으로부터 국가 핵심 인프라인 5G/6G 네트워크 및 클라우드를 보호하고 제로트러스트 기반 초신뢰 보안 실현을 위한 전문인력 확보 필요

[② 중대형 전략중점 연구과제(ETRI연구개발지원사업 등) 연계]

- “사이버보안”은 12대 국가전략기술이며, “네트워크·클라우드 보안”은 사이버보안의 4대 중점기술 중 하나로서 전략중점 기술 영역임
- 정부의 5G/6G 전략 뿐만 아니라, 5G 특화망(이음5G) 및 오픈랜(Open-RAN) 활성화 정책 등에 발맞추어 잠재적 보안취약점 해소, 외산 기술 대응 및 답보상태인 기술 격차 추격을 위한 핵심 기술역량 확보 필요
- 정부는 클라우드 네이티브 전환 계획을 내세우며, 26년까지 전환 대상 시스템의 70%를 클라우드 네이티브 전환하겠다는 목표 수립(23.4월, 디지털플랫폼정부위원회)한 바 있으며, 안전한 클라우드 네이티브 전환 및 활성화를 위한 핵심 보안기술 역량 확보 필요
- 지능정보 사회의 초연결과 클라우드 확산 등 공격 접점(attack surface) 확대와 AI 기술의 보편화로 인해 고도화되는 사이버 범죄 및 테러로부터 국가 핵심 인프라를 보호하기 위한 인공지능 기반 지능형 침해대응 기술 역량 확보 필요

[③ 기타]

- 직전 미채용 신규인력 총원 필요