보안 과제( ), 일반 과제(O) / 공개(O), 비공개( )
2023년 과학기술혁신정책지원사업 최종보고서

발간등록번호
11-B550936-000663-10

혁신정책 / 2023-011

국가R&D 보안정책 설계를 위한 기초연구

(Foundational Research for Developing Research Security Policies for National R&D Programs)

2024. 2.

한국과학기술기획평가원

과학기술정보통신부

제 출 문

과학기술정보통신부 장관 귀하

'국가R&D 보안정책 설계를 위한 기초연구'(2023. 11. 13. - 2024. 2. 10) 과제의 최종보고서를 제출합니다.

2024. 4. 1.

주관연구개발기관명 : 한국과학기술기획평가원 (대표자) :정병선

주 관 연 구 책 임 자 : 정 정 규

국가연구개발혁신법 시행령 제35조에 따라 최종보고서 열람에 동의합니다.

최종보고서

보안등급
일반[V], 보안[ ]

중앙행정기관명	과학기술정보통신부	사업명	사업명	2023년 과학기술혁신정책 지원사업	
전문기관명 (해당 시 작성)	한국과학기술기획평가원		내역사업명 (해당 시 작성)		
공고번호		총괄연구개발 식별번호 (해당 시 작성)			
		연구개발과제번호			

기술분류	국가과학기술 표준분류	HG1326. 과학기술	90%	HG1399	10%	3순위 소분류 코드명		%
	부처기술분류 (해당 시 작성)	1순위 소분류 코드명	%	2순위 소분류 코드명	%	3순위 소분류 코드명		%

총괄연구개발명 (해당 시 작성)	국문	2023년 과학기술혁신정책지원사업
	영문	2023 Science and Technology Innovation Policy Support Project
연구개발과제명	국문	국가R&D 보안정책 설계를 위한 기초연구
	영문	Foundational Research for Developing Research Security Policies for National R&D Programs

주관연구개발기관	기관명	한국과학기술기획평가원	사업자등록번호	229-82-01678
	주소	충북 음성군 맹동면 원중로 1339	법인등록번호	110271-0004210

연구책임자	성명	정정규	직위	연구위원
	연락처 직장전화	043-750-2438	휴대전화	010-2288-2338
	연락처 전자우편	j2key@kistep.re.kr	국가연구자번호	11412896

연구개발기간	2023. 11. 13. - 2024. 2. 10. (3 개월)

연구개발비 (단위: 천원)	정부지원 연구개발비	기관부담 연구개발비		그 외 기관 등의 지원금				합계			연구개발비 외 지원금
				지방자치단체		기타( )					
	현금	현금	현물	현금	현물	현금	현물	현금	현물	합계	
	127,000							127,000		127,000	

공동연구개발기관 등 (해당 시 작성)	기관명	책임자	직위	휴대전화	전자우편	비고	
						역할	기관유형
공동연구개발기관							
위탁연구개발기관							
연구개발기관 외 기관							

연구개발담당자 실무담당자	성명	황인영	직위	부연구위원
	연락처 직장전화	043-750-2637	휴대전화	010-3249-3412
	연락처 전자우편	iyhwang@kistep.re.kr	국가연구자번호	11439487

이 최종보고서에 기재된 내용이 사실임을 확인하며, 만약 사실이 아닌 경우 관련 법령 및 규정에 따라 제재 처분 등의 불이익도 감수하겠습니다.

2024년 4월 1일

연구책임자: 정 정 규 (서명)

주관연구개발기관의 장: 한국과학기술기획평가원장 (직인)

중앙행정기관의 장 귀하

< 요 약 서 >

<table>
<tr><td colspan="2">사업명</td><td colspan="3">2023년 과학기술혁신정책지원사업</td><td colspan="2">총괄연구개발 식별번호
(해당 시 작성)</td><td></td></tr>
<tr><td colspan="2">내역사업명
(해당 시 작성)</td><td colspan="3"></td><td colspan="2">연구개발과제번호</td><td></td></tr>
<tr><td rowspan="2">기술분류</td><td>국가과학기술
표준분류</td><td>HG1326. 과학기술</td><td>90%</td><td>HG1399</td><td>10%</td><td>3순위 소분류 코드명</td><td>%</td></tr>
<tr><td>부처기술분류
(해당 시 작성)</td><td>1순위 소분류 코드명</td><td>%</td><td>2순위 소분류 코드명</td><td>%</td><td>3순위 소분류 코드명</td><td>%</td></tr>
<tr><td colspan="2">총괄연구개발명
(해당 시 작성)</td><td colspan="6">2023년도 과학기술혁신정책지원사업</td></tr>
<tr><td colspan="2">연구개발과제명</td><td colspan="6">국가R&D 보안정책 설계를 위한 기초연구</td></tr>
<tr><td colspan="2">전체 연구개발기간</td><td colspan="6">2023. 11. 13. - 2024. 2. 10. (3개월)</td></tr>
<tr><td colspan="2">총 연구개발비</td><td colspan="6">총 127,000 천원
(정부지원연구개발비: 127,000 천원, 기관부담연구개발비 : 천원,
지방자치단체지원연구개발비: 천원, 그 외 지원연구개발비: 천원)</td></tr>
<tr><td colspan="2">연구개발단계</td><td colspan="6">기초[ ] 응용[ ] 개발[ ] 기타(위 3가지에 해당되지 않는 경우)[v]</td></tr>
<tr><td rowspan="2">연구개발
목표 및 내용</td><td>최종 목표</td><td colspan="6">○ 기술패권 경쟁 격화 및 국제공동연구 활성화 등 국내·외 R&D환경 변화를 반영한 국가R&D 보안정책 설계 근거 마련
- 국내·외 연구·산업 보안 집행조직에 대한 벤치마킹
- 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출
- 보안등급 운영지침 설계를 위한 부처(전문기관)·전문가 대상 보안등급 분류·운영 의견수렴 및 분류체계 기반 분류 자동화 가능성 탐색</td></tr>
<tr><td>전체 내용</td><td colspan="6">1 연구보안 전담조직 설립방향 수립을 위한 사전조사
○ 국외 연구보안 조직 사례 및 국내 산업보안 전담조직 운영현황 조사
- 주요국의 해외 연구보안 전담조직 수립·운영 현황과 국내 산업보안 전담조직의 기구적 특성·역할 등을 벤치마킹하여 연구보안 관점의 시사점을 도출
○ 정책수요자 및 전문가 의견을 종합한 조직 설립 방향 도출
- 조직의 미션, 기능·역할 및 설립형태 등
· 조직 위상 및 정체성, 조직 운영 핵심가치 및 원칙 등
- 조직 설립근거 마련 등을 위한 관련법 법률전문가 자문 등
· 예산·인력 확보를 위해 관련된 법제적 사안 등 포함

2 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출
○ 연구자와 연구기관을 대상으로 제도개선에 부합하는 연구보안 조치 이행을 돕는 현장지침 설계 근거를 수집하고 시사점을 도출
- 개선되는 연구보안 제도를 연구자와 연구기관이 이행하는 데에 참고가 될 수 있는 현장지침의 항목을 조사
- 현장연구자 중심의 연구보안 인식조사 등 설문조사를 통해 지침 설계 시 근거기반 확충 및 시사점 도출
- 연구기관·전문기관 담당자, 정부 등 다양한 이해관계자의 연구보안 인식을 수집하여 시사점 도출
- 연구보안 시범운영 정책설계지원을 통한 현장지침 근거기반 확충

3 보안등급 분류체계 설계를 위한 탐색적 연구
○ 제도개선사항에 부합하는 보안등급 분류체계 마련을 위한 현장 의견을 수집, 시사점을 도출하고 분류 자동화 가능성을 탐색
- 중간 보안등급으로 '민감과제'(가제) 신설
- 분류기준으로 국가전략기술 관련 과제·주요 출연연 과제 등 추가
- 전문가 자문을 통해 등급분류 고려사항에 대한 의견수렴</td></tr>
</table>

		· 부처, 전문기관, 과제기획위·평가단 참여 민간위원 위주로 필요시 위원회 구성·운영 – 국가전략기술 등 기술분야에 대한 보안과제 및 민감과제의 분류체계 기반 분류 자동화 가능성 탐색

연구개발성과	ㅇ 연구보안 체계 내실화 토론회 개최('23.11.14) ※ 연합뉴스 등 언론보도 8건 ㅇ 국외수혜정보보고 교육 지원 ※ '23.12.13(오프라인) 및 '23.12.20(온라인) ㅇ「연구보안 체계 내실화 방안」 주요 추진사항으로 명시한 보안등급별 현장지침, 등급분류 가이드라인 기초자료 확보
연구개발성과 활용계획 및 기대 효과	ㅇ 연구보안 집행 전담조직 설립을 위한「국가연구개발혁신법」및「국가연구개발사업 보안대책」등 관계법규 개정의 근거기반 확충 및 설립의 예산·자원 확보 위한 제도적 근거 마련 ㅇ 연구보안 현장지침 및 보안등급 분류지침의 설계 기초자료를 마련하여, 연구자·연구기관 및 전문기관의 보안사고 예방 등 연구보안 제고에 기여
연구개발성과의 비공개여부 및 사유	

연구개발성과의 등록·기탁 건수	논문	특허	보고서 원문	연구시설·장비	기술요약정보	소프트웨어	표준	생명자원		화합물	신품종	
								생명정보	생물자원		정보	실물

세부 정량적 연구개발성과 건수	과학적 성과			사회적 성과								기타
	논문 게재	학술회의 발표	보고서 원문	법령 반영	정책 활용	안건 상정	제도 개선	다른 연구에 활용	국제 협력	(정책) 홍보	포상·수상	

국문핵심어 (5개 이내)	연구보안	국제공동연구	기술패권	국가안보
영문핵심어 (5개 이내)	Research Security	International R&D Collaboration	Technology Competition	National Security

※ 연구과제의 목표, 내용, 성과 및 활용계획 등을 5장 이내로 작성합니다.

연구의 목적 및 내용	**1. 연구보안 전담조직 설립방향 수립을 위한 사전조사** **1 연구목적** □ 글로벌 기술패권 경쟁 격화로 연구보안의 국내 정책 대응 및 국제공조 필요성이 제기되고 있으나, 우리나라의 경우 전담조직 및 지원기능 부재로 정책집행 역량에 한계 □ 국내외 벤치마크를 통한 우리나라 연구보안 전담조직 설립방향 수립 시사점 도출 ○ 정책수요자 및 전문가 의견을 종합한 조직 설립 방향 도출 - 기관 정관, 기능·역할, 조직형태 - 예산·인력확보를 위한 관계법령 근거마련 필요성 등 **2 연구내용** □ 해외 주요국 연구보안 전담조직 사례 분석 ○ (미국) NSF에 연구안보전략정책실(OCRSSP) 신설('20.3.)하고 연구보안 정책 전담 - 연구안보 및 정보분석(RSI-ISAO) 집행전담조직 기획 중(연 1천만 달러 예산) ○ (일본) 내각관방 국가안전보장국(NSS) 경제반('20.4) 및 내각부 경제안전보장추진실('22.8) 수립 ○ (영국) 과학혁신기술부 산하에 연구협력자문팀(RCAT)을 신설('22.3)하고 국제협력 컨설팅 제공 ○ (호주) 교육부 산하 대학해외간섭TF(UFIT)을 신설('19.8), 대학向 연구보안 가이드라인 등 제공 □ 국내 산업보안 전담조직 유사 사례 분석 ○ (산업기술보호협회) 산업기술보호법 기반의 사단법인(약 30인)으로 정책개발, 해외유출 사례전파, 실태조사 및 교육홍보, 산업기술보호법 근거 산업부·국정원 지원업무 수행 ○ (영업비밀보호센터) 특허청 소관 한국지식재산보호원 하위부서(약 13인)로 컨설팅 위주 ○ (대·중소기업·농어업협력재단) 중소기업기술보호법 기반의 특수법인(약 13인)으로 기술보호지원부가 중소기업 중심의 기술보호 업무 수행 □ 연구보안 전담조직 설립방향 수립을 위한 주요 고려사항 ○ (설립목적에 '연구보안 지원' 명시 필요) NSF OCRSSP, 한국산업기술보호협회 등 사례를 바탕으로 연구보안 관리보다는 연구자산 유출에 따른 국가적 피해를 사전에 예방하겠다는 연구보안 지원을 명시하는 것이 적절 - (기능) 관리보다 지원 위주의 ①정책 ②교육 ③홍보 ④가이드라인 개발 등이 적절 ○ (조직형태) 유연성과 신속한 대응을 위해 국가조직(정부조직)을 제외한 민간조직 또는 공공조직 중에서, 단기간 설립을 추진하는 경우 기존 기관 내 부서가 적절 - (구조) 설립 초기와 중장기를 구분하여 초기에는 10인 전후 단일부서로 착수 ○ (근거법령) 법령 개정은 필수는 아니나 예산 안정성 확보에 따른 안정적 연구보안 집행 기능 수행을 위해 필요 시 관련 근거조항 마련이 바람직 **2. 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출** **1 연구목적** □ 연구보안 체계 내실화 방안을 연구현장에서 실천하기 위한 필드매뉴얼로, 국가R&D 연구자·연구기관 및 관계기관의 연구보안 인식 제고와 제도 안착을 촉진

□ 국내외 산업보안 및 연구보안 관련사례를 조사하고, 현장연구자와 연구기관을 대상으로 고려대상 항목을 도출하여 현장연구자 중심의 연구보안 인식조사 등 설문조사 및 시사점을 도출

○ 연구보안 시범운영 정책설계와 운영지원을 통해 현장지침 시사점에 반영

2 연구내용

□ 선행문헌(산업·연구보안) 분석을 통한 기존 지침의 구조적 한계 식별

○ (기존 문헌 한계) 법제도 준수, 5대 보안영역 등 보안관리에 매몰되거나 개념화 미비, 지침 사용자 범위 적절성 미흡 등으로 인해 효용성이 제한적

○ (시사점) 연구보안 이행 사항을 R&D전주기와 결합하여 연구보안 지침 접근성을 제고하고 정책 현장착근 및 연구현장 적용 실질성, 연구자 가독성 등을 고려할 필요성 확인

- 개념과 범위 구체화*, 구체성 및 가독성 제고 필요

  * 연구보안·연구윤리·산업보안 구분, 보안주체(기관유형)별 보안조치 등 차별화

□ 다양한 연구현장 이해관계자를 대상으로 한 정책피드백·선행 지침 의견·보안사고 사례를 취합하여 지침구성 시사점 도출

○ (연구자) 연구보안 정책 본격화에 공감하나 연구자가 위축되지 않도록 연구계를 설득해 가며 장기적·순차적 도입 필요

- (공통) 치명적인 자산 유출은 인력이동이며 연구보안 관리 주체는 결국 일선 연구자이기에 관련자의 연구진실성 교육 필요
- (대학) 학제 별 개방성 수준이 달라 일괄 적용하기보다 학자들의 합의가 이뤄지는 분야 위주 관리 필요
- (출연연) 보안정책 도입과 운영 경험이 상대적으로 많아 제도 거부장벽 자체는 낮은 편이나, 분야별 국제공동연구 특성 등을 고려할 필요
- (기업) 민감·보안과제 성과공개 지연 시 '미래가치 실현'을 포함한 보상 검토 등이 결부되어 기업 연구개발활동의 위축을 초래하지 않도록 고려 필요

○ (전문기관) 관리과제 수가 많아 전문위원 수준에서 개별적으로 과제 관련 보안 위반 사항을 파악하기 어려운 실정을 감안한 시스템적 접근 통한 관리 필요

□ 현장 연구자 중심의 연구보안 인식조사

○ (개요) 국가연구개발사업 세부과제 연구책임자 경험이 있는 연구자 410인을 대상으로 설문 수행(2024.1.4.~1.15)

○ (분석1) IPA(Importance-Performance Analysis) 등 분석방법론 활용한 결과 '연구현장 인식제고, 보안과제 연구자보상, 분류절차 명확화 등에 대한 정책집행 우선순위가 높음

○ (분석2) 컨조인트 분석결과 연구자는 성과활용 제약에 강하게 반발하는 것으로 나타남

□ 이해관계자 의견을 종합한 연구보안 현장지침 작성방향 제시

○ (개념·관점 정립) 보호의 근간이 되는 연구자산 정의·보호범위를 명확화하며 연구보안의 개념을 구체적으로 안내

○ (전주기 관점 도입) R&D 전주기 관점의 보안영역 및 과제등급 별 차별화를 통한 활용도 제고

○ (기관유형 및 보안등급 차별화) 연구개발기관 유형(산학연), 보안등급(보안/민감/일반)별 현장지침 수립 및 자가진단도구 제시를 통해 활용도 향상

	□ 연구보안 시범운영 사전협의 실무지원을 통한 연구현장 환류 체계 기초 확보 ○ (실무협의) 후보기관의 참여의사 확인(23.11.27, 과기정통부) 및 후보기관 유형 특정을 통한 현장지침 우선적용 가능성에 따른 환류체계 구축 **3. 보안등급 분류체계 설계를 위한 탐색적 연구** **1 연구목적** □ 연구관리 전문기관이 제도의 취지를 충족하면서 국가R&D과제 보안등급을 효율적이고 탄력적으로 분류할 수 있는 가이드 제시 ○ 「연구보안 체계 내실화 방안」및「세계를 선도하는 글로벌 R&D 추진 전략」세부 추진방안 이행 및 연구현장 착근을 위한 보안등급 세분화 가이드 수요 제기 **2 연구내용** □ 등급분류 가이드라인의 역할과 책임의 범위 제시 ○ 등급분류 가이드라인은 보안등급 판단의 참고자료(reference)로, 과제별 보안등급은 전문기관이 최종 판정 □ 과제 생애주기별 보안등급 분류절차 해설 제공 ○ (기획-선정평가 단계 이전) 기관유형별 체크리스트를 수립하여 기획연구진과 연구개발과제평가단이 해당 과제 기획 시 또는 자유공모과제의 선정평가 결과를 토대로 보안등급을 지정할 수 있는 체계 제시 ○ (협약 이후) 국가안보 → 국민경제 순으로 2단계 검토를 실시하는 방안을 제시 - (1단계) 특정 부처 또는 특정 출연연의 무기체계개발 직접활용여부에 따라 국가안보를 판정 - (2단계) 검토 대상 국가연구개발과제의 서지정보*와 선정평가 결과**를 활용하여 기술성과 경제성을 판단하는 원칙을 제시하되, 필요시 (외부)기술전문가 및 경제성 전문가를 활용하여 기술성과 경제성을 판단 가능 * 과제규모(정부연구비, 참여연구원) 상위 5% 여부, 기관유형별 가점, 공동연구 여부 등 ** 국가전략기술/국가핵심기술 해당여부 또는 선정평가 시 평가점수의 부분점수 등
연구개발성과	○ 연구보안 체계 내실화 토론회 개최('23.11.14) ※ 연합뉴스 등 언론보도 8건 ○ 국외수혜정보보고 교육 지원 ※ '23.12.13(오프라인) 및 '23.12.20(온라인) ○ 「연구보안 체계 내실화 방안」 주요 추진사항으로 명시한 보안등급별 현장지침, 등급분류 가이드라인 기초자료 확보
연구개발 성과의 활용계획 (기대효과)	○「연구보안 체계 내실화 방안」 후속조치로써 현장지침 수립 및 등급분류 가이드 제정의 기초자료로 활용 가능 - 업무영역 및 조직규모 사례는 관련 예산요구 및 소요자원 확보 시 근거자료로 활용 가능 ○「국가연구개발혁신법」,「국가연구개발사업 보안대책」 관계법령 등 제도개선 시 기초자료 또는 참고자료로 활용 가능 ○ 연구자·연구기관 및 전문기관의 보안사고 예방 등 연구보안 이행력 제고를 통해 실질적 연구자산보호 강화

핵심어 (5개 이내)	연구보안	국제공동연구	기술패권	국가안보	

목 차

표 목 차

그 림 목 차

제1장 서론

제1절 연구의 배경 및 필요성

❑ 국내·외 R&D환경 변화 : 기술패권 경쟁 격화 및 국제공동연구 활성화

○ (국제환경) 기술패권이 주요국 간 국제 정세에서 우선 사안으로 부상하면서 국외 기술유출 리스크에 대한 국가적 차원의 관리 방안 및 체계 정비 수요

- 무역전쟁을 기폭제로 미·중 갈등이 급속하게 고조되면서(Fajgelbaum et al., 2022) 양국의 과학기술 경쟁은 세계 최강대국 간의 전략적 격전지로 부상(과학기술정보통신부·한국과학기술기획평가원, 2023; Schmid and Edenfield, 2023).

○ (국내환경) 정부는 우리나라 과학기술의 근본적 역량향상을 위한 국제공동연구 활성화 정책을 명확화하고 집중 지원 추진

- 정부는 「세계를 선도하는 글로벌 R&D 추진 전략」*을 수립하고 전략적 기술동맹을 위한 국제공동연구 강화 등 우리나라 과학기술의 글로벌 R&D 활성화를 위한 투자 혁신 및 연구 생태계 조성을 관계부처 합동으로 추진

* 국가과학기술자문회의 전원회의 의결(2023.11.27.)

❑ 국가 간 기술패권 경쟁과 국제공동연구 촉진으로 인한 우리나라 연구자산의 유출 리스크를 관리하기 위한 연구보안 체계 내실화 필요성 제기

○ (주요국의 연구보안 정책) 미·일 등 주요국은 개방형 협력 기조를 전제로 하되, 연구자의 연구진실성(research integrity) 및 이해상충(conflict of interest) 관리에 기반한 연구보안 대책을 제도화하는 접근으로 연구보안 정책을 추진 중

- (미국) 국가안보대통령교서(NSPM-33, 2021)의 7대 정책방향* 제시를 필두로, 반도체와 과학법 시행(2022) 및 연구안보정책실(OCRSSP)** 신설(2022) 등 기존의 연구보안 정책을 고도화하고 이를 운영 중

* ① 연구안보 인식 제고, ② 이해상충 관련 정보공개, ③ 정부 연구시설 등에 접근 제한, ④ 외국인 연구참여 관리, ⑤ 연구안보 관련 정보공유, ⑥ 위험관리, ⑦ 국제협력 촉진과 기술보호 간 균형

** Office of the Chief of Research Security Strategy and Policy (NSF 내 설립)

- (일본) 종합이노베이션전략추진회의(2021)에 따른 연구활동의 국제화, 개방화에 따른 위협에 대한 연구진실성 확보 정책방향을 수립하고, '경쟁적 연구비의 적정한 집행을 위한 관리지침 개정안'(2021) 및 문부성 e-Rad 시스템 개편(2022) 등 기존의 연구보안 정책을 고도화하고 이를 운영 중(白井俊行, 2022)

○ (우리나라의 연구보안 정책) 정부는 「신뢰받는 연구생태계 구축을 위한 연구보안 체계 내실화 방안」*을 수립하고 정책방향을 제시하였으며, 「세계를 선도하는 글로벌 R&D 추진 전략」**에서도 이를 재확인[1)]

* 국가과학기술자문회의 심의회의 본회의 의결(2023.9.26.)

** 국가과학기술자문회의 전원회의 의결(2023.11.27.)

- (법·제도 정비) 국가R&D 연구책임자의 국외로부터의 지원(예정)현황에 대해 부처에 보고하는 체계 마련*, 국가R&D 과제에 대한 체계적인 보안관리 및 제재사유 명확화**를 위해 보안대책(고시) 상향입법 등 추진, 기관 차원 연구보안 의무를 강화하고 원자력·우주 등 연구기관 대상 외국접촉의 부처 사전보고 의무 부과 검토 등

* 「국가연구개발혁신법 시행령」(2024.2.6.시행) 제9조제3항제8호 : "연구책임자가 연구개발기간 동안 외국의 정부 · 기관 · 단체 등으로부터 받는 행정적 · 재정적 지원이나 노무 또는 자문 등을 제공하고 받는 대가에 관한 사항"

** (현행) 보안대책 위반시 → (개선안) 보안대책을 위반하고 연구개발성과 및 정보 유출 시, 보안과제 수행자 외국접촉 등 보고·승인 의무를 고의·중과실로 불이행 시 등

- (보안과제 관리 내실화) 잠재적 중요기술의 선제보호를 위해 보안·일반과제의 중간 보안등급(민감)을 신설하되 보안과제보다는 낮은 관리의무를 부여*, 해외 특허출원 제한 및 특허 비공개 대상 확대** 등 추진

* 종래의 국방·국산화 외에 원자력·우주 등 주요 분야 출연연과제, 국가전략기술 등 추가 고려하는 등 보안등급 분류 가이드를 수립하고, 보안·민감과제 성과 중 보안사항 외 성과는 활용되도록 부분공개 제도 신설

** (현행) 국방 상 필요 → (개선안) 국가안보와 관련

- (연구보안 지원체계 구축) 과기정통부 연구보안 정책기능 강화, 연구보안 전담 지원체계* 기획, 특성화대학 지정 등 연구보안 전문가 육성, 외국인 참여 보고체계 강화 및 연구현장 가이드라인 및 연구보안 교육포털 구축 등 추진

* 부처(전문기관), 공공(연), 대학 본부 및 산단, 기업의 연구보안 담당자 및 KISA(정보보호), 해외 거점 등과 폭넓은 채널을 구축하고 협의회 운영

❑ 「신뢰받는 연구생태계 구축을 위한 연구보안 체계 내실화 방안」 추진 기초자료 확보 필요

○ (산업보안 대비 체계 확충 필요) 국내·외 산업보안은 체계가 확립된 반면 연구보안의 경우 주요국에서도 근거법령 및 정책방향이 수립된 수준이어서 연구보안 집행 전담조직 사례에 대한 지속적인 벤치마크 필요

1) 본 단락의 일부 내용은 「신뢰받는 연구생태계 구축을 위한 연구보안 체계 내실화 방안」(2023.9.)에서 발췌

○ (내실화 방안 이행 근거자료 수집 필요) 연구보안 체계 내실화 방안(안)」이행 정책 수립에 필요한 기초자료 수집 및 시사점 도출을 통해 향후 정책설계 근거자료 마련 및 방향설정을 위한 기초자료 확보 필요

- (전담 집행조직) 국내·외 산업보안 및 연구보안 집행 전담조직 사례를 벤치마크하고 우리나라 실정을 반영하기 위한 현장연구자, 연구보안 업무 실무자의 복합적인 의견 수렴 필요
- (현장지침) 우리나라의 연구특성을 감안한 연구현장용의 연구보안 현장지침 설계를 위한 근거 마련 필요
- (등급분류) 우리나라 국가연구개발사업 세부과제 관리 특성 및 국가전략기술 등 기술적 특성을 감안한 연구보안 등급분류 체계 설계를 위한 실증적 근거 마련 필요

제2절 연구목표 및 내용

❑ 연구목표

○ 기술패권 경쟁 격화 및 국제공동연구 활성화 등 국내·외 R&D환경 변화를 반영한 국가R&D 보안정책 설계 근거 마련

- 국내·외 연구·산업 보안 집행조직에 대한 벤치마킹
- 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출
- 보안등급 운영지침 설계를 위한 부처(전문기관)·전문가 대상 보안등급 분류·운영 의견수렴 및 분류체계 기반 분류 자동화 가능성 탐색

1 연구보안 집행 전담조직 설립방향 수립을 위한 사전조사

❑ 국외 연구보안 조직 사례 및 국내 산업보안 집행 전담조직 운영현황 조사

○ (해외 주요국 연구보안 전담조직 조사) 미국, 일본, 영국, 호주 등 해외 주요국의 연구보안 전담조직 설립 및 운영 사례 관련 조직 구성 및 주요 활동 등 조사

○ (국내 산업보안 전담조직 조사) 국내 산업보안 전담조직의 설립목적, 법적 근거, 지원대상, 지원내용, 주요활동 및 조직 구성 등 조사

❑ 집행 전담조직의 기구적 특성에 대한 연구보안 취급 실무자 및 전문가 의견 수집

○ (실무자·전문가의견 수집) 연구기관 및 전문기관 실무자를 중심으로 조직의 기능·역할 및 설립형태* 등 포괄적 의견** 수합

* (예시) 기존 기관의 하위조직 혹은 부설기관, 독립법인, 사업단 등 포함

** (예시) 주요 임무, 업무 및 관련 범위, 성격과 책임 및 이해관계자, 역할 분담, 구성원 및 인력 구조 등

○ (법률자문) 조직 설립 근거 법령에 관한 법률전문가 자문

- 조직의 목적과 성격을 고려하여 관련 법률 및 규정, 법인 유형, 조직의 구성 및 운영 규정 등 검토가 필요한 제반 사항에 대한 법률 전문가 자문 수행

❑ 국내·외 사례를 종합한 벤치마크 관점의 시사점 도출

○ (시사점 도출) 조사한 해외 주요국 및 국내 산업보안 기관별 특장점을 토대로 벤치마킹 포인트 탐색 및 국내 연구보안 조직 설립방향 설정 관련 시사점 도출

- 조직의 역할범위(do's and don'ts) 제안
- 국내 사례에서는 기구적 특성과 역할을, 해외 사례에서는 연구보안 측면의 역할과 수행 논리 시사점을 도출

2 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출

❑ 연구보안 현장지침 항목 도출에 참고 가능한 국내외 산업보안 및 연구보안 현장지침 사례 조사

○ (해외 사례 조사) 연구보안 부문을 중심으로 주요국 유사 가이드라인 사례 조사

○ (국내 사례 조사) 국내 산업보안 가이드라인 사례 조사

❑ 현장연구자와 연구기관을 대상으로 현장지침 고려대상 항목 도출

○ (연구자) 연구개발 실무 과정에서 현장연구자의 주의사항 식별

※ (예시) 학회 참석, 메일 등을 활용한 의사소통 등

○ (연구기관) 연구시설(연구기관) 관점의 관리대상 식별

※ (예시) 10대 유형별 연구성과물, 기술이전, 시설 보안(출입카드) 등

- 출연(연), 대학, 기업 등 기관유형 특성 감안

❑ 현장연구자 중심의 연구보안 인식조사 등 설문조사 및 시사점 도출

○ (연구보안 인식) 연구보안 현장맞춤 요소 발굴을 위한 연구주체별(기관, 연구자그룹) 인식조사

- 기관유형(산·학·연), 연구분야, 과제특성, 참여연구원의 인적 구성 등을 반영 가능한 요소 발굴

○ (연구보안 내실화 의견) 연구보안 체계 내실화를 위한 현장 연구자들의 제언 기반 시사점 도출

※ 필요시 연구기관·전문기관 담당자, 정부 등 다양한 실무 이해관계자 중심의 전문가 위원회를 구성하여 집중적으로 논의

❑ 연구보안 시범운영 정책설계 및 운영지원

○ (시범운영 기초자료 수집) 시범운영의 목적, 관련법 등 법적 근거, 시범운영 대상 및 운영방식 정의, 시범운영 범위 등 도출

○ (시범운영 추진체계 탐색) 주요 시범운영 수행 내용 정의 및 결과 환류 주요 내용 탐색

- 국외수혜사항보고 및 보안등급별 연구보안 관리 차별화 등 시범운영기관(학/연)의 내규 개정 및 세부활동 상세설계 등을 지원하고 이를 현장지침(안) 설계의 근거로 활용할 수 있는 방안을 모색

3 보안등급 분류체계 설계를 위한 탐색적 연구

❑ 제도개선사항에 부합하는 보안등급 분류체계 마련을 위한 현장의견 수집

○ (전문가 자문) 전문가* 의견수렴을 통해 등급분류 고려사항에 대한 의견수렴을 통한 정책적·기술적 고려사항 탐색

* 부처, 전문기관, 과제기획위·평가단 참여 민간위원 위주로 자문 pool을 구성하고, 필요시 위원회 구성·운영

- (정책적 고려사항 탐색) 연구보안 정책방향, 관련 법률 및 규정, 윤리적 고려사항 등
- (기술적 고려사항 탐색) 기술 및 연구 분야, 분야별 데이터 민감성 및 보안 위험성 등

※ 과제지원유형별, 기술분야별, 과제수행 전주기별(단계별) 특성 등 국가연구개발 세부과제 속성을 전반적으로 검토

❑ 국가전략기술 등 기술분야별 보안과제 및 민감과제의 분류체계 기반 등급분류 자동화* 가능성 탐색

* 국가과학기술표준분류체계 및 요약문 등을 활용한 기계학습 기반의 자동분류

- (정책적 실행가능성 탐색) 분류 자동화 관련 정책적 · 법적 실행 가능성 탐색
- (기술적 구현가능성 탐색) 분류 자동화를 위한 기술적 구현 가능성 탐색

※ 국가연구개발사업 조사·분석 상 세부과제 수준의 정보를 활용하여 가능성을 탐색

제3절 연구개발과제의 추진전략·방법 및 추진체계

1 연구보안 집행 전담조직 설립방향 수립을 위한 사전조사

❑ 국외 연구보안 조직 사례 및 국내 산업보안 집행 전담조직 운영현황 조사

○ 주요국의 해외 연구보안 전담조직 수립·운영 현황과 국내 산업보안 전담조직의 기구적 특성·역할 조사

- (해외) 사례조사 및 문헌연구를 토대로 미국, 일본, 영국, 호주 등 주요국의 해외 연구보안 전담조직 수립 여부와 운영 현황 등을 조사
- (국내) 사례조사 및 문헌연구를 토대로 국내 산업보안 전담조직의 설립목적, 법적 근거, 지원대상, 지원내용, 주요활동 및 조직 구성 등 조사

❑ 집행 전담조직의 기구적 특성에 대한 연구보안 취급 실무자 및 전문가 의견 수집

○ 전문가 자문회의 기반으로 현장연구자, 전문기관/연구기관 실무자 및 법률전문가 의견 수집

- 필요시 위원회 구성 방안도 고려하되, 다양한 의견 수집 위주로 수행하며, 대면/화상/서면자문 등 다양한 채널 활용

○ 연구개발비의 지급 및 사용 관련 R&D 제도문의 질의 대응 체계 구축·운영

2 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출

❑ 연구보안 현장지침 항목 도출에 참고 가능한 국내외 산업보안 및 연구보안 현장지침 사례 조사

○ (사례조사 및 문헌연구) 국내·외 유사사례 조사 및 관련 문헌연구를 토대로 현장지침 항목 탐색

❑ 현장연구자와 연구기관을 대상으로 현장지침 고려대상 항목 도출

○ (관계자 의견 수렴) 전문가 자문회의 및 기관보안담당자 등 현장연구자, 연구기관 실무자 의견 수집

- 필요 시 위원회 구성 방안도 고려하되, 다양한 의견 수집 위주로 수행하며, 대면 및 화상회의, 서면자문 등 다양한 채널 활용

❑ 현장연구자 중심의 연구보안 인식조사 등 설문조사 및 시사점 도출

○ (문항 설계) 현장연구자의 특성을 고려한 연구보안 인식조사 문항 설계

○ (설문 수행) 설계한 문항을 토대로 현장연구자 대상 설문조사 수행

○ (결과 분석) 수집한 결과 분석 및 시사점 도출

❑ 연구보안 시범운영 정책설계 및 운영지원

○ (사례조사) 시범운영 관련 사례조사 및 문헌연구를 통해 시범운영 참고사항 도출

○ (실무협의체 설계) 시범운영 기관 소속 연구자 및 실무자 위주의 업무협의체 구성

3 보안등급 분류체계 설계를 위한 탐색적 연구

❑ 내실화 방안에 부합하는 보안등급 분류체계 마련을 위한 현장의견 수집

○ (전문가 자문) 정책적·기술적 고려사항 도출을 위해 분야별 전문가들을 대상으로 자문 수행

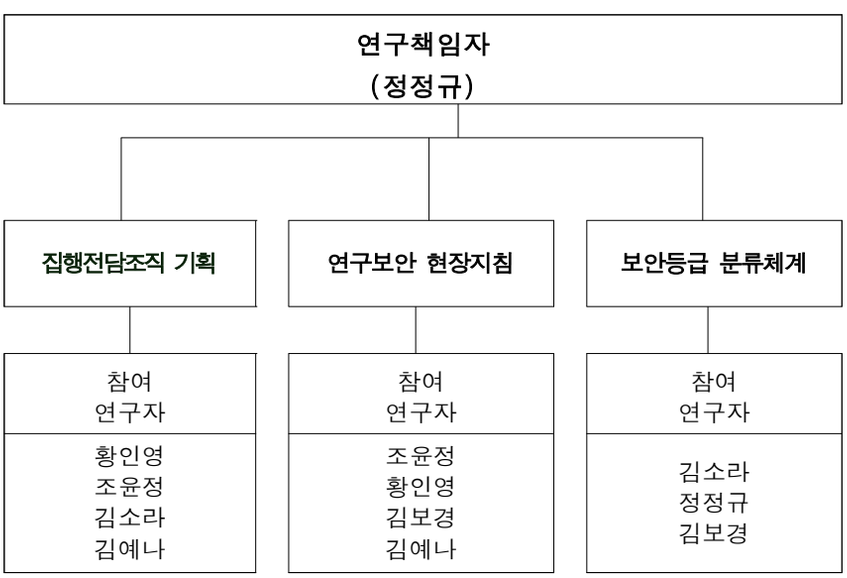
- 현장의견 수집 시, 연구기관의 운영실태 등도 포함하여 현장 적용 가능한 절차 도출 시 참고가 되도록 고려

❑ 국가전략기술 등 기술분야별 보안과제 및 민감과제의 분류체계 기반 등급분류 자동화 가능성 탐색

○ (전문가 활용) 필요시 전문가 자문 또는 활용을 통해 기계학습 SW 구현 가능성 탐색

〈표 1-1〉 **본 연구의 수행일정 및 주요 결과물**

구분	세부 연구목표	세부연구 개발 내용	가중치 (연구비)	추진일정				주요결과물
				11	12	1	2	
1	연구보안 집행 전담조직 설립방향 수립을 위한 사전조사	국외 연구보안 조직 사례 및 국내 산업보안 집행 전담조직 운영현황 조사	23.6% (30,000)	■	■	■		연구보고서
		연구보안 취급 실무자 및 전문가 의견 수집		■	■	■	■	법령개정안 연구보고서
		국내외 사례를 종합한 벤치마크 관점의 시사점 도출					■	연구보고서
2	연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출	국내외 산업보안 및 연구보안 현장지침 사례 조사	43.3% (55,000)	■	■			연구보고서
		현장연구자와 연구기관을 대상으로 현장지침 고려 대상 항목 도출		■	■	■	■	연구보고서
		현장연구자 중심의 연구보안 인식 등 설문조사		■	■	■		설문조사 보고서
		연구보안 시범운영 정책설계 및 운영지원		■	■	■	■	시범운영 방안(안)
3	보안등급 분류체계 설계를 위한 탐색적 연구	보안등급 분류체계 마련을 위한 현장의견을 수집	33.1% (42,000)	■	■	■	■	연구보고서
		분류체계 기반 등급분류 자동화 가능성 탐색			■	■		연구보고서



[그림 1-1] **본 연구의 추진체계 도식**

제2장 연구보안 전담조직 설립방향 수립을 위한 사전조사

제1절 개요

1 연구배경 및 필요성

○ 최근 글로벌 기술패권경쟁과 더불어 R&D 전주기적 해외 간섭(foreign interference) 위협 사례들이 이슈화되어* 미국, 일본, 영국, 호주 등 기술선진국들을 중심으로 연구보안 관련 체계적 정책 대응 및 국제 공조 강화를 추진 중임

* (미국) 하버드대 찰스리버 교수 기소(`20.1.), (일본) 요미우리 신문 일본인 연구자 44인 해외 인재 프로젝트 연루 보도(`21.1.1.), (호주) 호주 의회 정보 · 안보공동위원회(PJCIS)의 '호주 고등교육 및 연구 부문에 영향을 미치는 국가안보 위협에 대한 보고서' 발간 (`22.3.25.) 등

○ 이러한 환경 변화 속에서 정부는 연구보안 체계 내실화를 위한 각종 제도적 · 정책적 기반을 강화 중이나, 현재 전담조직 및 인력, 상담 채널등 전담 지원기능의 부족으로 인해 향후 체계적 집행 관련 한계 가능성 존재

※ 전문기관은 전담조직(6%, 1개) 및 인력(26%, 4개)이 미비하며, 연구기관 중 전담조직이 있는 기관은 47.2%(43개), 전담인력이 있는 기관은 18%(9개) ('23.6월 설문)
※ 국정원이 R&D 소관부처와 합동으로 연구보안 실태점검을 실시하나, 인력 부족 등 물리적 한계로 인해 국가R&D 수행기관 13,964개('21년 기준) 중 연 10개~20개 기관에 대한 점검만을 실시하는 상황임
※ 대학 연구자 45.8%가 참여연구원의 이·퇴직 등으로 인한 연구성과 유출을 우려하나, 연구자가 유출 우려를 소속기관과 상담한 경험은 미미(4.1%) ('23.6월 설문)

- 「국가연구개발혁신법」 시행(`21.1.)에 따라 「국가연구개발사업 보안대책」(8개 부처 고시)을 과기정통부 주관으로 제정(`22.6.)하고, 「국가전략기술 육성에 관한 특별법」 제정(`23.3.) 등을 통해 연구보안 규정을 체계화하여 제도적 기반을 강화하였고, 「신뢰받는 연구생태계 구축을 위한 연구보안 체계 내실화 방안(안)」 국가과학기술자문회의 의결(`23.9.)에 따라 구체적 정책방향 제시
- 보안대책 연구현장 안착을 위한 정부의 노력에도 불구하고 전반적인 연구현장의 인식 미비와 인력 부족 등으로 인해 관련 정책의 효과적 집행에 한계가 존재하는 바, 연구보안 정책을 전담 집행하는 조직 신설의 필요성이 절실한 상황임

○ 과거 2000년대 초 첨단기술 유출의 심각성이 대두*되어, 정부는 「산업기술유출방지 및 보호에 관한 법률」 제정(`06.10.) · 시행(`07.4.) 및 한국산업기술보호협회 신설(`07.10) 등 산업기술 보호를 위한 기반 마련을 추진한 바 있음

* '07년 한해 국가정보원에 의해 적발된 기술 해외유출 사건은 32건으로, 피해액이 89조 7,000억원에 달하였으며 생계형 기술유출에서 외국 정부와 연계된 기업형으로 변모하는 등 대형화 추세가 지적됨

- 당시 정부는 「산업기술유출방지 및 보호에 관한 법률」 제16조에 의거, 산업기술 유출방지 및 보호에 관한 시책을 효율적으로 추진하기 위해 산업보안 분야의 국내 최초 민간기구인 한국산업기술보호협회를 설립*한 바 있음

  * 미국 산업보안협회(ASIS) 및 독일 산업보안협회(ASW) 등 해외 민간단체 사례 참고

○ 최근 G7등 국제협의체에서 연구보안이 주요 이슈로 제기되는 등* 주요국들을 중심으로 연구보안 정책의 중요성에 대한 글로벌 공감대가 형성 중인 바, 이들 주요국들은 심화되는 연구보안 위협에 선제적으로 대응하기 위해 전담 조직의 필요성을 일찍이 절감하고 현재 총괄조직 및 집행조직을 이미 신설하였거나 신설 중에 있음

* 2022년 6월 12일부터 14일까지 독일 프랑크푸르트 암마인에서 개최된 G7 과학장관회의*에서 「G7 과학장관성명」(G7 Science Minister's Communiqué) 발표 ('22.6.14)하였으며, 주요국 정부들은 연구생태계의 지속적 자유, 개방성, 진실성, 보안과 더불어 기술의 책임 있는 사용을 효과적으로 보장할 책임 강조

- 미국 NSF의 OCRSSP* 설립 사례와 같이 주요국들은 연구보안 집행조직 신설을 통해 연구보안 정책 추진기반 강화 중

  * Office of Chief of Research Security Strategy and Policy

○ 우리나라 역시 마찬가지로 현장 연구보안 수요에 효과적으로 대응하고, 체계 내실화 방안(안)에서 제시한 후속조치의 지속적 이행을 위해서는 전담 인력을 갖춘 집행조직이 절실한 상황으로, 이에 대한 진정성 있는 검토가 필요한 시점임

- 전담 집행조직 설립을 통해 체계 내실화 방안(안) 및 보안대책 등 연구보안 정책의 체계적·효과적 이행 및 연구현장의 지속적 의견 반영을 통한 제도 개선, 보안점검 활성화, 연구현장 교육 및 정책 수용도 제고 등이 가능할 것으로 기대

2 연구내용 및 방법론

❑ 연구내용

○ 연구보안 전담 집행조직 설립을 위한 사전 기획을 통해 설립방향 수립 시 고려할 주요 사항들에 대한 검토 및 벤치마킹이 가능한 국내외 주요 사례들 분석

- 해외 주요국* 연구보안 전담조직 및 국내 산업보안 집행조직** 유사 사례 분석

  * 미국, 일본, 영국, 호주

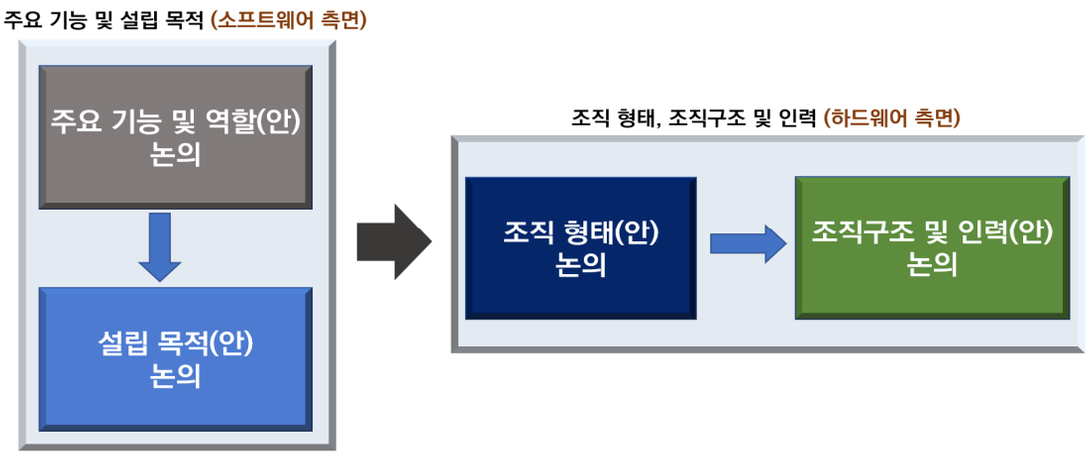
  ** 한국산업기술보호협회, 영업비밀보호센터, 대·중소기업·농어업협력재단

- 연구보안 전담조직 설립방향 수립을 위한 주요 고려사항* 검토 추진

  * 설립 목적 , 조직 기능 및 역할, 조직 형태, 조직 구조 및 인력, 법률적 고려사항(안) 등

○ 주요 고려사항의 경우, ①주요 기능 및 역할, ②설립 목적, ③조직 형태, ④조직구조 및 인력 등 조직 신설 관련 주요 이슈를 토대로 국내·해외 유사 사례 및 법률·전문가 자문 결과 등을 참고하여 기획

- 조직의 역할 및 설립 목적 등(소프트웨어 측면)에 적합한 형태 및 구조(하드웨어 측면) 탐색 추진



[그림 2-1] **연구보안 전담조직 설립방향 수립 프로세스(안)**

❑ 연구방법론

○ (문헌 연구) ①조직설립 사전기획 보고서, ②해외 연구보안 조직 신설 사례, ③국내 산업보안 조직 유사 사례, ④관련 법령 등 각종 문헌 분석 수행

- ①R&D인력교육원, ②NST연구개발전략위원회, ③서해연구소, ④기술동향예측기획센터 등 조직 신설 사전기획 보고서 다수 및 국내·외 유사 조직 신설 사례 등 참고

○ (전문가자문단 운영) 과학기술정책 및 행정조직 전문가 등 9인으로 구성하여 운영

- 전문가자문단 회의 총 2회(`23.12.4./`24.1.11.) 개최를 통해 ①설립 목적, ②주요 기능, ③조직 형태, ④조직 구조 및 인력, ⑤기타 조직 신설 관련 이슈 논의

○ (기타 전문가 자문) 연구보안 전문가를 대상으로 조직 신설 관련 자문 및 원고 위탁 등

○ (법률 자문) 과학기술정책 경험이 풍부한 법률전문가(변호사 포함) 대상 연구보안 조직 신설 관련 법률자문 수행

제2절 해외 주요국 연구보안 전담조직 사례 분석

1 미국

NSF OCRSSP*(연구안보전략정책실) ('20.3.신설)

* Office of Chief of Research Security Strategy and Policy

- (설립 배경) 개방적 국제협력 증진 및 국가R&D 연구보안 강화를 위해 신설, 이후 「CHIPS and Science Act」('22.9.)에서 NSF 내 해당 조직을 지속 유지할 의무 부여*

  * 「CHIPS and Science Act」 Sec. 10331-10332

- (조직 구조) **NSF내 Office of the Director(ODC, 이사장실) 산하 9개 Office 중 하나**로, 소규모 관리자급 조직임

- (인력 구성) 「CHIPS and Science Act」에 따라 풀타임 직원 **4인 이상으로 구성하여야 하나***, 현재는 Chief(실장), Deputy Chief(부실장), Staff Associate(사원) 등 3인 재직 중으로 확인됨**

  * SEC. 10331. OFFICE OF RESEARCH SECURITY AND POLICY.

  ** '24년 1월 기준

〈표 2-1〉 **NSF OCRSSP 인력 구성 ('24년 1월 기준)**

직위	성명
Chief of Research Security Strategy and Policy	Rebecca Lynn Keiser
Deputy Chief of Research Security Strategy and Policy	Sarah Stalker-Lehoux
Staff Associate	Paul E. Morris

- (주요 기능) 연구보안 관련 ①정책지원, ②자료제공, ③인식개선, ④교육, ⑤정보공개, ⑥위험평가, ⑦부처간 협력 등*

  * 기능 중 일부는 RSI-ISAO를 통해 수행

〈참고〉 **NSF OCRSSP의 주요 기능**

「CHIPS and Science Act」는 NSF의 연구보안 정책 부서의 기능에 대해 **"NSF 전반에 걸친 모든 연구보안 정책 문제를 조정하는 것"**으로 정의하며, **일곱 가지 세부 기능**은 다음과 같음

❶ **(정책지원)** 연구보안 정책 이슈를 전반적으로 조율하고, 유관 기관과 협력하여 국가안보에 영향을 미칠 수 있는 위험 식별 및 대응

❷ **(자료제공)** NSF에서 지원하는 연구보안 및 무결성 관련 모든 문제에 대해 자원 제공

❸ **(인식개선)** 연구 정책, 보안 위험, 지식재산 보호 방법 등에 대한 교육 및 홍보

❹ **(교육)** 잠재적 보안 위협 평가 관련 NSF의 프로그램 관리자와 타 부서 직원 교육

❺ **(정보공개)** 자금 신청자 및 수혜자에게 요구사항 공개 및 보고

❻ **(위험평가)** 정부 누락 점검을 위해 분석 도구를 활용하여 제안서 및 선정 내용에 대한 위험 평가(risk assessment) 수행

❼ **(부처간 협력)** 타 연방 기관과 협력하여 연구개발의 무결성을 위협하는 보안 위험을 식별 · 소통 · 대응하기 위한 정책 및 절차 수립

❑ RSI-ISAO*(연구안보 및 무결성 정보공유분석조직) (신설 진행 중)

* Research Security and Integrity Information Sharing Analysis Organization

- (설립 배경) 「CHIPS and Science Act」(`22.9.)에서 '연구보안 관련 정보 분석 및 집행 조직을 신설한다'는 조항*에 따라 설립

  * 「CHIPS and Science Act」 Sec. 10338

- (조직 및 인력) 현재 조직 공모 중으로 구체적 조직 및 인력 규모는 미정이나*, 복잡한 조직(Complex organization)으로 명시

  * 미국 내 기존 법인(대학 등) 대상 공모를 진행 중이며, 최종 선정된 법인이 RSI-ISAO 임무 수행

- (역할) ①연구 커뮤니티의 모든 구성원에게 균일한 품질의 서비스 제공, ②연구기관 등을 통한 연구자의 지원요청 대응, ③기밀이 아닌 정보만 처리, ④연구 이해관계자의 이익을 위해 다양한 정보를 기반으로 분석 수행 및 보고서 게시

- (주요 기능) 연구보안 관련 ①정보교환, ②위험평가, ③커뮤니케이션, ④보고서 작성, ⑤교육, ⑥정보수집, ⑦위험식별, ⑧기타 연구보안 조치 등

〈참고〉 **RSI-ISAO 신설(안) 개요**

○ NSF OCRSSP는 **소수 관리자로 구성된 NSF내 연구보안 총괄조직**이며 향후 **별도의 연구보안 집행조직(RSI-ISAO) 신설*** 예정으로, NSF는 해당 조직 신설 관련 프로그램을 공지한 바 있는데, 세부 내용은 다음과 같음**

* CHIPS and Science Act(SEC 10338)에 명시

** 의향서 마감일(Intent due: '23.9.22.), 제안서 마감일(Full proposal deadline: '23.10.30.)

- **(예산)** 1차년도 예산은 **최대 950만 달러**이고 2차년도부터 5차년도까지는 **연간 최소 1,000만 달러** 지원 가능하며, 지정된 목표 관련 성과에 대해 매년 평가를 받아야 함

  ※ (참고) NSF의 연구보안 예산은 FY2022 1백27만 달러, FY2023 1천만 달러가 확정된 바 있으며, FY2024(요구)는 1.3천만 달러임

  ※ (출처) NSF, FY2024 Budget Request to Congress, March 13, 2023

- **(임무)** ①정보 교환, ②표준 위험 평가 프레임워크 및 모범사례 개발, ③커뮤니케이션, ④연구보안 위험 관련 적시 보고서 제공, ⑤교육 및 지원, ⑥표준화된 정보 수집 활성화, ⑦위험 패턴 분석 및 식별 지원, ⑧연구보안 강화를 위한 기타 적절한 조치 수행

- **(대상자)** 고등교육기관, 비영리·비학술 조직, 영리 조직 등이 참여 가능하며, 모든 조직은 미국 내에 위치해야 하고 미국 법률에 따라 미국 법인으로 운영되어야 함*

  * 프로그램 공지에 따르면 NSF는 6개월 이내에 수상자 선정 여부를 안내하도록 노력한다고 명시된 바, '24년 4월 내외로 수상자가 결정될 것으로 예상

〈표 2-2〉 **미국의 연구보안 총괄조직(NSF OCRSSP)과 집행조직(RSI-ISAO) 비교**

	NSF OCRSSP	RSI-ISAO
조직 형태 및 근거 법령		
조직 형태	정부 기관 내 부서 (이사장실 직속)	미국 내 법인(독립 조직)으로, 구체적 형태는 미정 (고등교육기관, 비영리 · 비학술 조직, 영리 조직 등)
근거 법령	CHIPS and Science Act Sec. 10331-10332 (Office of Research Security and Policy and Chief of Research Security)	CHIPS and Science Act Sec. 10338 (Research Security and Integrity Information Sharing Analysis Organization)
설립 목적, 역할 및 주요 기능		
설립 목적	연구보안 관련 고급 모니터링 및 검증 활동 수행	연구보안 및 연구진실성 관련 정보공유 · 분석 수행
역할	연구보안 총괄 · 조정	연구보안 정책 집행
주요 기능	①**(정책지원)** 연구보안 관련 정책 조율 및 위험 대응 협력 ②**(자료제공)** NSF 지원 연구보안 및 무결성 문제에 대한 자원 제공. ③**(인식개선)** 연구 정책과 보안 위험에 대한 교육 및 홍보 ④**(교육)** NSF 직원 대상 보안 위협 평가 교육 ⑤**(정보공개)** 자금 신청자 및 수혜자에게 요구사항 공개 ⑥**(위험평가)** 제안서 및 선정 내용에 대한 위험 평가 수행. ⑦**(협력)** 타 연방 기관과 협력하여 보안 위험 대응 정책 수립 ※일부는 RSI-ISAO를 통해 수행	①**(정보교환)** 연구보안 관련 정보 교환 ②**(위험평가)** 표준 위험 평가 프레임워크 및 모범사례 개발 ③**(커뮤니케이션)** 포럼 및 기타 커뮤니케이션을 통해 보안 위협 정보 및 대응 노력 · 교훈 등 공유 ④**(보고서 작성)** 연구보안 위험 관련 적시 보고서 제공 ⑤**(교육)** 연구보안 교육 및 지원 ⑥**(정보수집)** 표준화된 정보수집 활성화 ⑦**(위험식별)** 위험 패턴 분석 및 식별 지원 ⑧**(기타)** 연구보안 강화를 위한 기타 적절한 조치 수행 ※Dear Colleague Letter에 "시간에 따라 기능을 단계적으로 확장한다"고 명시
조직 구조 및 인력		
조직 구조	단일 부서	미정 (조직 공모 중) ※복잡한 조직(Complex organization)으로 명시
인력 구성	4인(현재 3인)	미정 (조직 공모 중)
예산 및 주요 사업		
예산	• FY2022 1백27만 달러 • FY2023 1천만 달러 • FY2024(요구) 1천3백만 달러	• 착수연도 950만 달러 (2~5차연도) 최소 1천만 달러
주요 사업	• 연구보안 사례조사 • RSI-ISAO 설립 • 연구보안프로그램(RRSP) 연구	구체적 사업은 미정 (조직 공모 중)

2 일본

○ 일본 정부는 연구보안 업무 총괄을 위해 문부과학성 과학기술·학술정책국 산하 국제전략 전담 참사관(과장급1인)급 조직을 운영 중이며, JST에서 연구진실성 관련 업무를 연구윤리의 일환으로 수행해왔으나, 최근 조직 신설 사례는 없음

○ 그러나 최근 유사 사례로 일본 정부의 경제안보 조직 신설 사례가 존재하며, 구체적으로 국가안전보장국(NSS) 경제반 및 내각부 경제안전보장추진실 신설 사례를 참고 가능

❑ 국가안전보장국(NSS) 경제반 (`20.4.신설)

○ (설립 배경) 아베 정권기 미·중 무역마찰 등 경제패권 경쟁이 국가안보와 밀접하게 관련되어 있다는 판단 하에 경제정책을 외교·안보와 통합 추진하기 위해 신설하였으며, 이에 따라 기존 외무성·방위성 중심이던 NSS 조직을 경제 중시로 전환

○ (조직 구조) 내각관방* 국가안전보장국(NSS)**(정부 부처)내 부서로, 단일 부서임

* 우리나라의 국무조정실에 해당하나, 위상은 우리나라의 대통령비서실과 유사

** 우리나라의 국가안보실에 상응

○ (인력 구성) 약 20명 규모*

* 내각심의관(경제산업성 출신) 1인, 과장급 참사관 4인(총무성, 외무성, 재무성, 경찰청 출신) 포함

○ (주요 기능) 국가안보 문제와 관련된 경제정책을 기획·입안하고 관계부처 간 업무를 조정하는 경제안보 총괄·조정* 역할 (예: 경제안보 법제화 주도** 등)

* NSS경제반과 경제안전보장추진실 간 역할 분담이 명확하지 않으며, 양 조직 간 일부 기능의 중첩 가능성 존재

** NSS경제반 반장이 경제안전보장법제실(경제안전보장추진실 전신) 실장으로 이동하여 경제안보 법제화 주도

※ 출처: 박재적 외, (2023) '인도·태평양 지역 경제안보" 주요국의 국내정치 동학과 한국의 경제안보전략. 대외경제정책연구원.

❑ 내각부 경제안전보장추진실 (`22.8.신설)

○ (설립 배경) 「경제안전보장추진법」 공포(`22.5.) 후 「경제재정운영과 개혁의 기본방침」에서 '정세 변화에 신속·유연하게 대응하기 위해 관계부처 사무를 조정하는 조직 신설'을 명시함에 따라 신설하였으며, 기존 경제안전보장법제준비실을 개편

○ (조직 구조) 내각부(정부 부처) 내 부서로, 단일 부서임

○ (인력 구성) 총 50여 명으로, 기존 경제산업성, 방위성 등에서 간부급 18명(실장1명, 차장3명, 참사관 14명) 등의 직원을 모아 출범

○ (주요 기능) NSS 경제반과 함께 범부처 경제안보 논의를 신속 주도하며, 성청 간 경제안보 정책조정 역할 담당

3 영국

❑ RCAT*(연구협력자문팀) ('22.3.신설)

* Research Collaboration Advice Team

○ (설립 배경) 연구자들에게 적대적 활동으로부터 연구자산을 보호하는 방법에 대한 조언을 제공하고, 국제협력이 안전하게 이루어지도록 지원하기 위해 정부 내에 전담 팀 신설

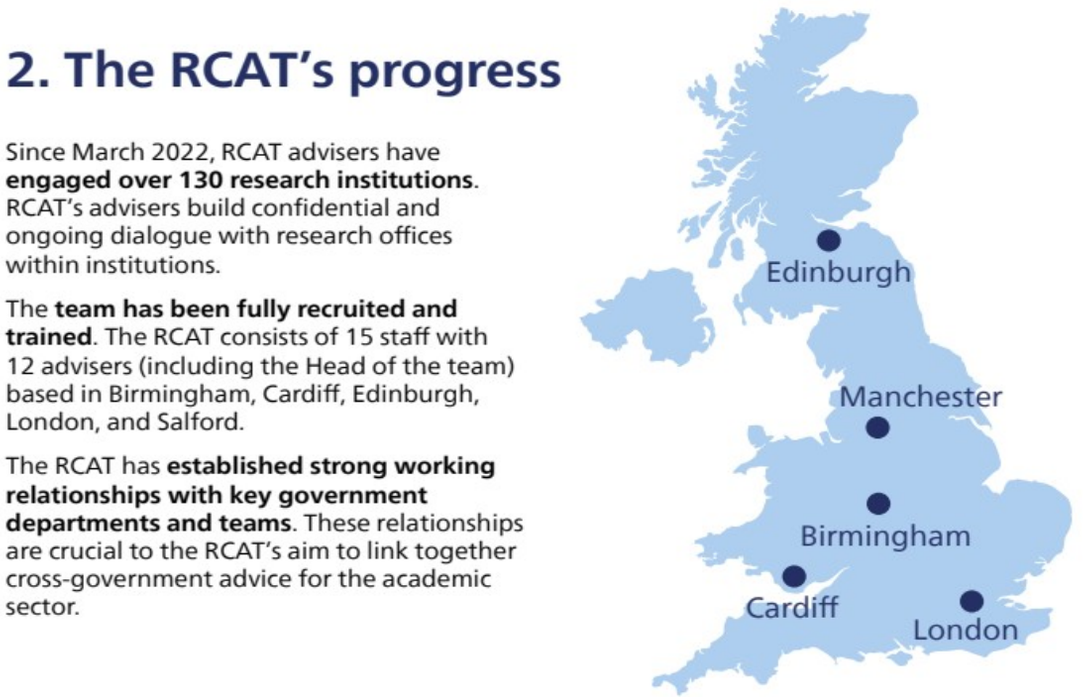
※ 출처: BEIS. (2021) "Dedicated government team to protect researchers' work from hostile activity", Press Release.

○ (조직 구조) 과학혁신기술부 산하 특별기구(정부 부처)로, 현재 런던, 맨체스터, 에딘버러, 버밍엄, 카디프에 사무실 운영

○ (인력 구성) 총 27명으로, 15명의 직원(staff) 및 12명의 자문역(adviser)으로 구성

※ 출처: Department for Science, (2023) "Innovation & Technology, RCAT Update August 2023".

○ (주요 기능) ①국제연구협력시 국가안보 문제해결을 위한 조언 ②기관 연구문화 지원 및 연구보안 인식 제고, ③정보수집 및 공유



[그림 2-2] RCAT 소개 및 주요 사무실 위치

자료: Department for Science, Innovation & Technology. (2023) RCAT Update August 2023. DSIT Report.

4 호주

❑ UFIT*(대학해외간섭TF) ('19.8.신설)

*University Foreign Interference Taskforce

- (설립 배경) 외국의 간섭으로부터 대학을 보호하고, 신뢰와 회복력을 갖춘 환경을 조성하며, 세계적 수준의 연구 성과를 도출할 수 있도록 지원하기 위해 설립
- (조직 구조) 교육부 산하 특별기구 (정부 부처)
- (인력 구성) 미공개
- (주요 기능) ①대학을 위한 연구보안 가이드라인 제공, ②국가이익에 필수적인 기술정보 제공, ③대학의 사이버보안능력 강화 방안 제공

제3절 국내 산업보안 전담조직 유사 사례 분석

1 한국산업기술보호협회

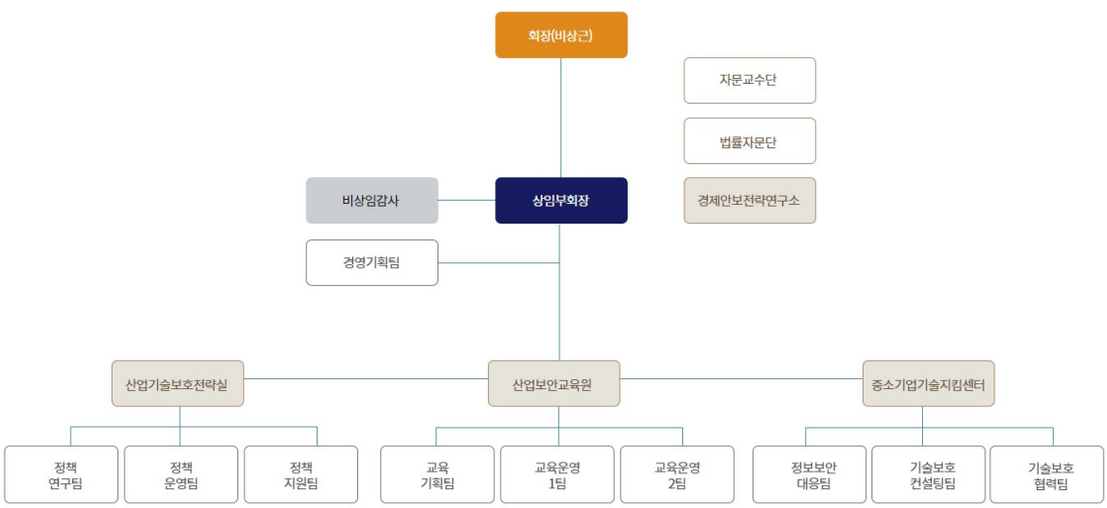
※ '07년 신설

○ (설립 배경) 「산업기술의 유출방지 및 보호에 관한 법률」 제16조*에 따라 산업통상자원부 및 국정원이 설립 추진

* 산업기술보호협회의 설립 등

○ (조직 구조) 산업통상자원부 소관 비영리법인(사단법인)으로, ①산업기술보호전략, ②산업보안교육, ③중소기업기술보호 관련 3실 9팀으로 구성

※ (출처) 산업통상자원부 비영리법인 현황 정보 (산업통상자원부)



[그림 2-3] **한국산업기술보호협회 조직도**

자료: 한국산업기술보호협회 홈페이지(kaits.or.kr)

〈참고〉 **한국산업기술보호협회 설립 초창기 조직도**

○ 설립 초창기 당시 주요 업무는 ①정책 연구 및 지원, ②실태조사 실시, ③산업기술보호 교육 프로그램 운영, ④기업지원, ⑤국제협력 추진, ⑥산업기술보호 인식제고 활동으로 소개

자료: 한국공학교육학회 (2008) 연구센터소개-한국산업기술보호협회, Ingenium, 15(1): 42-44.

○ (인력 구성) 30명 내외로 구성*

* '24년 1월 기준(출처: 사람인)

○ (주요 기능) 「산업기술의 유출방지 및 보호에 관한 법률」 제16조제4항에 명시된 바와 같이 ①정책 개발 및 협력, ②해외유출 정보 전파, ③상담 · 홍보 · 교육 · 실태조사, ④자료수집 · 분석 및 발간, ⑤산업기술 보호 지원, ⑥산업기술분쟁조정위원회 업무 지원, ⑦기타 사업 수행

산업기술의 유출방지 및 보호에 관한 법률

제16조(정관의 기재사항) ④협회는 다음 각 호의 업무를 행한다.

1. 산업기술보호를 위한 **정책의 개발 및 협력**
2. 산업기술의 **해외유출 관련 정보 전파**
3. 산업기술의 유출방지를 위한 **상담 · 홍보 · 교육 · 실태조사**
4. 국내외 산업기술보호 관련 **자료 수집 · 분석 및 발간**

4의2. 국가핵심기술의 보호 · 관리 등에 관한 지원 업무

5. 제22조제1항에 따른 산업기술의 보호를 위한 **지원업무**
6. 제23조의 규정에 따른 **산업기술분쟁조정위원회의 업무지원**
7. **그 밖에** 산업통상자원부장관이 필요하다고 인정하여 위탁하거나 협회의 정관이 정한 사업

2 영업비밀보호센터

※ 한국지식재산보호원의 하위부서로 `19년 신설

- (설립 배경) 한국지식재산보호원은 「발명진흥법」 제55조의2*에 따라 특허청 주도 하에 설립되었으며, 이후 「특허청공고 제2016-6호(부정경쟁행위방지 및 영업비밀보호 사업 위탁기관 지정)」에 따라 한국지식재산보호원 내 경영혁신본부 산하에 영업비밀보호센터 설립

  * 한국지식재산보호원의 설립

- (조직 구조) 특허청 산하 공공기관(한국지식재산보호원) 내 부서로 1센터 1팀

- (인력 구성) 13명* 재직 중이며, 센터장1명, 팀장1명, 책임2명, 전문위원1명**, 선임2명, 전임3명, 주임3명으로 구성되어 ①영업비밀보호 법률상담(변호사 전문위원 포함), ②컨설팅 수행 및 ③기타 업무를 수행중인 것으로 확인

  * `24년 1월 기준

  ** 전문위원은 변호사로 법률자문, 판례분석, 컨설팅, 교육 수행

※ (출처) 한국지식재산보호원 공식 홈페이지 내 조직도

〈표 2-3〉 **영업비밀보호센터 인력 구성 (`24년 1월 기준)**

직위	담당업무
센터장	총괄
팀장	사업 기획/관리, 대외협력
책임	법제도 연구, 법률상담
책임	영업비밀 보호 기초컨설팅 운영, 수행
전문위원(변호사)	법률자문, 판례분석, 컨설팅, 교육
선임	IP-MAX 전략 기초컨설팅 운영 및 수행
선임	영업비밀 보호 심화컨설팅 수행
전임	영업비밀 보호 심화컨설팅 수행
전임	연구용역 운영, 관리, 정기교육 운영
전임	제도/지원사업 홍보
주임	관리시스템, 홈페이지 운영
주임	사업관리 지원, 판례수집, 법률자문
주임	원본증명서비스 운영

○ (주요 기능) 공식 홈페이지에 주요 업무 여덟 가지 명시

- (교육) 영업비밀 보호 교육
- (컨설팅) 영업비밀 보호 컨설팅
- (디지털포렌식 지원) 영업비밀 유출 디지털포렌식 지원
- (상담) 온·오프라인 상담
- (시스템) 영업비밀 관리시스템 보급·운영
- (법률자문) 영업비밀 유출분쟁 법률자문
- (디지털증거 보존) 영업비밀 유출예방 디지털증거 보존지원
- (원본증명) 영업비밀 원본증명서비스

※ (출처) 영업비밀보호센터 공식 홈페이지(https://tradesecret.or.kr) (`24년1월 기준)

3 대·중소기업·농어업협력재단

※ 기술보호 전담기능 `14년도에 신규 추가

○ (설립 배경) 「대·중소기업 상생협력 촉진에 관한 법률」 제20조*에 의거하여 설립되었으며, 「중소기업기술보호법」 제14조**에 의거하여 중소기업기술 보호 지원 업무 수행

* 대·중소기업·농어업협력재단의 설립

** 중소기업기술 보호 지원 전담기관

○ (조직 구조) 중소벤처기업부 소관 비영리법인(특수법인)

※ (출처) 중소벤처기업부 비영리법인 현황 정보 (중소벤처기업부)

○ (인력 구성) 상생거래본부 산하 기술보호지원부는 1부 13명으로 구성되어 기술보호 업무를 전담하며, 부장1명, 차장2명, 과장3명, 대리4명, 사원3명으로 구성

〈표 2-4〉 **기술보호지원부 인력 구성 ('24년 1월 기준)**

직위	담당업무
부장	부서 총괄
차장	대정부/사업관리
차장	사업성과/손해액산정
과장	인식개선/홍보
과장	법제도/연구회
과장	선도기업
대리	예산관리/손해액산정
대리	실태조사/선도기업
대리	설명회/연구회/포상
대리	현장자문/신고센터
사원	선도기업/인력양성 지원
사원	예산 및 사업관리
사원	현장자문/신고센터 지원

○ (주요 기능) 「대 · 중소기업 상생협력 촉진에 관한 법률」 제20조제2항에 사업 명시*

* 해당 조문은 기관의 전체적인 기능을 명시하였기 때문에 대 · 중소기업 협력 관련 업무가 주를 이루고, 기술보호 업무는 전체 기능 중 일부로 명시됨

대 · 중소기업 상생협력 촉진에 관한 법률

제20조(대 · 중소기업 · 농어업협력재단의 설립) ② 재단은 다음 각 호의 사업을 한다.

1. 대 · 중소기업 간 **협력사업의 개발 및 운영 지원**
2. 제9조에 따른 **기술협력 촉진사업의 관리 · 운영 및 평가 지원**
3. 제17조에 따른 **수탁기업협의회의 구성 및 운영 지원**
4. 제21조, 제22조, 제22조의2, 제23조, 제24조, 제24조의2 및 제25조에 따른 **수탁 · 위탁거래의 공정화 지원**
5. 위탁기업과 수탁기업 간 **분쟁의 자율적 조정 지원**
6. 제20조의5에 따른 **대 · 중소기업상생협력기금의 관리 · 운용**
7. 「자유무역협정 체결에 따른 농어업인 등의 지원에 관한 특별법」 제2조제19호에 따른 상생협력을 위하여 농림축산식품부장관과 해양수산부장관이 지정 · 위탁하는 사업 및 같은 법 제18조의2제1항에 따른 **농어촌상생협력기금의 관리 · 운용**
8. **상생결제**의 관리 · 운영 및 보급 · 확산 지원
9. **그 밖에** 중소벤처기업부장관이 지정 · 위탁하는 사업

〈표 2-5〉 **해외 연구보안 전담조직 및 국내 산업보안 전담조직 신설 사례**

			설립일	설립 근거	조직 및 인력	역할	주요기능
해외 연구보안 전담조직	미국	NSF OCRSSP	`20.3.	「CHIPS and Science Act」 Sec. 10331-10332 (유지근거)	• NSF 내 단일부서 (정부부처) • 풀타임 4인 이상(현재 3인)	연구보안 총괄 · 조정	정책지원, 자료제공, 인식개선, 교육, 정보공개, 위험평가, 협력 ※일부는 RSI-ISAO를 통해 수행
		RSI-ISAO(예정)	(진행중)	「CHIPS and Science Act」 Sec. 10338 (설립근거)	• 미국 내 법인 (예: 대학)과 계약 예정 • '복잡한 조직' 명시	연구보안 집행 및 데이터분석	정보교환, 위험평가, 커뮤니케이션, 보고서 작성, 교육, 정보수집, 위험식별, 기타 연구보안 조치
	일본 *	국가안전보장국(NSS) 경제반	`20.4.	경제정책을 외교 · 안보와 통합 추진하기 위해 신설	• NSS 내 단일부서 (정부부처) • 20인 규모	경제안보 총괄 · 조정 ※경제안보실과 역할분담 불명확	국가안보 문제와 관련된 경제정책을 기획 · 입안하고 관계부처 간 업무를 조정
		내각부 경제안전보장 추진실	`22.8.	2022 「골태방침」	• 내각부 내 단일부서 (정부부처) • 50인 규모	경제안보 총괄 · 조정 ※NSS경제반과 역할분담 불명확	NSS 경제반과 함께 범부처 경제안보 논의를 신속 주도하며, 성청 간 경제안보 정책조정
	영국	RCAT	`22.3.	연구자산 보호 및 안전한 국제연구협력 지원을 위해 신설	• 과학혁신기술부 산하 특별기구 (정부부처, 지역 사무실 5개소 운영) • 27인 규모	연구보안 컨설팅	국제연구협력 연구보안 컨설팅, 기관 연구보안 인식 제고, 정보수집 및 공유
	호주	UFIT	`19.8.	외국 간섭에서 대학 보호, 신뢰와 회복력 환경 조성, 연구 성과 도출 지원	• 교육부 산하 특별기구 (정부 부처) • 인력 미공개	연구보안 가이드라인 등 정보 제공	연구보안 가이드라인 제공, 기술정보 제공, 대학 사이버보안능력 강화 방안 제공
국내 산업보안 전담조직	한국산업기술보호협회		`07.	「산업기술의 유출방지 및 보호에 관한 법률」 제16조	• 산자부 소관 비영리법인으로, 3실 9팀으로 구성 (사단법인) • 30인 규모	산업기술 유출 방지 지원 (집행)	정책 개발 및 협력, 해외유출 정보 전파, 상담 · 홍보 · 교육 · 실태조사,자료수집 · 분석 및 발간, 산업기술 보호 지원,산업기술분쟁조정위원회 업무 지원, 기타
	영업비밀보호센터		`19.	「특허청공고 제2016-6호」	• 특허청 산하 공공기관 내 부서로, 1센터 1팀으로 구성 • 13인 규모 (상근 변호사 1인 포함)	영업비밀 보호 지원 (집행)	교육, 컨설팅, 디지털포렌식 지원, 상담, 시스템, 법률자문, 디지털증거 보존, 원본증명
	대 · 중소기업 · 농어업협력재단		`14. (기술보호 업무)	「대 · 중소기업 상생협력 촉진에 관한 법률」 제20조	• 중소벤처기업부 소관 비영리법인으로, 1부로 구성 (특수법인) • 13인 규모	중소기업기술 보호 지원 (집행)	대 · 중소기업 협력 관련 업무가 주를 이루고, 기술보호 업무는 전체 업무 중 일부인 것으로 확인

* 일본은 연구보안 관련 최근 조직 신설이 없는 관계로, 경제안보 조직 신설을 유사 사례로 참고 가능

제4절 연구보안 전담조직 설립방향 수립을 위한 주요 고려사항 검토

1 설립 목적 고려사항(안)

○ 기관 특성·성격에 따라 부여된 기능·역할을 수행 가능하도록 명시*하여야 하며(Mission Statement), 설립목적에 '연구보안 지원' 명시 필요

* 독립법인·부설기관뿐만 아니라 기존 조직 내 부서 신설 경우에도 설립 기획 단계에서 목적 설정을 통해 향후 조직의 임무와 방향성 등을 명확화 필요

〈참고〉 공기업·준정부기관의 설립목적

○ **「공공기관의 운영에 관한 법률」 제16조**(정관의 기재사항)는 공기업·준정부기관의 정관에 **설립 목적 등을 기재하도록 의무화**하고 있음

공공기관의 운영에 관한 법률

제16조(정관의 기재사항) ①공기업·준정부기관의 정관에는 다음 각 호에 관한 사항을 기재하여야 한다. 다만, 그 공기업·준정부기관의 형태와 특성 및 업무내용상 해당되지 아니하는 사항은 기재하지 아니할 수 있다.

1. 목적
2. 명칭

〈중 략〉

14. 그 밖에 대통령령으로 정하는 사항

②공기업·준정부기관은 제6조의 규정에 따라 공기업·준정부기관으로 지정된 후 3개월 이내에 제1항의 규정에 따른 정관에 대하여 주무기관의 장의 인가를 받아야 한다. 인가받은 정관의 기재사항을 변경하는 경우에도 또한 같다.

- 따라서 본 법률에서 정의하는 설립목적은 연구보안 전담조직이 공기업 또는 준정부기관인 경우에 정관에 명시할 의무를 지님
  ※ 본 법률 외에도 타 개별법에서 정의하는 기관(예: 비영리법인) 역시 해당 근거법이나 시행령 또는 규칙에서 정관에 설립목적을 명시할 의무를 규정하기도 함
  * (예)「산업기술의 유출방지 및 보호에 관한 법률 시행령」제21조(산업기술보호협회의 설립 등)는 산업기술보호협회를 설립하려는 대상기관이 정관에 목적을 명시하여 산업통상자원부장관의 인가를 받아야 할 의무를 명시
- 그러나 기존 조직 내 부서 등 타 유형의 조직일 경우에도 설립 기획 단계에서 목적을 명확화하여 **향후 조직의 임무와 방향성 등을 정의하는 데에 유용**

○ 참고 가능한 유사 사례로 해외 연구보안 전담조직 및 국내 산업보안 전담조직의 설립 목적을 볼 때, 대부분 관리보다는 지원을 토대로 국가 수준에서 긍정적 파급효과를 창출하고자 하는 의지를 명시

- (미국 NSF OCRSSP) CHIPS and Science Act.에 직접 설립 목적이 명시되어 있지는 않으나, NSF 공식 홈페이지에 **"OCRSSP는 연구 보안과 관련된 고급 모니터링 및 검증 활동을 수행하도록 승인 된 NSF 내 유일한 사무소***"임을 명시

  * (원문) OCRSSP is the only office within NSF approved to conduct advanced monitoring and verification activities related to research security.

- (한국산업기술보호협회) **"산업기술의 부정한 유출을 방지하고, 산업기술을 보호함으로써 국내 산업의 경쟁력을 강화하고 회원 간 상호협력을 도모함으로써 국민경제 안정에 기여함"**

- (영업비밀보호센터) 영업비밀보호센터는 한국지식재산보호원의 원내 부서로, 한국지식재산보호원의 설립목적은 **"지식재산 보호에 관한 지원 사업을 통한 국가 지식재산 경쟁력 제고와 국민 경제 발전에 기여"**임

- (대 · 중소기업 · 농어업협력재단) **"대·중소기업·농어업 간 기술, 인력, 판로 등 협력사업을 추진하고 우수 협력 모델의 발굴을 통해 동반성장 문화를 확산하여 공정거래 관계 조성을 지원하기 위하여 설립"**

〈표 2-6〉 **국내외 유사 기관들의 설립목적 예시**

기관	설립 목적
NSF OCRSSP	• OCRSSP는 연구 보안과 관련된 고급 모니터링 및 검증 활동을 수행하도록 승인된 NSF 내 유일한 사무소 ※ (원문) OCRSSP is the only office within NSF approved to conduct advanced monitoring and verification activities related to research security.
한국산업기술보호협회	• 산업기술의 부정한 유출을 방지하고, 산업기술을 보호함으로써 국내 산업의 경쟁력을 강화하고 회원 간 상호협력을 도모함으로써 국민경제 안정에 기여함
한국지식재산보호원	• 지식재산 보호에 관한 지원 사업을 통한 국가 지식재산 경쟁력 제고와 국민 경제 발전에 기여
대 · 중소기업 · 농어업협력재단	• 대·중소기업·농어업 간 기술, 인력, 판로 등 협력사업을 추진하고 우수 협력 모델의 발굴을 통해 동반성장 문화를 확산하여 공정거래 관계 조성을 지원하기 위하여 설립

○ 전문가자문단 자문의견 취합 결과 역시 마찬가지로 **지원기능을 강조할 필요**가 있다는 의견이 많았고, 이를 통해 **국가 차원의 연구보안 수준 강화, 산업 선도 및 혁신역량 제고 등의 파급효과를 기대**할 수 있다는 의견이 제시됨

〈표 2-7〉 **설립목적 관련 전문가 자문 결과**

	전문가 의견
의견1	• 자율규제를 유도할 수 있는 지원기능 강조 필요 (기본적으로 규제기능을 완전히 포기할 수 없으므로, 자율규제를 유도하는 형태로 규제기능 강화)
의견2	• 국가연구자산을 보호하고 부정한 유출을 방지하기 위함.
의견3	• ① 연구자산의 보호, ② 연구보안의 이해/인식의 공유, ③ 연구보안 전략/정책 기획으로 구성
의견4	• 각 연구기관의 국가차원의 전략과학기술을 체계적으로 보호할 수 있도록 '보안' 지원 역할
의견5	• "연구 보안" 기준 이행을 위한 연구 현장 자원 서비스 제공 • "연구 보안" 인프라·제도 구축 및 운영
의견6	• 연구보안 활동을 수행하고 연구기관 등의 연구보안을 지원함으로써 국가연구혁신역량을 강화하기 위함
의견7	• 연구 안정성, 산업 및 과학기술(R&D) 경쟁력 강화 • ① R&D 경쟁력 → 과학기술 선도, ② 산업 경쟁력 → 산업 선도, ③ 국가 안보
의견8	• 각 연구기관의 보안 이슈를 자체적으로 관리할 수 있는 노하우를 얻을 수 있는 Reference center • 이를 통해 국가차원 전략기술 및 자산을 보호

○ 국내외 유사 사례들 및 전문가 자문 결과를 종합할 때, 연구보안 전담 집행조직의 설립목적 설정 시 **관리보다는 연구보안 현장 및 정책 지원 등을 토대로 연구자산 유출에 따른 국가적 피해를 사전에 예방하겠다는 방향**으로 추진 고려 필요

○ 이러한 설립 목적은 조직 명칭과도 관련 있는 바, 향후 조직 명칭 부여 시 '관리'라는 표현을 지양하고 '지원', '협력' 등 키워드를 활용하여 다양한 각도로 고민 필요

2 조직 기능 및 역할 고려사항(안)

❑ 주요 기능

○ 문헌연구, 사례조사 및 전문가 자문 등을 토대로 연구보안 전담 집행조직의 ①주요 역할 및 기능을 선정하고 ②기능 간 우선순위(안) 도출을 추진함

- 전문가 자문 및 국내외 유사 조직의 역할 및 기능을 토대로 향후 연구보안 전담 집행조직이 수행 가능할 것으로 고려되는 기능(안) Pool 도출
- 전문가 자문을 통해 해당 기능들의 우선순위(안) 도출
- 국내·외 유사 조직들이 지닌 주요 기능과의 비교를 통해 현실 적용가능성 및 타당성 검토

○ 해외 연구보안 전담조직 및 국내 산업보안 전담조직 등의 기능을 참고하여 전문가 자문 등을 토대로 연구보안 전담조직이 수행 가능할 것으로 고려되는 기능(안) 14개 Pool을 도출하였으며, 아래와 같음

※ 전문기관 · 연구기관·KISA(정보보호)·산업보안 집행조직 등과 협의체 운영

(1) 전문기관·연구기관 협조 · 관리

※ 전문기관 · 연구기관·KISA(정보보호)·산업보안 집행조직 등과 협의체 운영

(2) 국내 · 해외 연구보안 동향 파악 및 정책연구

(3) 연구보안 빅데이터 분석

(4) 보안·민감과제 분류가이드 마련 및 분류지원

(5) 연구보안 컨설팅

(5) 연구현장 보안인프라 구축지원

(6) 보안·민감과제 참여 연구원 관리

(7) 연구현장 보안 가이드라인 마련

(8) 연구보안 교육 콘텐츠 개발·보급

(9) 연구보안 상담창구 운영 · 위험관리

(10) 부처 · 국정원 실태점검 지원

(11) 핵심인력 상담 · 보고 · 지원

(12) 연구보안 전문인력 육성

(13) 해외 자금 수혜신고사항 검증

(14) 연구보안 법률자문

○ (기능) 규제기관이라는 인식 등 연구현장의 반발 가능성을 고려, **관리보다는 지원에 초점**을 맞춰 **①정책, ②교육, ③홍보, ④가이드라인 개발** 등을 중심으로 구성 필요

- 전문가자문단 자문 결과 **①연구보안 동향 파악 및 정책연구, ②빅데이터 분석, ③가이드라인 마련** 등의 우선순위가 높았으며, 이는 현재 **미국 NSF OCRSSP의 주요 기능*과도 유사**

  * 「CHIPS and Science Act」에 따르면 NSF OCRSSP는 ①정책지원, ②자료제공, ③인식개선, ④교육, ⑤정보공개, ⑥위험평가, ⑦협력 기능을 수행하도록 규정하여 규제보다는 연구현장 지원에 초점을 맞춤

〈표 2-8〉 **조직 기능(안) 우선순위 전문가자문단 자문 결과**

기능(안)	우선순위
국내·해외 연구보안 동향 파악 및 정책연구	1
연구보안 빅데이터 분석	2
연구현장 보안 가이드라인 마련	3
보안·민감과제 분류가이드 마련 및 분류지원	4
연구현장 보안인프라 구축지원	5
전문기관·연구기관 협조·관리	6
연구보안 컨설팅 및 법률자문	7
연구보안 교육 콘텐츠 개발·보급	8(동점)
연구보안 상담창구 운영 및 위험관리	8(동점)
핵심인력 상담·보고·지원	10
보안·민감과제 참여 연구원 관리	11(동점)
연구보안 전문인력 육성	11(동점)
부처·국정원 보안 실태점검 지원	13
해외 자금 수혜 신고사항 검증	14

- 따라서 향후 기획 구체화 시 본 우선순위(안) 도출 결과를 참고하여 **조직의 기능을 연구보안 지원 위주로 설정**하되, 조직이 필수로 수행해야 할 기능을 1~2개 정도 추가하는 방향으로 추진 가능*

  * (예) 보안 실태점검 지원 등

○ (역할) **'관리'를 지양**하고, **연구보안 '지원'을 주력**으로 하는 조직으로 방향 설정 필요

- 설립 초기부터 과제관리에 집중 시 규제기관의 성격이 부각되어 연구자 반감이 거셀 수 있으므로, 연구기관·연구자 대상 연구보안 지원에 초점*

  * **한국산업기술보호협회** 역시 **설립 초창기에** ①정책 연구 및 지원, ②실태조사 ③산업기술보호 교육 프로그램 운영, ④기업지원, ⑤국제협력 추진, ⑥산업기술보호 인식제고 활동을 주로 수행하여 **규제보다는 지원 역할에 초점을 맞춘 사례가 존재**하여, 이를 **참고 가능**

3 조직 형태 고려사항(안)

○ 조직의 형태는 크게 **국가조직, 공공조직, 그리고 민간조직**으로 구분되며 연구보안 전담 집행조직의 형태 역시 해당 틀 안에서 논의 가능한 바, 각 조직의 특성은 다음과 같음

- (국가조직) 넓은 의미의 정부조직을 뜻하며 입법부, 사법부, 행정부로 구성. 행정부는 국가행정조직과 지방자치단체로 구성
- (공공조직) 「공공기관의 운영에 관한 법률」 등에서 규정된 정부 출연기관, 공단, 공사, 공공시설 등을 포함
- (민간조직) 경영의 효율화를 통한 이윤 극대화를 추구

○ 우리나라 연구보안 전담 집행조직 신설 시 국가조직(정부조직)을 제외한 **민간조직 또는 공공조직의 두 유형 내에서 논의하는 것이 현실적**

- 국제연구협력과 연구보안을 국익의 관점에서 동시에 고려해야 하는 업무의 성격을 고려하면 공무원들이 주축이 되는 정부 조직으로 설치하는 것도 고려 가능하나*, 심사를 거쳐야 하기 때문에 설치 시기가 늦어질 수도 있음

  * (참고) 미국은 공무원 조직인 NSF 내에 연구보안전략정책실이 설치되어 있음. 일본, 호주, 네덜란드 등도 연구지원 전문기관이 아니라 공무원 조직으로 연구보안업무을 추진하고 있음

- 집행조직의 특성상 설치 후에 업무가 확대될 가능성이 높으며 그에 따라 정원과 예산을 늘려야 하는데 정부 조직이라는 경직성 때문에 상대적으로 유연한 대응이 어렵다는 한계 존재*

  * 상기한 국가조직 신설의 경우 「정부조직법」 개정이 필요한 사안이며, 참고 가능한 유사 사례로 국내 산업보안 전담 집행조직은 국가조직(정부조직)이 아닌 비영리법인 및 공공기관 내 부서의 형태로 운영 중임

- 따라서 연구보안 전담조직이 집행조직의 성격을 지닌다고 가정할 때 **중앙행정기관의 형태보다는 민간 또는 공공조직이 보다 현실적**

○ 참고 가능한 유사 사례로, 국내 산업보안 전담 집행조직은 특정 개별법에 따라 설립된 정부부처 산하 비영리법인의 형태 또는 공공기관 내 부서 형태로 존재

〈참고〉 국내 산업보안 전담 집행조직 형태

❶ (한국산업기술보호협회) 산업통상자원부 산하 비영리법인(사단법인)*

* 「산업기술의 유출방지 및 보호에 관한 법률」 제16조(산업기술보호협회의 설립 등)에 의거하여 설립

※ (출처) 산업통상자원부 비영리법인 현황 정보 (산업통상자원부)

❷ (영업비밀보호센터) 특허청 산하 공공기관(한국지식재산보호원) 내 부서*

* 특허청공고 제2016-6호(부정경쟁행위방지 및 영업비밀보호 사업 위탁기관 지정)에 따라 한국지식재산보호원 내 경영혁신본부 산하 센터로 개설되어 운영 중임(`24년 1월 기준)

❸ (대 · 중소기업 · 농어업협력재단) 중소벤처기업부 산하 비영리법인(특수법인)*

* 「대 · 중소기업 상생협력 촉진에 관한 법률」 제20조(대 · 중소기업 · 농어업협력재단의 설립)에 의거하여 설립

※ (출처) 중소벤처기업부 비영리법인 현황 정보 (중소벤처기업부)

○ 따라서 본고는 고려 가능한 3개 형태(안)을 **①독립 법인*, ②부설 기관**, ③기관 내 부서*****로 제시하며, 각 형태(안)의 장 · 단점 및 실현 가능성 등을 종합적으로 검토하고자 함

* (예) 한국과학기술젠더혁신센터(GISTeR)

** (예) 국가과학기술인력개발원(KIRD)

*** (예) K-DARPA 추진단

○ 조직 형태(안)별 장 · 단점 및 실현 가능성 등을 정리하면 다음과 같음

- **(1안: 독립 법인)** 예산 및 전문인력 확보가 가장 용이하나, 독립 법인 신설을 위해서는 행정안전부 및 기획재정부의 심의를 거쳐야 하므로 불확실성이 높고 시간과 노력이 많이 소요될 가능성 존재
- **(2안: 부설 기관)** 독립 법인 신설에 비해 기존 기관 내 부서를 부설기관으로 전환하는 것이 더욱 수월하고 예산 및 전문인력의 확보도 용이하다는 장점이 존재하나, 부설 기관 신설을 위해서는 행정안전부 및 기획재정부의 심의를 거쳐야 하기 때문에 불확실성이 높고 시간과 노력이 많이 소요될 가능성 존재
- **(3안: 기관 내 부서)** 기존 기관이 축적하고 있는 연구관리 전문성 및 국제 네트워크, 인력 등 유 · 무형의 자원 활용이 가능하다는 장점이 존재하나, 향후 기관 내 업무 재조정 등에 영향을 받아 조직의 영속성 및 예산의 안정성 등이 1,2안에 비해 낮을 수 있으며, 이는 법제화를 통해 개선 가능한 사항임

〈표 2-9〉 **조직 형태(안)별 특성 요약**

순번	조직 형태(안)	장점	단점	실현 가능성
1안	**독립 법인**	• 예산 및 전문인력 확보가 가장 용이	• 독립 법인 신설을 위해서는 **행안부 및 기재부의 심의**를 거쳐야 하기 때문에 불확실성이 높고 **시간과 노력이 많이 소요**	낮음
2안	**부설 기관**	• 독립 법인 신설에 비해 기존 기관 내 부서를 **부설기관으로 전환하는 것이 더욱 수월** • 예산 및 전문인력의 확보 용이	• 부설 기관 신설을 위해서는 **행안부 및 기재부의 심의**를 거쳐야 하기 때문에 불확실성이 높고 **시간과 노력이 많이 소요**	낮음
3안	**기관 내 부서**	• **기존 기관이 축적하고 있는** 연구관리 전문성 및 국제 네트워크, 인력 등 **유·무형 자원 활용 가능**	• 향후 기관 내 업무 재조정 등에 영향을 받아, **조직의 영속성 및 예산의 안정성 등 낮음** (법제화를 통해 개선 가능)	비교적 현실적

○ 조직 형태 관련 전문가자문단 및 연구보안 전문가 등을 대상으로 의견을 수렴하였으며, 주요 자문 의견은 다음과 같음

〈참고〉 **조직 형태 관련 전문가 자문 결과**

❶ **(형태)** 조직은 독립 법인보다는 **기존 기관의 부설 형태로 설립**하는 것이 조직에 힘을 실어줄 수 있음

❷ **(인식)** 초기부터 독립 법인 형태로 신설 시, **독립 기관의 필요성 및 국고지원의 당위성 등에서 광범위한 공감을 얻기 어려울 수 있음**

❸ **(전략)** 우선 기존 기관 내 **센터 단위의 워킹그룹을 만든 후 차후 구체적인 세팅** 필요
(예: 기관 내 부서로 출범 → 향후 부설 기관으로 확대)

❹ **(기타) 특정 부처 전문기관이 수행하는 것은** 타 부처 전문기관과의 충돌 가능성 등이 있으므로 **지양 필요**

○ 따라서, 고려 가능한 3개 형태(안)을 토대로 신설이 가능하지만 장·단점 및 실현 가능성 등을 종합적으로 고려 시 **기관 내 부서(3안)형태로 출범 후 향후 부설 기관(2안) 등으로 확대 전환**하는 방향으로 추진 가능

4 조직 구조 및 인력 고려사항(안)

○ **(조직 구조)** 조직 형태에 영향을 받는 점을 고려, **설립 초기**와 **중기 이후**를 구분하여 **시간에 따른 발전 방향을 제시**하는 것이 현실적

- 최초 공공기관 내 추진단 형태로 설립 시 10인 내외*의 단일 부서로 구성

  * 영업비밀보호센터와 대·중소기업·농어업협력재단 기술보호지원부의 경우 12~13인 규모로 운영 중인 것을 참고 가능

- 향후 부설기관으로 확대 시 30인 내외*의 다부서로 재편

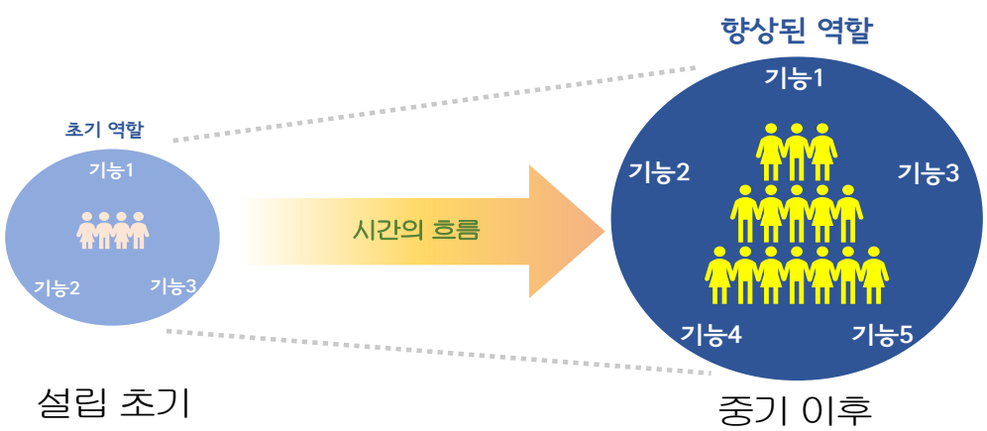
  * 한국산업기술보호협회의 경우 3실 9팀 구조로 되어 있으며, 30인 내외로 운영 중인 것을 참고 가능

○ 국내외 유사 사례들에서도 설립 초기 이후 기능이 추가되며 점점 조직 구조가 확장되는 모습을 볼 수 있음

- 참고 가능한 해외 사례로, 미국 RSI-ISAO의 경우 Dear Colleague Letter에 "시간에 따라 단계적으로 기능을 강화한다"라고 명시하고 있는데, 본 조직 역시 시간에 따라 기능과 규모 등 확장 고려 가능

- 유사 국내 사례로, 한국산업기술보호협회의 경우 설립 초기는 조직 구조가 비교적 단순하였으나*, 현재는 과거에 비해 더욱 복잡한 모습을 보임

  * 설립 초기 사업본부, 기술보호본부, 사무국, 산업기술보호연구소, 산업기술보호아카데미로 구성



[그림 2-4] **시간에 따른 조직 확장 개념도**

○ **(인력 구성)** 국가R&D에 대한 이해도가 높은 인력을 연구보안 주요 업무에 배치하고, 보안성이 조금 낮은 부분은 공모직으로 배치 가능

- 인력 구성의 경우, 향후 우선순위가 높은 기능들을 토대로 업무 담당 인력 및 필요한 전문인력 유형* 등 제시 필요

  * **(예)** 법률 전문가(변호사, 변리사), 빅데이터 전문가, R&D 정책기획 전문가, 교육/훈련 분야의 전문인력 등

〈표 2-10〉 **국내 산업보안 전담 집행조직의 조직 및 인력 구성**

조직	조직 구성	인력 구성
한국산업기술보호협회	3실 9팀	30인 내외
영업비밀보호센터	1센터 1팀	**12~13인** (변호사 포함)
대 · 중소기업 · 농어업협력재단 내 기술호보지원부	1부	**12~13인**

〈참고〉 **조직 구조 및 인력 관련 전문가 자문 결과**

❶ (조직구조) 초기 단일부서로 출범하되, 향후 다부서(3실 5팀)로 확장*
❷ (필요 인원수) 초기 10인 내외로 시작하되, 중기 이후 30명 내외로 구성
❸ (인력구성) 변리사 포함 전문인력 채용이 필수적이며, 데이터 · 보안 전문가, R&D 정책기획 전문가, 기술사업화/창업, 특허(IP, 지식재산), 교육/훈련 분야 전문인력 필요

5 법률적 고려사항(안)

❑ 조직 신설 형태별 법 개정 필수 여부

○ (1안: 독립 법인* 신설) 국가연구개발혁신법 개정이 필수적 선결 조건은 아님

* (예) 한국과학기술젠더혁신센터(GISTeR)

- (비영리법인) 민법 제32조*에 근거, 법인의 요건을 갖추고 동시에 부처의 인가를 받아야 함

* 비영리법인의 설립과 허가

※ 대부분 기관 설립 후 법률 개정을 통해 법적 근거를 추가하여 보완

○ (2안: 공공기관 산하 부설기관*) 상위 공공기관의 정관 개정(이사회 의결) 필요

* (예) 국가과학기술인력개발원(KIRD)

○ (3안: 공공기관 내 추진단*) 가장 현실성 있는 대안으로, 별도의 법 개정 불필요

* (예) K-DARPA 추진단

❑ 조직 신설 시 혁신법 시행령 개정 필수 여부

○ 혁신법 시행령 개정이 필수 선행요건은 아니나, 개정 시 안정적으로 연구 보안 업무를 수행할 수 있음.

- 조직 신설 이후에도 개정 가능하며, 개정시 연구보안 관련 내용을 명확하게 나열하고 해당 업무를 과기부가 연구보안 조직에 위탁한다고 명시하는 방향으로 개정 추진 가능
- 따라서 법 개정 등이 필수 선결조건은 아닌 바, 기관 설립 사후 법제화도 가능
- 그러나, 법제화 시 조직의 영속성 확보가 가능하다는 장점이 존재하여 안정적 업무 수행을 위해 관련 법령 개정 검토 필요

❑ 조직 예산 근거조항 필수 삽입 여부

○ 예산 근거 조항은 기관의 위상 및 부처의 예산에 대한 지원 의지일 뿐, 법조문에 예산 근거 조항이 없어서 예산을 기관에 못 주는 것은 아니므로 필수적 선결 요건이라고 볼 수는 없음

※ (예) 부처로부터 과제비를 매년 지원받는 식으로 별도의 출연금 없이 협회와 유사하게 운영 가능

- 그러나 예산 근거 조항 삽입 시 관련 기능을 보다 안정적으로 수행 가능하다는 장점이 존재하며, 반대로 예산 근거 조항이 없는 경우 기관운영비 등 예산 출처 변경이 가능하여 상대적으로 불안정성이 커질 수 있음

  ※ (사례1) 모 기관의 경우 출연 가능하다는 명확한 법적근거가 부재하여 기관운영비가 출연금에서 보조금으로 변경된 바 있음

- 따라서 예산의 안정성 확보에 따른 안정적 연구보안 집행 기능 수행을 위해 필요 시 관련 근거조항 마련 필요

6 전문가자문단 회의 운영

6-1. 전문가자문단 회의 운영 개요

❑ 목적

○ 연구보안 전담 집행조직 설계를 위한 사전 기획 단계에서 핵심 이슈들을 도출하고 조직의 역할과 기능, 구성 등에 대한 포괄적 논의를 통해 전반적인 기획방향 탐색 지원

❑ 구성 및 운영

○ (구성) 과학기술분야의 전문성과 조직신설 관련 특수성을 고려, 과학기술정책 전문가뿐만 아니라 조직설계 관련 행정학 전문가들로 구성

- 산학연 전문가 9인으로 구성

○ (운영) 각 회차별 안건에 따라 조직 신설 관련 핵심 내용들을 검토하고 관련 의견 수렴

- 총 2회 개최

6-2. 전문가자문단 회의 개최 실적 및 주요 내용*

* 본 내용은 전문가 의견을 요약 · 정리한 것으로 연구진의 견해가 아님을 밝힘

❑ 제1차 전문가자문단 회의

○ 회의 개요

- (일시) 2023.12.4.(월)/ 10:00~13:00
- (참석자) 전문가(8인), KISTEP(4인)

○ 논의 주제

- 연구보안 전담 집행조직 신규 설계방안 논의*

* 조직의 성격, 역할, 구성 등

○ 주요 토론 내용

- (기관 유형) 조직은 기존 기관의 부설 형태로 만드는 것이 힘을 실어줄 수 있음

> - 기존 조직 내 센터 단위의 워킹그룹을 만든 후 차후 구체적 세팅 필요
> - 연구보안의 경우 걸쳐있는 부처가 많아서 조직의 법적 위상에 따라 추진력이 달라짐
> ※ (대통령 직속 기관) 임명을 받아야 하며, 대통령의 정치적 견해와 합이 맞아야 함, (위원회) 위원회의 가장 큰 단점은 집행력이 없다는 것이므로 규제 목적의 경우 위원회 형태는 문제가 있음

- (인력 구성) 국가R&D에 대한 이해도가 높은 인력을 연구보안 주요 업무에 배치하고, 보안성이 조금 낮은 부분은 공모직으로 배치

> - 국가R&D 및 연구과제에 대한 이해도가 높고 기술력과 전문성을 갖춘 인력 구성이 필요하며, 인센티브에 대한 고민 필요

- (조직 성격) 조직의 성격은 근본적으로 규제기관이 될 것으로 보이나, 사람 중심의 보호 정책을 통해 연구현장 인식 제고 필요

- 대외적으로는 지원조직을 표방하나, 집행조직은 강제성을 내포한다고 생각됨
- 기관명이 '보호원'이면 규제기관이라는 본질과 의미적으로 상충되어 용어에 대한 고민 필요
- 현재 연구보안규정이 이미 있음에도 불구하고 해당 규정으로 해결하지 못하는 부분이 발생한다면 연구보안 정책강화는 충분히 타당성이 있음. 이를 설득시키기 위해 현재 연구보안 규정에서 허점이 있는지 설득할 수 있는 논리 필요
- 사람 중심의 보호정책이 필요하며* **, 과제관리 차원으로 접근 시 연구자 반감이 거셀 수 있음

* 해외 주요국 중 미국의 경우 사람이 유출하는 경우가 많으므로 사람 중심의 보호정책이 강함

** 민간기업 연구자산유출 최근 동향은, 실제 모 대기업의 사례와 같이 해외 전화컨설팅을 통해 회사 기밀이 유출되는 경우가 많음

- (용어 등 명확화 필요) 업무를 정의하기 전에 '연구자산' 및 '역할'에 대한 정확한 정의 필요

- 연구자산이란 무엇인지에 대한 조직의 입장 명확화 필요
- 역할은 무형자산의 보호인지? 아니면 과제관리인지? 명확한 방향성 설정 필요
- '이해상충' 이라는 용어가 과연 합당한지 고려 필요

- (업무량 사전 파악) 우선적으로 조직을 통해 처리해야 하는 업무량 파악 필요

- (산학연 중 대학 집중) 대학 컨트롤이 특히 중요

- 공공연구소 내 과제를 분류하고 결과물에 대해 보안정책을 적용하는 것은 가능성이 있어 보이나, 대학은 과기부 외에도 산자부 등 타부처 과제를 수행하는데 대학 교수님들의 혼란이 있을 것임
- 기업은 이미 스스로를 보호하려고 노력 중

- (기초원천 특수성 감안) 기초원천 등 TRL 앞단 과제들은 특히 분류기준과 관리대상 명확화 필요

- 산업부 과제를 수행하는 경우 기술이 유출되면 바로 처벌이기 때문에 오히려 깔끔하게 처리할 수 있는 반면, 비목적성 성격을 띠는 기초원천연구는 해외 및 국내 논문의 확산과 공유가 기본 업적인데 이에 대한 교통정리 필요

- (연구자 인센티브) 현재는 기관차원의 인센티브만 고려하는 것 같은데 연구자들 대상 인센티브 역시 중요

❑ 제2차 전문가자문단 회의

○ 회의 개요

- (일시) 2024.1.11.(목)/ 10:00~13:00
- (참석자) 전문가(8인), KISTEP(4인)

○ 논의 주제

- 연구보안 전담 집행조직 신규 설계방안 논의*

* 기존 회의 결과에 따른 집행조직 설계 심층 논의

○ 주요 토론 내용

- (관리의 효율화) 연구보안 전담조직은 총괄 모니터링을 수행하고, 개별 연구자의 경우 과제를 직접 수행하고 집행하는 기관별로 관리하는 것이 효율적
- (주요기능(안) 분류) 14가지 주요기능을 보면 상하관계로 이뤄진 것들이 있으므로 4~5가지의 카테고리로 분류하고 하위에 세부기능을 추가

> - 분류의 방법으로 전문기관·연구기관의 연구과제 파악, 이에 대한 정책연구, 가이드라인 도출 등 '인풋' 설정, 보안 관리에 관한 교육 및 홍보 등 '프로세스'로 설정, 보안대책 운영 시 발생하는 문제 및 이에 대한 대책연구를 '아웃풋'으로 설정하여 분류
> - 연구보안 집행조직의 주요 기능 정의 및 구체화 필요
>
> ※ ❶ 전문기관·연구기관 협조·관리 : 참여과제별(보안·민감과제) 연구원 관리 등 관리 대상 범위
> ❷ 핵심인력 상담·보고·지원 : 해외에서 컨택이 있을만한 국내 R&D핵심인력(은퇴연구자 등)에 대한 지원 및 사전 스크리닝

- (데이터보안 기능 추가) 컴퓨터, 시스템, 인프라 등을 다루는 사이버 보안에 데이터를 추가하여 '데이터 보안 관리'라는 기능 추가 필요
- (전담조직 명칭) 최근 조직이름 트랜드는 관리라는 이름을 지양하므로 지원, 협력 등을 활용하여 다양한 각도의 조직명 고민 필요

> - 산업기술·보안 쪽에 문제 발생 시 심각한 상황으로 될 수 있으므로, 이를 사전에 예방하자는 취지로 접근
> - 직접 관리가 아닌 연구보안 대책 수립에 대한 방향성 안내 및 지원으로 불필요한 마찰, 경제적 피해를 사전에 예방하겠다는 방향

- (전담조직 성격 명확화) 연구보안에 대한 '지원'을 주력으로 하는 조직으로 조직의 성격 명확화 필요

- 정책, 교육, 홍보에 중점 필요
- 연구보안 전담조직은 국가차원에서 진행되는 부분이며 국가차원 관리를 지원하는 기관임을 설립목적을 통해 조직 성격을 명시
- 연구기관 보안 행동에 대한 상한선을 정해주고 교육, 가이드라인 검토 등의 기능을 수행하면 지원적 성격과 규제적 성격을 동시에 가질 수 있음

- (연구현장 수요조사) 전담조직에 대한 수용성을 위한 연구현장의 수요조사 필요

- 조직 필요성, 조직의 주요 기능에 대한 의견 수렴
- 국정원, 검찰과 같은 처벌적 성격이 아닌 연구현장 및 연구자 지원 조직임을 강조
- 특히 최근 AI등장으로 인한 새로운 유출 문제가 대두되고 있기 때문에 연구보안 부재 시 발생할 수 있는 새로운 문제를 안내함으로써 연구보안 중요성 및 조직 설립의 근거 보완

- (연구보안 정의) 산업부와 차별성을 가지는 명확한 연구보안 정의 필요
- (주체별 안내 필요) 국가, 기관, 연구자 세 주체의 입장으로 연구보안 전담기관 부재 시의 문제점 및 보안대책 및 행동 등에 대한 개략적인 가이드 우선 설명 필요

- 연구현장 및 전문가를 통한 조직 설립의 수요는 분명 존재하나 관리, 통제기관으로 오해할 수 있기 때문

- (정책성격 변질 주의) 추후 키 퍼포먼스를 제출하는 등의 보여주기식 정책으로의 변질을 주의하기 위해 연구보안 및 전담조직 설립 목적 명확화 필요

제5절 소결

❑ 결론

○ 연구보안 지원 역할을 중심으로 설정하되, 설립 목적 및 세부 기능 등 조정 필요

- 관리보다는 지원에 초점을 맞춰 ①정책, ②교육, ③홍보, ④가이드라인 개발 등을 중심으로 구성하되, 조직이 필수로 수행해야 할 기능을 1~2개 정도 추가하는 방향으로 추진 가능
- 연구현장 수용성 제고 측면에서도 관리보다는 지원에 초점을 맞추는 것이 유리하며, 관리 측면이 부각될 경우 연구현장의 수용도가 낮아질 수 있음
- 미국 NSF OCRSSP의 기능이 ①정책연구 및 모니터링, ②데이터 분석, ③가이드라인 개발 등 관리보다는 지원 중심으로 구성된 것을 참고 가능하며, 국내 산업보안 유사조직 사례 중 한국산업기술보호협회 역시 설립 초창기 지원 역할에 초점을 맞춘 사례가 존재하여, 이를 참고 가능

○ 현 시점에서 추진단 등 기관 내 부서(10인 내외)로 출범하는 것이 가장 현실적이며, 향후 확장을 통해 30인 내외의 다부서로 재편 가능

- 미국 RSI-ISAO가 “시간에 따라 단계적으로 기능을 강화한다”고 명시한 사례를 벤치마킹 가능
- 국내 산업보안 유사조직의 경우 소규모 조직은 12~13인, 중규모 조직은 약 30인 규모를 유지 중인 것을 참고 가능
- 기존 조직 내 부서 형태로 출범할 경우, 해당 조직이 지니는 인적·물적 자원 및 네트워크 등을 설립 초기에 승계 및 활용할 수 있다는 장점을 지님

○ 조직 신설 관련, 법률 개정이 필수적 선결요건은 아니나, 조직의 영속성 및 예산 안정성 확보 차원에서 유리하므로 법제화 추진 고려 필요

- 민법 제32조에 따라 법인의 요건을 갖추고 동시에 부처의 인가를 받으면 조직 설립이 가능하여, 법리적으로는 조직 설립 후 법제화도 가능
- 조직을 급박히 신설해야 할 경우 신설 후 사후적으로 법적 근거를 추가하여 보완하는 순서로 진행 가능
- 하지만 이는 조직 신설을 위한 최소 요건일 뿐이며, 실제로 사전 법제화가 미비하여 예산 근거조항이 약한 타 기관들의 경우 관련 조문의 법제화를 적극 추진 중인 것을 감안할 때 선제적 법제화 작업을 통해 조직 안정성 확보 가능

❑ 시사점

- 향후 기획 구체화 작업을 통해 ①조직 형태, ②설립 목적 및 명칭(안), ③역할 및 기능, ④조직 구조 및 인력 등 구체화된 기획(안) 도출 추진 필요
  - 현장자문위원회뿐만 아니라 별도의 조직 신설 관련 전문가자문단 운영 등을 통해 관련 전문가들의 자문 의견을 지속적으로 반영 필요
- 법제화 추진 시 조직 및 예산 안정성 확보가 가능하므로, 향후 법률전문가 자문을 통해 관련법 개정(안) 도출 및 검토 추진 필요
  - 법제 실무 경험이 풍부한 과학기술법률 전문가들의 자문 내용을 바탕으로 개정(안) 초안을 도출하고, 변호사를 통해 법리적 타당성 등을 교차 검증 추진 필요
- 연구보안 전담조직 부재 시 예상되는 국가·연구기관·연구자 수준의 문제 및 전담조직의 기대효과 등을 토대로 조직 신설 논리를 개발하여 향후 연구 현장 설득 및 인식 제고에 활용 가능

제3장 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출

제1절 서론

1 연구배경 및 필요성

❑ 연구보안 정책 내실화*에 따른 현장의 연구보안 정책 이해 제고 및 제도안착을 위한 연구보안 현장지침 필요성 대두

* 근거: 연구보안체계 내실화 방안('23.9.26, 국가자문위)은 '연구기관 및 연구자'를 대상으로 한 가이드라인 마련을 정책방향 중 하나로 제시

○ 연구보안체계 내실화방안에 따라 '연구보안'이 전통적 보안영역* 뿐 아니라 '과제관리', '연구진실성' 등의 개념과 결부되어 확장되고 '국가R&D 수행기관' 단위 보안관리 책임성 강화 등의 변화가 존재

* 시설, 정보통신망, 인력, 성과물에 대한 보안대책 및 관리조치

○ 이와 같은 정책 변화를 국가R&D 연구자·연구기관 등을 대상으로 안내하므로 연구보안 인식 제고와 제도안착을 촉진하고 최종적으로 연구자산 유출 방지를 지원해야 할 시점

- (기관) 연구보안의 1차 관리 책임을 맡아 기관 자원을 활용하여 내실화 방안 이행 등 연구현장이 관련 법·제도를 준수*할 수 있도록 유도

* (예) 혁신법 및 관계 규정과 연구보안 현장지침을 기관 내규에 반영하고 이행

- (연구자) 국가R&D 수행 시 준수해야 하는 연구보안 원칙 주의사항을 '현장지침' 매뉴얼 등에서 참조하여 연구윤리에 입각한 보안관리 추진

❑ **'연구보안 체계 내실화 방안'을 현장에 적용할 시, 다양한 이해관계자의 입장 및 협력 환경, 관련 법과의 관계 등을 종합적으로 고려하여 현장에서 즉각 활용할 수 있는 실질적인 안내서 마련 필요**

○ 국가연구개발사업에 참여하는 산·학·연 특성에 따라 연구보안 정책 적용의 주안점이 달라지기도 하고, 때로는 각 주체가 상호 협력을 통해 연구를 진행하는 등 연구 환경의 다양성이 존재하는 상황을 반영한 지침 마련

○ 연구보안 외에도 국가연구개발사업과 연관된 보안 법제와 규정, 매뉴얼이 산재한 실정이므로 이와 같은 상황을 고려한 체계적 안내서 방향 설정 검토

- 연구현장 담당자는 여러 가지 법을 숙지하고 적용해야 하므로 실무에 어려움이 있을 수 있음
- 비록 연구보안 현장지침에서 '산업보안'을 포괄해서 안내할 필요는 없으나 지침 간 상충이 없도록 하고 공통적인 부분에 대해서는 유사성을 지니도록 '현장지침' 작성하는 방향성에 대해서 고려 가능

〈표 3-1〉 **과학기술 보호를 위한 관련 법규정 예시**

구분	예시
연구보안 관련법	혁신법 및 시행령, 보안대책(고시), 국가전략기술법
산업보안 관련법	산업기술보호법, 첨단전략산업법, 부정경쟁방지법, 중소기업기술보호법, 방위산업기술보호법
그 외 관련법	정보통신망법, 정보통신기반법, 사이버안보 업무규정

❑ **최근 국제공동연구가 확대되는 정책 기조에 따라 연구교류라는 '개방성'을 유지하면서도 '연구자산 유출'을 방지할 수 있는 균형감각과 실리적 접근의 지침 마련 요구**

○ 혁신법제2조는 해외 연구개발기관을 주관·공동연구개발기관으로 인정할 수 있도록 법개정(24.2.6)을 추진하였으며 이에 따라 해외 연구개발기관의 성과소유가 가능해지는 등의 변화 발생

○ 이에 발맞춰 과학기술정보통신부는 국제공동연구개발사업매뉴얼(24.2)을 발간하며 국제공동연구 시 지켜야 할 '보안정책' 등에 대해 안내하고 있으며 해당 내용을 '연구보안 현장 매뉴얼'에서도 반영 필요

❑ **기술패권 경쟁이 가속화됨에 따라 주요국들은 자국 연구개발기관과 연구자로부터의 연구자산 유출을 방지하기 위하여 현장에서 지켜야 할 필드 매뉴얼을 발행하고 있음**

○ 미국이 대중국 정책 기조를 '경쟁적 공존관계'로 변환하고 바이든 정부가 '기술경쟁'을 대중국 견제 수단으로 선택함에 따라 연구보안 정책 강화가 가속화 추세이며 이는 연구자, 연구기관에도 영향[2)]

※ (대중국정책기조) 구조적 참여정책(Constructive Engagement)⇒경쟁적 공존정책(Competitive Coexistence)

2) 민정훈 (2023). 미국 118대 연방의회의 정치적 특징 및 전망분석, IFANS 주요국제문제분석 2023-4. 국립외교안보연구원

- 미국 NSTC는 NSPM-33 법에 기반하여 '대학 및 연구개발 기관'을 대상으로 한 권고안을 발행하며 '외국인 연구자, 성과계약, 데이터 관리' 뿐 아니라 조직 차원에서 보안에 대응하기 위한 목표 등을 제시[3)]
- NSF의 과학자 자문 그룹인 JASON에서도 국제협력 시 '위험성'을 진단하기 위한 체크리스트를 제시하므로 연구현장이 개방성을 높이면서도 위험성을 저감할 수 있는 진단 도구를 지원

○ 영국은 연구현장 관련자들이 국제 협력 추진 시 원활하게 협업하면서도 자산을 보호할 것을 당부하고 있으며 구체적으로 '학계 및 산업계'를 대상으로 '협력 파트너'를 구별 할 수 있는 '방침'을 제시함

○ 일본 문부과학성은 국제화와 연구개방성 확대에 '대학 및 공공연구기관'이 적절히 대응할 수 있도록 '조직의 상담 및 교육 체계, 정보화 교육' 등과 관련된 체크리스트를 연구현장에 배포하고 제시하였음(2023)

제2절 연구보안 관련 법·정책 분석 사항

1 연구보안 체계 내실화 방안에 따른 현장지침 적용 사항

□ '연구보안 체계 내실화방안'은 국가R&D 단계별 '연구기관 및 연구자'의 '연구자산 보호, 이해상충 방지 등'의 위험관리를 지원하고자 하는 취지에서 다양한 정책방향을 제시하였으며 주요 신규 정책 적용 사항은 아래 사항과 같음

□ 보안과제와 일반과제의 중간 보안등급으로 '민감과제'를 신설하여 기존에 국방기술 위주로만 관리되는 '보안과제' 외에도 '경제안보' 등의 분야도 관리할 수 있도록 하되 민감과제는 보안과제보다 완화된 보안조치 적용하는 방향 설정

〈표 3-2〉 **보안등급 정의(안)**

일반과제	민감과제	보안과제
보안 또는 민감과제로 분류되지 않은 과제	유출 시 기술적·재산적 가치의 상당한 손실이 예상되어 국민경제에 영향을 미칠 수 있는 과제	국가안보와 관련되거나, 국민경제에 중대한 영향을 미칠 수 있는 과제

3) NSTC (2019). 'Recommended Practices for strengthening and security and integrity of America's science and technology research enterprise

❑ 과제수행 전 단계에서 연구자의 ‘국외수혜정보보고’, ‘외국인 참여연구원 관리 강화’ , ‘보안과제 및 전략기술과제 수행 연구자’ 등 ‘인력관리’에 대한 관점이 강화됨

- 국외수혜정보는 외국기관 및 외국이 실질적으로 지배하는 국내기관으로부터 금전적, 비금전적 지원을 받거나 받을 예정인 연구책임자가 ‘연구계획서’ 작성 당시 및 IRIS 연구자정보시스템(NRI)을 통해 신고함
- 보안과제는 외국인 참여 시 보고체계를 강화하여 현행 부처·국정원 사후통보를 사전보고 체계로 개선
- 실질적으로 외국정부 등의 지배를 받는 연구기관의 참여를 제한
- 특정 분야(예 원자력, 우주) 및 핵심 전략기술 관련 유학·취업비자 심사 강화 등 검토
- 보안과제 수행자, 국가전략기술 전문가 등의 국가연구자번호를 식별하여 해당 연구자 대상 교육 및 보고·상담 체계화

❑ 보안·민감과제 중 보안이 필요한 부분 외에는 성과활용을 촉진할 수 있도록 성과 부분공개 제도를 신설하여 성과보호와 동시에 활용도 지원하는 등 연구개발성과 관련 정책의 유연성 확보

❑ ‘보안대책 고시’에 따라 연구기관의 보안대책 포함 필요사항은 ‘참여연구원, 연구성과 및 정보 관리, 정보통신망, 연구시설’ 및 ‘보안관리 체계’ 전반으로 해당 사항은 향후 상향입법 되어 전 부처가 따를 수 있도록 조치될 예정임

※ 과기정통부 · 농림축산식품부 · 환경부 · 경찰청 · 농촌진흥청 · 산림청 · 기상청 · 교육부 · 문화재청 등 9개 부처 공동 고시(2023.11.20. 개정, 2022.11.20. 시행)

- 기존의 보안과제, 비공개성과 중심의 보안체계는 국가R&D를 수행하는 기관이 보안체계를 정립하는 방향으로 추진될 예정임
- 일반과제 및 보안과제 중간의 민감과제 등급이 신설되고 민감과제의 경우 보안과제보다 완화된 보안조치를 적용하게 되므로 이에 따라 연구기관이 지켜야 보안조치는 과제별로 달라질 수 있게됨

〈표 3-3〉 **보안등급 별 보안조치 사항**

구분	보안과제	민감과제	일반과제
❶참여 연구원 보안관리	- 수행자 외국인·기관 접촉 시 사전승인(과제종료3년이내) - 해외출장 전 부처가 자료 보안성 검토	- 수행자 외국인·기관 접촉 시 사후보고(과제종료1년이내) - 해외출장 전 연구기관 자체적으로 자료 보안성 검토	-
❷성과물·기술이전	- 원칙적으로 불가, 해외 이전 시 부처 사전승인	- 해외 이전 시 부처 사전보고	-
❸정보통신망 관리	- 미허가 외부메일, 메신저 등 사용제한	-	-
❹연구시설 보안관리	- 연구실보호구역 지정 및 출입권한 차등화	- 연구실보호구역 지정 및 출입권한 차등화	-
❺실태점검	- 부처·전담조직에서 전수조사	- 부처·전담조직에서 표본조사, 자체점검결과 보고	- 연구기관 자체점검 ※ 필요시 부처·전담조직 점검

❑ '연구자 및 연구기관' 대상 인센티브 또한 확대될 예정이며 이와 관련한 홍보, 제도개선 등이 이뤄지며 연구보안 인식제고에 기여할 것으로 보임

○ 연구자 대상 보안수당 확대가 검토되고 정부표창 신설 등이 추진될 예정

○ 연구기관의 경우 연구지원체계평가 등을 활용하여 '연구보안 관리비 의무사항, 간접비 비율조정' 등을 검토

2 국가연구개발혁신법 상 연구보안 관련사항 분석

❑ (개요) 현행 혁신법 및 하위법령 상 연구보안은 '연구개발 전주기' 상 중요한 연구개발성과 정보가 유출되는 것을 예방하기 위하여 주요 절차를 정립하는 것이라고 볼 수 있음

○ 보호대상 및 보호를 위한 지침을 제시하고 관련 대책을 위반하거나 정보를 누설하였을 시 제재조치를 가하므로 국가연구개발사업의 관련 보안 체계를 구축하는 것이 주요 목적

- 보호대상은 '산업기술유출방지법'에 따른 비공개 연구개발성과, 보안과제로 분류된 연구개발과제의 연구개발성과를 지칭함

〈표 3-4〉 **국가연구개발사업 혁신법 및 하위법령 상 연구보안의 개념 요약**

구분	주요 내용
범위	• 국가연구개발사업 대상 – 보안대책은 고시이므로 중앙행정기관장의 지침에 따라 갈음 가능
보호대상	• 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 보안이 필요한 연구개발과제 관련 중요한 정보 – 중요한 정보(연구개발성과, 연구개발정보, 데이터 등)
보호행위	• 중앙행정기관 중심으로 연구개발 과제에 대한 보안 등급 분류 • 각 연구개발기관이 연구개발과제, 연구원, 시설, 정보통신망을 관리하므로 보안대책을 준수하고 주요 자산의 유출을 방지
부정행위	• 연구보안 대책 위반 • 보안과제로 분류된 연구개발과제의 보안사항 누설, 유출 행위
보안주체	• (중앙행정기관) 보안과제 분류 등 연구개발사업 전주기 상 관리 • (연구개발기관) 보안담당자 및 보안관리 규정 담당자를 지정 • (연구자) 연구윤리 준수를 통한 연구로 연구자산 보호
제재조치	• (연구자 및 연구개발기관) 2~5년 이내 연구개발과제 참여제한 • (연구개발기관) 연구개발과제 전액~100분의 250의 제재부과금 부과 • (연구자 외) 연구개발과제 20~50%의 제재부과금 부과

❑ (법구조) 혁신법 상 연구보안에 대한 관련 내용은 '연구개발 전주기 추진 절차 상 연구보안, 보안대책 수립, 부정행위 및 제재처분 등으로 나누어 이해할 수 있음 4)

※ 보안대책, 과제분류, 보안사고 보고 등의 중요한 보안 행위가 고시로 규정되어 있는 한계점은 존재

〈표 3-5〉 **혁신법 상 연구보안 법령 구조**

구분		법	시행령	관련 고시
연구개발과제 추진 절차 상 보안 관련 사항		법제9조~제17조	영제9조~영제34조	
보안과제 분류		법제21조	영제45조	
보안대책 수립/관리	**보안대책 수립**	법제21조	영제44조	국가연구개발사업 보안대책
	보안관리 조치		영제46조	
	실태점검/보안사고		영제47-영제48	
보안 업무 추진 시 관련 비용		–	–	연구개발비 사용기준 (보안수당 사용용도)
부정행위 및 제재 처분		법제31조~33조	영제56조-영제59조	–

4) 국가연구개발혁신법, 보안대책, 혁신법매뉴얼(2023) 내용을 참고하여 재구성

○ 국가연구개발사업 추진 절차 상 연구보안(혁신법제9조~제17조)

- 연구개발과제의 사전기획, 수행기관 선정, 과제평가, 공개 등 보안과제를 전반적으로 관리하기 위한 원칙을 제시하고 있음

〈표 3-6〉 **국가연구개발사업 추진 절차 상 연구보안 관련 내용(혁신법)**

구분	관련 법령 및 내용
예고 및 공모 등 (법제9조4항)	• (수요조사) 국가안보, 국방 등에 대해서는 수요조사의 결과를 반영하지 않을 수 있음 (제9조제2항)
	• (사전기획) 사전기획 시 보안과제 해당 여부 검토(영제8조제2항)
	• (공모 외) 공모를 통해 연구개발기관을 선정하거나 다만 '국가안보 또는 사회경제에 중대한 영향을 미치는 연구개발과제' 등은 공모 외 방법으로 선정(법제9조4항)
	• (공모) 연구개발기관 및 기관을 공모를 통하여 선정할 경우, 보안과제로 분류되었는지 여부 등을 포함시켜야 함(해당 사항공고가 곤란할 경우 제외)(영제9조1항1호라목)
연구개발과제 및 수행연구개발 기관 선정(법제10조)	• (사전검토) 보안사안 위반 등 부정행위가 있는 지 등을 검토하여 참여제한 대상여부를 사전에 검토해야 함 • (선정평가) 보안사안 위반 등 부정행위 존재 시 선정평가를 불리하게 할 수 있음(영제12조5항)
협약 (시행규칙 별지2호 예시)	• (중앙행정기관장 권한/의무) 국가연구개발사업 정보에 대한 보안조치 • (연구개발기관 권리/의무) 연구개발과제 보안관리, 협약체결 이후부터 보안담당자를 지정하고 보안관리 규정을 마련 및 운영
연구개발과제의 수행 및 관리 (법제12조제2항)	• (평가) 보안과제로 분류된 과제는 단계 및 최종평가를 실시하지 않을 수 있음(영제16조제3항1호)
연구개발과제의 평가 등 (법제14조제3항)	• (평가단) 보안과제의 경우 평가단을 구성하지 아니하거나 평가단 구성 시 법제9조2항의 사항을 적용하지 않아도 됨
연구개발성과의 활용 (법제17조제2항)	• (공개) 보안과제로 분류된 경우 최종보고서, 연구개발성과 정보의 비공개를 신청할 수 있음(최대 3년 후 연장 신청)(영제35조제2항제3호)

○ 중앙행정기관의 장은 연구개발과제에 대한 보안과제 분류(혁신법제21조)를 추진할 수 있으며 그 시기와 절차 등은 아래와 같음

- (분류대상) 중앙행정기관의 장은 시행령 제45조제1항에 해당하는 연구개발과제를 보안과제로 분류할 수 있으며, 그 외에는 일반과제에 해당함

보안과제로 분류할 수 있는 과제(시행령 제45조제1항)

1.「방위사업법」 제3조제1호에 따른 방위력개선사업과 관련된 연구개발과제
2. 다음 각 목의 어느 하나에 해당하는 기술과 관련된 연구개발과제
 가. 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술
 나. 중앙행정기관의 장이 보호의 필요성이 있다고 인정하는 미래핵심기술
 다.「산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호에 따른 국가핵심기술
 라.「대외무역법」 제19조제1항에 따른 수출허가 등 제한이 필요한 기술
3. 그 밖에 중앙행정기관의 장이 보안과제로 분류할 필요가 있다고 인정하는 연구개발과제

- (분류시기) 중앙행정기관의 장은 시행령 제45조제1항에 해당하는 연구개발과제를 공모 전까지 보안과제로 분류하여야 하나 다만 아래와 같은 예외 사항에 대해서도 인정하고 있음

1. 법 제9조제4항 단서에 따라 지정 등 공모 외의 방법으로 연구개발기관을 선정한 경우
2. 보안과제로 분류되었는지를 제9조제1항에 따른 공고에 포함시키는 것이 곤란한 경우

- (재분류)「국가연구개발사업 보안대책」을 적용받는 경우 과제 수행 중 또는 연구개발결과에 따라 보안과제/일반과제로의 재분류 가능

※ 연구개발기관의 장은 수행 예정이거나 수행하고 있는 보안과제가 재분류가 필요하다고 판단되는 경우 또는 일반과제를 보안과제로 분류해야 한다고 판단되는 경우에 보안과제분류위원회에 보안과제 분류를 요청할 수 있음

※「국가연구개발사업 보안대책」을 적용하는 중앙행정기관의 장은 연구개발결과에 따라 보안과제가 달라질 수 있는 경우 최종평가 시 “연구개발과제평가단으로 하여금” 연구개발 결과를 고려한 보안과제 분류의 적절성을 검토하게 할 수 있음

- (분류절차)「국가연구개발사업 보안대책」을 적용하는 중앙행정기관의 장은 소관 연구개발과제를 보안과제로 지정·해제하는 등 분류가 필요할 때에는 검토를 위하여 해당 연구개발 분야 및 보안업무 전문가 등으로 구성된 보안과제분류위원회를 설치하여 운영하여야 함

※ 단, ①연구개발과제 발굴을 위한 사전 기획을 통해 보안과제로 분류될 수 있는 경우 ②자유공모 과제에 대하여 연구개발과제평가단을 통해 보안과제로 분류될 수 있는 경우 ③다른 법령에 의한 절차를 통해 보안과제로 분류될 수 있는 경우*, 보안과제분류위원회의 검토를 생략함

※ 혁신법 시행령 제45조 제1항제2호 다목 해당여부는 보안과제 분류위원회의 검토 없이「산업기술의 유출방지 및 보호에 관한 법률 시행령」 제13조의2에 따른 국가핵심기술 해당여부에 대한 의사결정으로 판단 가능

〈표 3-7〉 **국가연구개발과제 추진 시기 별 보안과제 분류 절차**

시기		보안과제 분류 절차
사전기획~공모 전 (영제8조2항 및 영제45조제2항)		(중앙행정기관의 장) 기획단계에서 보안과제 해당여부를 검토하고(영제8조2항) 공모 전 보안과제 여부를 결정하는 것이 원칙(영제45조제2항)
연구개발기관 선정	공모 (법제9조4항)	(중앙행정기관의 장) 보안과제 분류 여부를 공고에 포함 (영제9조1항제1호)
		(중앙행정기관의 장) 보안과제로 분류되었는지 여부를 공고하는 것이 곤란한 경우 연구개발기관 선정 후 보안과제 분류 (영제45조제2항제1호)
	지정 등 공모 외 방법 (법제9조4항)	(중앙행정기관의 장) 연구개발기관 선정 후 보안과제 분류 (영제45조제2항제2호)
연구개발과제 수행예정 또는 수행 중		(연구개발기관의 장) 수행 예정 또는 수행 중에도 보안과제분류위원회에 보안과제 여부 재분류 요청(보안대책제3조 제2항 및 제3항)* ※ 보안→일반, 일반→보안
연구개발과제 종료		(중앙행정기관의 장) 연구개발결과에 따라 보안과제 분류의 적절성 재검토 가능(보안대책제14조)*

* 국가연구개발사업 보안대책을 적용하는 경우에 해당 사항

○ (보안대책 수립·시행) 관계 중앙행정기관의 장 및 연구개발기관의 장은 소관 국가연구개발사업 및 연구개발과제와 관련하여 연구개발성과 등 대통령령으로 정하는 중요 정보가 유출되지 아니하도록 보안대책을 수립 · 시행하여야 함(법제21조 및 보안대책)

- 국가연구개발혁신법 제21조제1항 및 동법 시행령 제44조에 따라 중요한 정보가 유출되지 않도록 과학기술정보통신부 등 9개 부처는 「국가연구개발사업 보안대책」 제정*을 통해 중앙행정기관이 수립하는 소관 연구개발사업 및 연구개발과제에 관련한 보안대책을 수립

  * 과기정통부 · 농림축산식품부 · 환경부 · 경찰청 · 농촌진흥청 · 산림청 · 기상청 · 교육부 · 문화재청 등 9개 부처 공동 고시(2023.11.20. 개정, 2022.11.20. 시행)

※ 다만, 중앙행정기관의 장이 해당 국가연구개발사업에 대하여 그 특성에 따라 별도의 보안 규정을 마련 시, 보안대책에 앞서 해당 지침을 우선 적용 가능

- 「국가연구개발사업 보안대책」을 적용하는 중앙행정기관의 국가연구개발사업을 수행하는 연구개발기관장은 보안대책 수립 시 동 규정 별표에 따른 사항을 포함하여 정하여야 함

※ 공동연구개발기관이 자체 보안대책을 마련하기 어렵거나, 주관연구개발기관과 통일성 있는 보안대책이 필요한 경우 주관연구개발기관의 보안대책을 따를 수 있음

〈표 3-8〉 **연구개발기관 자체 보안대책에 포함 필요한 사항(국가연구개발사업 보안대책 제4조)**

구분	보안대책 상세내용
1. 보안관리 체계	• 연구보안심의회의 구성 · 운영 방법, 심의 내용 등에 관한 사항 • 제16조 비공개연구성과에 보안대책 (보안대책 적용의 범위) • 연구개발기관 내 보안관리 업무의 종합계획 · 관리를 담당하는 보안대책 총괄담당자 지정, 보안대책 총괄담당자의 업무 등에 관한 사항 • 보안 우수자 및 보안 관련 규정 위반자에 대한 상벌 기준 • 영 제48조에 따른 보안사고 발생 시 대응 · 조치 절차 • 소속 직원의 보안교육 이수 의무에 관한 사항
2. 보안과제 참여 연구자관리	• 참여연구자의 연구기관보안대책 위반 시 징계에 관한 사항 • 퇴직하였거나 퇴직 예정인 자가 반출 또는 반출 예정인 자료에 대한 보안성 검토, 회수, 전산망 접속 차단 등의 조치에 관한 사항 • 참여연구자의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시 • 보안과제를 수행하거나 수행한 적이 있는 연구자의 외국 정부·기관·단체 접촉시 보고 및 외국 정부·기관·단체와의 연구 승인 등에 관련된 절차 및 형식 등 제반사항
3. 연구개발내용 및 연구개발성과의 보고	• 보안등급 표기가 필요한 문서 및 데이터의 종류 • 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차
4. 연구시설 관리	• 보안과제 수행에 사용된 노트북, 외장형 하드디스크 드라이브 등 정보통신매체에 대한 출입 절차 • 연구개발기관 외곽, 주요 시설물에 폐쇄회로 텔레비전, 침입감지센터 등 장비 등의 설치 · 운용 • 연구개발과제와 관련된 핵심기술 및 정보를 보관하는 전산실 및 중요시설물에 대한 보안관리 조치 • 연구실 및 연구개발기관에 대한 출입권한 차등화의 방법 · 기준, 출입현황 관리 방법 등에 관한 사항 • 외부인 및 외부입주기관(벤처기업 포함)의 보안과제 관련 연구시설의 내부 출입통제 조치에 관련된 사항 • 화재, 홍수, 재난, 재해 등 비상시 대응계획 수립에 관련된 사항
5. 정보통신망 관리	• 보안사고 발생을 예방하기 위한 다음 사항을 포함하는 일반적인 정보통신망 관리 조치 • 보안과제에 대한 다음 사항을 포함하는 강화된 정보통신망 관리 조치

❑ (보안관리) 보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 보안교육 실시, 보안책임자 지정 등의 보안관리 조치를 하여야 함

〈표 3-9〉 **보안과제 수행 연구개발기관의 보안관리 조치**

① 보안과제를 수행하는 연구실에 대한 보호구역 설정 ② 보안과제를 수행하는 연구자의 연구실 출입권한 차등 부여 및 출입 현황 관리 ③ 보안과제를 수행하는 연구자에 대한 보안교육 실시 및 보안서약서 제출 요청 ④ 보안과제를 수행하는 외국인 연구자의 연구 수행에 대한 연구개발기관의 장의 승인 및 중앙행정기관의 장에 대한 보고 ⑤ 연구개발기관이 운영하는 연구관리시스템에 대한 보안관리 조치 ⑥ 연구개발정보 처리 과정 및 그 결과에 대한 보안관리 조치 ⑦ 보안책임자 지정

○ 「국가연구개발사업 보안대책」을 적용하는 연구개발기관의 장은 해당 고시에 따라 보안과제와 관련된 '연구자, 다양한 형식의 자료·문서, 연구개발성과 활용' 등을 관리해야 하며 연구개발기관 내 연구보안심의위원회를 두어 보안관리 조치와 보안대책을 심의해야 함

- (보안교육 및 보안서약) 보안과제를 수행할 예정이거나 수행하고 있는 연구자를 대상으로 교육을 실시하고 보안서약서*를 제출받아야 함

  * 보안서약서 (국가연구개발사업 보안대책 제7조제2항 및 제3항 [별지 제1호 서식])

- (외국 정부 등과의 접촉 관리 등) 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국 소재 '정부·기관·단체' 외국인과 접촉 하거나 관련 지원을 받는 경우 등 관리

※ 보안과제 참여 연구자의 외국 정부 등과의 접촉사항, 외국인 연구자의 보안과제 참여사항 등은 발생 후 1개월 이내 국가정보원장에게 통보

〈표 3-10〉 **보안과제 수행 연구자(3년 지나지 않은 연구자 포함)의 외국 정부 등 접촉 시 조치**

상황	연구개발기관의 보안관리 조치(보안대책 제8조)
보안과제 관련 외국 정부 등과 접촉(연구자 상호작용 및 반복 접촉)	• 보안과제 수행 연구자가 보안과제 관련하여 외국 정부 등(정부·기관·단체·외국인)과 상호작용 하거나 유의미한 정도로 접촉을 반복하는 경우, 접촉일로부터 10일 이내 접촉·일시·장소·방법·내용을 연구개발기관의 장에게 보고 • 연구자 퇴직 또는 혁신법제2조제3호에 따른 연구개발 기관이 아닌 곳으로 이직할 시 마지막 소속 연구개발기관 장 보고
보안과제 관련 연구자 대상 외국정부 등의 지원	• 보안과제 수행 연구자의 해외 수혜 통한 연구개발 추진에 대해 연구개발기관 장은 연구보안심의위원회를 통해 사전 승인 필요

- (외국 연구자 등의 보안과제 참여) 원칙적으로 보안과제의 외국인 참여는 내국인을 통한 보안과제 달성이 어려울 경우에만 연구보안심의위원회의 심의를 거쳐 가능

〈표 3-11〉 **외국인 연구자 보안과제 참여 및 보안과제 국제 공동 연구 시 보안관리 조치 사항**

상황	연구개발기관의 보안관리 조치(보안대책 제9조)
외국인 연구자의 보안과제 참여	• 연구개발기관 내 보안심의위원회에서 외국에의 기술 유출 가능성 등을 종합적으로 검토
외국·정부·기관단체 등 보안과제 참여	• '외국 정부 등'과 보안과제 공동 연구를 추진하거나 일부를 수행하게 하려는 경우 중앙행정기관장의 사전 승인을 얻어야 함

- (보안등급 표기) 보안과제 수행과정에서 산출되는 문서와 다양한 형식의 자료 및 데이터에 대하여 추가적인 보안이 필요한 지 여부를 판단하고, 추가적인 보안이 필요한 경우 자율적으로 보안등급을 구분하여 표기할 수 있으며 아래와 같은 기준 준용 가능

〈표 3-12〉 **보안과제 관련 문서·데이터·자료 등에 대한 연구개발기관의 보안등급 구분 기준 예시**

보안등급 구분	연구개발기관의 보안관리 조치(보안대책 제10조)
Ⅰ급	• 유출될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획 · 정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 보안과제의 핵심적인 정보
Ⅱ급	• 유출될 경우 국가안전보장 및 국가경쟁력 확보에 막대한 지장을 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 유출로 이어질 수 있는 경우
Ⅲ급	• 유출될 경우 국가안전보장 및 국가 경쟁력 확보에 해를 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 또는 간접적인 유출로 이어질 수 있는 경우

- (연구개발성과 귀속·실시) 보안과제에서 창출된 연구개발성과를 소유한 기관은 원칙적으로 해당 성과를 이전하지 않는 것으로 해야 하며 실시계약 시에는 '제3자 기술실시 금지협약' 체결 등이 필요

〈표 3-13〉 **보안과제에서 창출된 연구개발성과의 귀속과 실시**

상황		연구개발기관의 보안관리 조치(보안대책 제15조)
소유권 이전 원칙		• 보안과제에서 창출된 연구개발성과 소유권은 이전하지 않음
소유권 이전 특수상황	**국내 다른 기관 소유권 이전**	• 이전받는 기관이 '국가연구개발사업 보안대책' 제3조~15조까지를 준수하도록 계약 체결
	외국으로 소유권 이전	• 불가피하게 외국으로 소유권 이전 시 중앙행정기관장의 사전 승인 필요
국내외 실시계약		• 다른 기관과 실시계약 체결 시 '제3자 기술실시(사용)권 금지협약' 체결 • 외국기업 또는 외국으로 수출 시 중앙행정기관 장의 사전 승인 필요

- (보안심의위원회) 상기 연구개발기관의 보안과제 관련 보안관리 조치와 보안대책은 연구보안심의위원회에서 심의함

〈표 3-14〉 **연구개발기관의 연구보안심의위원회 심의 사항(보안대책제6조)**

1. 연구기관보안대책의 수립 · 변경(연구보안에 관한 자체규정의 제 · 개정을 말한다)에 관한 사항
2. 법 제21조제3항에 따른 보안관리 조치를 위한 계획에 관한 사항
3. 법 제21조제3항에 따른 보안관리 조치에 관한 자체점검 결과 및 자체점검 결과에 따른 조치방안에 관한 사항
4. 제8조에 따른 외국 정부 등과의 접촉 관리에 관한 사항
5. 제9조에 따른 외국 연구자 등의 참여에 관한 사항
6. 보안사고에 대한 조치계획 및 재발방지 대책에 관한 사항
7. 연구기관보안대책을 위반한 연구자에 대한 징계에 관한 사항
8. 보안과제 참여 연구자에 대한 보안수당 지급에 관한 사항
9. 그 밖에 연구개발기관의 장이 보안과 관련하여 심의가 필요하다고 인정하는 사항

○ (실태점검) 중앙행정기관의 장은 보안대책 수립시행 및 보안관리 등의 실태를 점검할 수 있으며 해당 연구개발기관에게 관련 조치를 수행할 수 있도록 명할 수 있음

- 조치 사항을 명받은 연구개발기관은 6개월 이내에 중앙행정기관의 장에게 제출해야 함

○ (사고관리) 연구개발기관의 장은 보안사고가 발생한 경우 이를 알게 된 즉시 조치를 하고 중앙행정기관의 장에게 보고를 해야 함

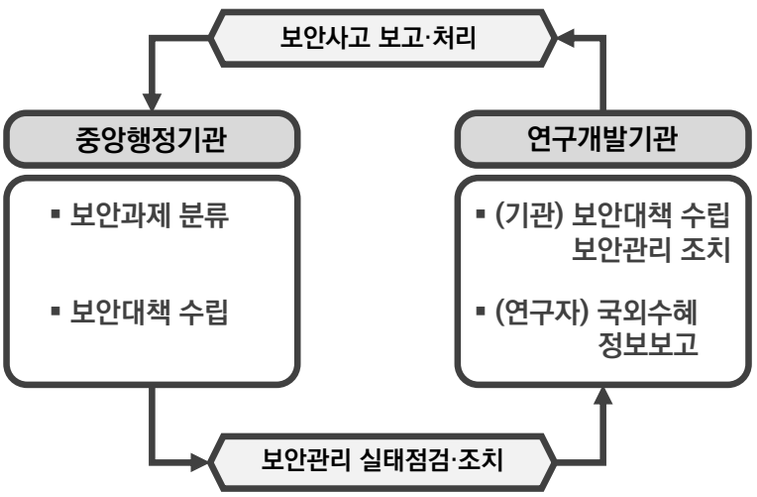
- 보안사고는 시행령 제44조제1항 각호에 해당하는 연구개발성과의 침해·유출·누설·분실·훼손·도난 또는 해당 연구개발성과를 유통·관리·보존하는 시스템의 유출·파손·파괴를 말함
- 연구개발기관의 장이 중앙행정기관의 장에게 보고해야 할 사항은 ① 보안사고의 일시·장소 ② 보안사고를 낸 사람의 인적사항③ 보안사고의 세부 내용임
- 중앙행정기관의 장은 보고받은 보안사고에 대한 경위를 조사할 수 있으며 연구개발기관 및 연구책임자는 조사에 성실히 협조해야 함

❑ (관계자 역할) 혁신법 및 보안대책(고시)은 주요 이해관계자 별 구체적인 보안 관리를 위한 역할을 부여하므로 국가연구개발사업 관련 중요 정보의 유출을 자발적으로 방지할 수 있도록 하고 있음

○ 중앙행정기관 및 연구개발기관은 '보안과제 분류, 보안대책 수립 및 관리, 보안사고 보고처리'등에서 밀접하게 연결되어 있는 구조

〈표 3-15〉 **국가연구개발사업 연구보안에 대한 주요 이해관계자 역할**

구분	관련 법령 및 내용 (협약의 세부조건(예시))
중앙행정기관	• 국가연구개발사업 정보에 대한 보안 관리 및 조치
연구개발기관	• 연구윤리규정 마련 및 운영 • 부정행위 등 발생 시 중앙행정기관에 보고 • 연구개발과제의 보안관리
연구자	• 연구윤리를 준수하고 진실하고 투명하게 국가연구개발과제를 수행해야 함



[그림 3-1] **국가연구개발 보안 관련 이해관계자 조치 사항 범위**

※「(고시) 국가연구개발사업 보안대책」을 적용하는 중앙행정기관의 장은 해당 고시 준용,
연구자는 보안과제 여부와 관련 없이 국가연구개발과제를 수행한다면 국외수혜 정보 보고 필요

○ 혁신법 및 보안대책 상 연구개발기관 및 연구자에게 부여된 주요 연구보안 조치 사항은 아래와 같으며 이는 연구보안 현장지침에 반영 필요한 사안임

〈표 3-16〉 **혁신법 및 보안대책 고시에 따른 연구개발기관·연구자 연구보안 조치 필요사항**

구 분	상세내용
보안대책 수립	① 보안관리 체계 ② 보안과제 참여 연구자관리 ③ 연구개발성과보고 ④ 연구시설·정보통신망 관리
보안관리 조치	① 보안과제 관련: 연구실 보호구역 설정, 출입권한 관리, 보안교육, 외국인 연구자 관리 ② 제반 사항: 연구관리시스템, 연구개발정보처리 및 결과, 보안책임자 지정
보안사고 관리	보안사고 발생 시 중앙행정기관장 보고 조치
실태점검 이행	중앙행정기관장의 실태점검에 응해야 하며 관련 조치 명령 이행 필요
국외수혜 신고	연구개발수행 기간 중 발생한 국외수혜 관련 연구자의 신고조치

○ 연구보안 현장지침은 국가R&D 주요 단계 별 '연구자 및 연구개발기관'이 주로 지켜야 할 법절차를 설명하고 있으므로 지침 구성에 앞서 아래와 같이 연구개발과제 전주기 상각 이해관계자가 지켜야 할 법률에 대해 분석함

〈표 3-17〉 **참고: 국가연구개발사업 연구개발과제 전주기 연구보안 절차 요약**

연구 전주기	주요 연구보안 절차		연구보안 주체		
			중앙 행정기관	연구 개발기관	연구자
사전기획	보안과제 분류	• 사전기획 시 보안과제 해당 여부 검토(영제8조제2항) • 공모 전 보안과제 분류(영제45조제2항)	√		
연구개발 기관 선정		• 공모 시 보안과제 해당 여부를 포함하여 공고(영제9조1항제1호라목) • 지정 등 공모외 방법이거나 공고 시 보안과제 해당 여부를 알리기 어려운 경우 연구개발기관 선정 후 보안과제 분류(영제45조2항)	√		
협약체결	보안대책 수립	• 국가연구개발사업 보안관리에 대한 연구개발기관의 의무를 포함하여 협약 체결(시행규칙 별지2호 협약조건 예시) • 중앙행정기관장 및 연구개발기관장의 보안 대책 수립(영제44조)	√	√	
	국외수혜 정보보고	• 연구책임자의 국외수혜정보를 연구계획서에 기재(영제9조제3항)			√
연구수행/ 성과관리	보안관리 추진	• 보안과제 관련 연구개발기관장의 보안관리 조치(영제46조)		√	
	보안과제 분류	• 연구개발기관 장 요청에 따라 중앙행정기관장이 보안과제 재분류 가능(보안대책제3조제2항~3항)	√	√	
	국외수혜 정보보고	• 과제 수행 도중 발생한 연구책임자의 국외수혜정보를 IRIS 연구자정보(NRI)에 현행화(영제9조제3항)			√
평가/ 성과관리	보안과제 평가	• 보안과제의 경우 단계 및 최종평가를 실시하지 않을 수 있음(영제16조제3항1호)	√		
	소유권 이전/실시	• 보안과제 연구개발성과는 이전하지 않는 것이 원칙이나 특수 상황 및 조건에서 연구개발성과 이전 및 실시가능(보안대책제15조)	√		
	보안과제 분류	• 최종평가 시 연구개발결과에 따라 보안과제 재분류 검토(보안대책제14조)	√		
제반 사항	보안 실태점검	• 중앙행정기관장의 실태점검과 그 결과에 따른 연구개발기관 장의 조치 사항(영제47조)	√	√	
	보안사고 처리	• 연구개발기관장의 보안사고 보고 조치(영제48조제1항~2항) • 중앙행정기관장의 보안사고 경위조사(영제48조제3항_)	√	√	
	부정행위 규정	• 보안과제 관련성과 누설 및 유출, 보안대책 위반(법제31조제1항의4호)		√	√
	부정행위 제재조치	• 연구개발과제 2~5년 참여제한(영제59조제1항) • 연구개발과제 제재부가금 처분(영제59조제2항)	√		
	인센티브	• 보안과제 참여 연구자에 대한 수당(연구개발비 사용기준 제11조의2)	√	√	√

3 유관 법령 분석

❑ (개요) 우리나라 법체계 내에서는 보호가 필요한 여러 종류의 기술을 개별 부처 법령에 따라 지정하고 보안관리 조치를 진행하고 있으므로 유관 법률에서의 보안 관리 조치 사항을 확인하여 '연구보안 현장지침'에서 관련 법 간 상충 방지 필요

❑ (전략기술육성법) 국가전략기술의 정보보호 및 보안에 관한 사항, 전략연구과제의 보안과제 분류, 외국 정부 등의 정보제공 요청에 대한 대처 등에 대한 사항이 혁신법과 발맞추어 제시되고 있음

- 혁신법의 보안과제 관리와 마찬가지로 국가전략기술의 보안관리 조치를 수행할 수 있음
- 다만 국가전략기술의 기술적 특성을 반영한 보안관리 체계의 수립이 가능하며 보안과제가 아니더라도 국가전략기술에 해당 시 외국 정부 등 정보제공 요청에 대해 알려야 할 필요성이 있음

〈표 3-18〉 **국가전략기술육성법 상 보안관련 사항**

구 분	상세내용
국가전략기술 정보보호 및 보안 주체의 역할	• 국가, 지방자치단체, 기술육성주체는 국가전략기술에 관하여 보유하고 있는 정보의 유출로 인해 국가안전보장 및 국민경제에 악영향을 미치지 않도록 정보보호에 필요한 인력확보, 설비 구축, 정보 유출 예방등에 조치 필요
외국 정부 등의 정보 제공 요청에 따른 통보	• 기술육성주체가 국가전략기술 관련 정보제공 요청 시에 해당 사실을 중앙행정기관의 장에게 알려야 함 • 이 때 알려야 하는 정보의 범위는 보안과제로 분류된 전략연구과제 중 '인력, 성과, 전략기술 관련 경영정보' 및 '국가전략기술 관련 정보' 등임 • 중앙행정기관 장에게 '정보제공을 요청한 외국정부 및 기관, 요청받은 정보의 내용'에 대해 알려야 함
보안과제 분류 및 보안관리 조치	• 혁신법에 따른 보안과제 분류가 가능하며 전략연구과제의 기술적특성 등을 반영한 보안관리 조치 사항 별도 지정운영 가능 • 중앙행정기관의 장은 보안관리 조치 실행을 위한 예산 지원 가능
보안관리 실태점검	• 중앙행정기관의 장은 전략연구사업을 수행하는 기술육성주체에 대한 보안관리 실태점검을 할 수 있음

❑ (유사법령) 혁신법과 마찬가지로 '국가정보원법, 산업기술유출방지법, 방위산업기술보호법' 등에서 '인력·외국인관리·보안점검·사고관리·정보통신망 및 시설관리' 등의 영역에서 보안관리를 추진하고 있으며 '보안관리 조직(위원회)' 구성 등에 대해서도 제시

- 유사법령에서도 보안심의위원회, 보안전담인력 등 연구개발기관의 '보안조직 및 인력'에 대해서 제시하고 있으며 '보안' 업무의 영역이 '사업 및 통신 분야' 에 포괄적으로 제시되어 있음

- 외국인에 대해서는 유사 법률 전반적으로 ‘외국인 접촉 시 관리, 관리계획’ 등을 제시하고 있으며 산업기술유출방지법에서는 외국인 투자 등에서도 관리하고 있음
- 보안관리 실태점검·사고관리, 상벌 규정은 유사 법률에서 모두 존재하며 산업기술유출방지법에서는 신고자에 대한 포상금 최대 1억원 지급, 방위산업기술보호법에서는 위반자에 대해 최대 20년 이하 징역을 부과 등 특징 존재

〈표 3-19〉 보안 관련 유사 법령에서 다루고 있는 보안업무 현황

구분	국가연구개발혁신법	국가정보원법				산업기술의 유출방지 및 보호에 관한 법률	방위산업기술 보호법
	국가연구개발혁신법 시행령 국가연구개발사업 보안대책	보안업무규정 과학기술정보통신부 보안업무시행세칙	방첩업무규정 과학기술정보 통신부 방첩업무규정 시행지침	사이버안보 업무규정	국가정보보안 기본지침 과학기술정보 통신부 정보보안기본지침	산업기술의 유출방지 및 보호에 관한 법률 시행령 산업기술보호지침	방위산업기술 보호법 시행령 방위산업기술보호법 시행규칙 방위산업기술보호지침
위원회	• 연구보안심의회	• 보안심사위원회	–		• 보안심사위원회	• 산업기술보호위원회 분야 별 전문위원회	• 방위산업기술보호위원회 (위원장:국방부장관)
책임자	• 연구보안책임자	• 보안담당관, 분임보안 담당관, 정보보안담당 관 (단, 중앙행정기관은 위에 추가로 통신보안 담당관,특례기관보안 담당관,**과학기술분야 연구개발사업 보안담 당관,**정보통신방송분 야 연구개발사업 보안 담당관을 둠) • 보안부서장 • 원격재택근무보안 전담관(각 부서장)	• 방첩담당관	• 국가정보원장 (출연연적용됨)	• 정보보안 최고책임자 • 정보보안담당관 • 분임정보보안 담당관(청사, 시설, 비밀부서)	• 국가핵심기술 관리책임자	• 기술보호총괄책임자
전담 조직/ 인력	• 연구보안 전담인력 (연구지원 체계평가 편람)		• 방첩업무 담당 부서		• 정보보안 전담조직 /정보보안 전담 인력	• 보안 전담인력의 지정 핵심기술취급전문인력 구분관리	• 기술보호책임자 최소인원 가이드라인 준수 (업체인원수별최소인원지정, ex:1000명이상업체는최소 7명)

구분	국가연구개발혁신법	국가정보원법				산업기술의 유출방지 및 보호에 관한 법률	방위산업기술 보호법
	국가연구개발혁신법 시행령 국가연구개발사업 보안대책	보안업무규정 과학기술정보통신부 보안업무시행세칙	방첩업무규정 과학기술정보 통신부 방첩업무규정 시행지침	사이버안보 업무규정	국가정보보안 기본지침 과학기술정보 통신부 정보보안기본지침	산업기술의 유출방지 및 보호에 관한 법률 시행령 산업기술보호지침	방위산업기술 보호법 시행령 방위산업기술보호법 시행규칙 방위산업기술보호지침
교육	• 보안교육, 보안서약	• 보안교육 (자체계획 수립)	• 방첩교육	• 사이버공격위협에 대한 예방대응 교육	• 정보보안 교육/ 사이버보안 진단의 날	• 최소 연2회 이상 교육 실시 • 핵심기술취급인력별도교육	• 연1회 이상 교육 실시, 교육결과 30일 이내 방위사업청장 제출
외국인 관리	• 외국 정부 접촉 관리 • 외국 연구자 참여관리	• 외국인 공직임용 관련 보안대책 • 외국인 비밀취급 인가 제한 • 외국인에 대한 교육실시	• 외국인 접촉시 정보보호, 외국인 접촉절차, 특이사항신고, 외국 정보기관원접촉, 외국 정보기관 방문 등	–	–	• 외국기업 투자, 외국인 투자 진행시 장관에게 신고	• 외국인 관리계획 작성 필요 • 해당 외국인이 출입국시방위산업기술 보호교육 실시
보안 점검	• 보안대책, 실태점검 (점검주체는 중앙행정기관)	• 자체보안감사, 보안점검, 보안진단의 날	–	• 사이버공격위협 대응 훈련 • 사이버공격 위협에 대비한 진단점검 • 사이버 공격 위협에 대한 예방대응 실태 평가	• 정보보안 실태 조사, 점검	• 산업기술보호를 위한 실태조사 및 개선권고 (설문조사, 현장방문조사)	• 실태조사, 개선권고, 시정명령, 실태조사 심의위원회

구분	국가연구개발혁신법	국가정보원법				산업기술의 유출방지 및 보호에 관한 법률	방위산업기술 보호법
	국가연구개발혁신법 시행령 국가연구개발사업 보안대책	보안업무규정 과학기술정보통신부 보안업무시행세칙	방첩업무규정 과학기술정보 통신부 방첩업무규정 시행지침	사이버안보 업무규정	국가정보보안 기본지침 과학기술정보 통신부 정보보안기본지침	산업기술의 유출방지 및 보호에 관한 법률 시행령 산업기술보호지침	방위산업기술 보호법 시행령 방위산업기술보호법 시행규칙 방위산업기술보호지침
사고 관리	• 보안사고 조사 및 국정원 통보	• 보안사고의 통보 및 조치	–	• 사이버공격 위협의 탐지대응 • 경보발령 • 사고조사	• 정보보안사고 처리 및 조사 • 사이버공격 대응 및 조치(보안관리, 예방활동, 초동 조치, 사고통보 및 복구)	• 유출사고 대응체계 구축	• 방위사업청장 또는 정보수사기관의 장 조사권한 부여 • 기술보호를위한실태조사가능
상벌 관리	• 보안우수자 및 위반자 관리	• 위반자의 처벌(공무원 징계령 시행규칙 및 국가공무원 복무징계 관련 예규 준용) • 별표3 보안위규자 처벌기준	–	–	–	• 예산의 범위 내에서 포상금 지급 (최대 1억원) • 신고포상자에 대한 신변보호 • 공이 큰 외국인에 대한국내정착 및 국적취득	• 공고에 따른 신청이나 기관추천을 통해 포상자 선정 (포상금 최대 1천만원) • 위반자에 대해서는 최대20년 이하의 징역,2 0억원이하의 벌금 부과(위반 내용에 따라 차등) • 경미한 위반사항은 최대 3천만원 이하의 과태료 부과
참여 연구자 관리	• 퇴직자/퇴직예정자 관리 • 국외출장 시 사전보안교육 및 귀국보고 • 외국정부/기관접촉 시 보고 등	• 신원조사 • 원격 재택근무 관련보안 준칙	–	–	–	(법령이 기술 자체의 관리로 구성)	• 직무 상 해외출장 관리 보직이동 및 퇴직 관리 신원조사

구분	국가연구개발혁신법	국가정보원법				산업기술의 유출방지 및 보호에 관한 법률	방위산업기술 보호법
	국가연구개발혁신법 시행령 국가연구개발사업 보안대책	보안업무규정 과학기술정보통신부 보안업무시행세칙	방첩업무규정 과학기술정보 통신부 방첩업무규정 시행지침	사이버안보 업무규정	국가정보보안 기본지침 과학기술정보 통신부 정보보안기본지침	산업기술의 유출방지 및 보호에 관한 법률 시행령 산업기술보호지침	방위산업기술 보호법 시행령 방위산업기술보호법 시행규칙 방위산업기술보호지침
연구 시설 관리	• 노트북, 외장하드 등 매체관리 • 주요시설 CCTV,침입감지센터 • 전산실 및 중요시설물 보안조치 • 연구실/연구기관출입권한 차등 및 출입통제 • 화재/홍수/재난/재해 등 비상 시 대응계획	• 시설보안 • 국가보안시설보호 대책수립 • 보호지역의 설정,보호지역보호대책 • 보호지역출입통제	-	-	• 정보통신실 보안관리	• 보호구역 설정 및 출입허가 • 출입 시 휴대품 검사 • 보호구역 통신시설 및통신수단 보안	• 기술보호구역 설정 및 보호대책 수립 • 기술보호구역 출입 권한부여 및 마스터키 관리 • 외부인/외국인 근무구역관리 • 기술보호구역 정보통신장비 사용 통제 • 외부인/외국인 방문 시 출입통제
정보 통신망 관리	• 방화벽 시스템 등 전산보안장비 • 업무용 컴퓨터 업데이트 • 정보시스템사용 기록 6개월 이상 보관 • 내부망의 물리적 분리 • 외부자료 전송 시 사전신고 • 직책 및 업무에 따른 전자자료 차등 접근권한	• 비밀의 분류, 대외비 관리 • 통신보안,암호자재 • 정보보안(과기부 정보보안 기본지침 준용)	• 문서의 보존기간(10년)		• 정보시스템 보안책임 • 정보시스템 유지보수 • 서버보안/제어시스템보안/공개서버보안 • 로그기록유지 • 사물인터넷/원격근무보안 • 저장매체불용처리 등	• 정보처리과정 및 결과 자료 보호	• 정보보호시스템 설치 및 운용 • 정보통신망 관리운용 • 정보통신기기 및 저장 매체관리 • 전산자료반출관리

❑ (정보통신망 관련 법) '과학기술정보통신부 보안업무 시행세칙 및 국정원 보안업무 규정'의 '정보통신'에 대한 사항을 준용하되 산업계에서 주로 참고하는 '정보통신망 및 클라우드법' 또한 참고 필요

○ 대학 및 과기부 산하기관 등은 '국가정보원 보안업무규정'을 기본으로 하여, 기관 특성에 맞게 정보통신망 보안업무 가이드라인을 제시하고 있음

○ 기업의 경우 정보통신망 관련법 등에 영향을 받으며 관련하여 인터넷진흥원(KISA)은 정보통신망 보안과 관련하여 'SW, 기반시설'의 보안약점을 진단할 수 있는 상세 가이드라인을 배포

〈표 3-20〉 **정보통신망 보안관련 법령 목적 및 내용**

법령	법 목적	주요 내용
정보통신기반 보호법 (시행령, 시행규칙)	• 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장	• 정보통신기반시설의 보호체계의 구축 – 정보통신기반위원회 운영, 보호대책 및 계획 • 주요 정보통신기반시설의 지정 및 취약점 지정 – 주요 정보통신기반시설 지정권고와 취약점 분석평가 등 • 주요 정보통신기반시설의 보호 및 침해사고 대응 – 보호지침의 지정, 보호조치 명령, 침해행위 금지, 사고통지, 복구조치, 대책본부 구성, 정보공유 • 기술지원 및 민간협력 등 – 정보통신기반시설 보호위한 전문인력 양성, 관리기관, 국제협력 등
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 (시행령, 고시)	• 클라우드컴퓨팅의 발전 및 이용을 촉진하고 클라우드컴퓨팅서비스를 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 국민경제의 발전에 이바지함을 목적으로 함	• 클라우드컴퓨팅서비스 제공자는 침해사고 등이 발생하였을 시 이를 이용자에게 알려야하며 '정보통신망 이용촉진 및 정보보호 법'에 따른 사고 발생 시 이를 과기부 장관에게 알려야 함 • 클라우드컴퓨팅서비스 보안인증 유형 및 등급에 대해 안내
정보통신망 이용촉진 및 정보보호 등에 관한 법률 (시행령, 시행규칙)	• 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 함	• "정보통신망 이용촉진 및 정보보호등"에 관한 사안을 규정하고 있음 • 정보통신망 보안에 관해서는 '과학기술정보통신부 보안업무 지침'을 준용하도록 되어 있음
과학기술정보통신부 보안업무 시행세칙	• 국가정보원의 보안업무규정 제29조를 기준으로, 과학기술정보통신부의 보안업무 수행에 필요한 절차와 구체적 운용 사항을 규정	• 보안심사위원회, 인원, 문서, 시설, 통신 등 과학기술정보통신부의 감독을 받는 산하 공공기관의 보안 전반적 사안에 대한 지침 제공

법령	법 목적	주요 내용
국정원 보안업무 규정	• 국가정보원장이 정하는 각급기관(국가기관, 지자체, 교육청, 학교, 군 기관) 정보보안 기본업무에 대한 규정 사항	• 각급기관의 기능 유지를 주 목적으로 정보통신망 및 정보시스템을 통해 수집가공저장검색, 송수신정보 유출 등을 방지하기 위한 물리적/기술적/관리적 수단 등을 강구하는 것을 정보보안이라고 하며 정보보안과 관련된 전반적 사안에 대해 안내
교육부 정보보안 기본지침	• 국가정보원의 '국가 정보보안 기본지침'에 따른 교육기관 정보보안 기본지침	• 국가정보원 보안업무 규정과 유사하나 적용 범위가 교육기관(사립유치원 등 포함)인 것이 차별적인 사안

제3절 선행 연구보안 현장지침 검토 및 시사점 도출

1 해외 연구보안 지침 사례

□ (미국) NSTC가 NSPM-33법을 기반으로 '대학 및 연구개발 기관'을 대상으로 한 권고안을 제시한데 이어 NSF에서는 '연구자 및 연구개발기관'이 위험성을 진단할 수 있는 도구를 제공하고 있고 NIH는 사례적 접근을 통해 '연구현장'에 지침 제시

○ NSTC의 지침은 NSPM-33 이행을 위해 연구기관이 추진해야 할 5가지 목표와 추진사항 21개를 제시하였으며 연구기관 차원의 보안정책 마련과 위험관리 의무를 강조하고 있음[5)]

- 보안 관련 조직 구성(책임자, TF) 및 기관 내규 구성 등에 대한 조직차원 접근을 권고하고 있음
- '외국인 연구원 관리 방안, 외국과의 계약' 등에서 이해상충이 없고 투명성을 유지할 수 있는 시스템 및 제도 등을 구축하도록 연구기관에 촉구
- 외국기관과의 공동연구에 관한 내부 승인 및 검토절차, 국외출장·외국인방문자·데이터 보안조치 등 잠재적 위험요인에 대해서도 기관차원의 대응이 가능하도록 가이드라인을 제시

5) 'Recommended Practices for strengthening and security and integrity of America's science and technology research enterprise(NSTC, 2019) 'Recommended Practices for strengthening and security and integrity of America's science and technology research enterprise

〈표 3-21〉 NSTC 과학기술 연구자산 유지·보호를 위한 권고안 주요 내용

법령	주요 내용
❶ 조직 리더십 및 감독 입증	• 리더십 차원에서 연구 보안과 무결성의 중요성을 전달 • 연구 보안에 대한 조직적인 접근 방식을 보장 • 연구안보 및 무결성 워킹그룹 및 태스크포스(TF) 구성·운영 • 종합 연구안보 프로그램 수립 및 운영
❷ 개방성과 투명성에 대한 기대치 설정	• 이해상충, 역할상충 및 공개 관련 기관정책 수립·관리 • 잠재적 이해상충, 역할상충 식별을 위해 필요한 정보공개 요구 • 외국인 학생 및 연구자 정보시스템(SEVIS) 관련 정보공개 정책 수립 • 디지털 영구 식별자(DPI) 관련 정책 수립 • 외국으로부터 계약 등의 보고 의무
❸ 교육, 지원 및 정보 제공 및 공유	• 책임있는 연구수행에 대한 교육 제공 • 외국정부가 후원하는 인재채용 프로그램 참여 가이드라인 마련 • 연구안보 강화를 위해 지역 FBI 현장사무소와 협력 • 외국정부 지원 프로그램 계약에 대한 특정내용 보고 • 외국 기관 지원내용에 대한 정보공개 및 공유
❹ 조직 정책 준수를 위한 효과적인 메커니즘 보장	• 정보공개 정책 및 위반활동 등에 대한 대책 수립 및 이행 • 정보공개 위반 및 위반활동 등에 대한 처분방안 마련 • 연구안보 및 무결성을 지원하는 고용계약 조항 마련
❺ 협업 및 데이터와 관련된 잠재적 위험 관리	• 공동연구 현황 파악을 위한 기관 차원의 검토 및 승• 인절차 마련 • 국외출장 관련 위험기반 보안 절차 마련·운영 • 외국인 방문자 및 방문 학자와 관련된 위험관리 원칙 수립 • 데이터 보안조치 수립 및 관리

*출처: 과학기술정보통신부 및 KISTEP(2023.6). 국제연구협력 시 연구자산 유출 방지를 위한 주요국 정책사례집

○ NSF의 지침은 연구책임자 및 연구기관 등이 외국과 협력할 시에 파트너 선정, 협약 시 위험, 수출통제 정책과의 상충 등 위험성을 진단할 수 있는 사안에 대해 제시

〈표 3-22〉 「원천연구 안보에 관한 JASON 보고서」위험성 진단도구 주요 내용

연구책임자(PI)	연구기관·조직
• 계약·협약 내용 등의 내용과 조건이 명확한가?	• 미국의 국가안보, 정치, 사회, 인간적 권리에 해가 될 수 있는 요인들은 무엇인가?
• 모든 참여자들의 이해충돌과 역할상충 관련 모든 정보가 문서화되어 있는가?	• 미국의 국가 경쟁력에 위협이 되거나 수출통제 정책에 위배되지는 않는가?
• 불필요하거나, 명시되어 있지 않거나, 특이한 계약의 내용이 있는가?	• 지적재산 관련 위험요인은 무엇인가?
• 협약·계약에 따른 활동 수행을 위한 자금 및 비금전적 지원의 출처는 어디인가? 명확한가?	• 데이터 공개, 학술지 게재 및 발표 등과 관련한 지침이 명확한가?
• 참여자가 해당 계약·협약을 마치고자 할 때 절차는 어떻게 되는가?	• 조기 종료(중단)에 따른 위험은 무엇인가?

연구책임자(PI)	연구기관·조직
• 협약·계약 내용에 따라 연구자 등은 소속 기관 외의 공간에서 연구를 하여야 하는가? • 소속기관·조직에 보고하여야 하는 사항은 무엇인가?	• 계약·협약 내용이 잘못 해석되는 경우 발생할 수 있는 위험은 무엇인가? • 기관 자체의 핵심 가치에 위배될 위험이 있는가? • 기관이 해당 계약·협약에 참여하지 않았을 때 위험(손실)은 무엇인가?

* 출처: 과학기술정보통신부 및 KISTEP(2023.6). 국제연구협력 시 연구자산 유출 방지를 위한 주요국 정책사례집

○ 미국 NIH는 150개의 이해상충 관련 실제사례를 기반으로 4가지로 유형화하고 웹사이트에 공개하므로 연구자들의 이해를 제고하고 있음 6)

〈표 3-23〉 NIH의 외국협력 이해상충 사례 예시(가상의 시나리오)

구분	주요 내용
국내외 기관과 이중펀딩 사례	• 미국 내 펀딩기관에서 12개월 동안 지원을 받으면서 국외 대학의 수혜가 6개월 동안 중복된 경우 • 해당 과학자의 국외수혜가 연간 50만달러 이상이고 장비, 공간, 인력 등에 대해서 지원받았으나 해당 사항을 미국 내 펀딩기관에 알리지 않았으며, 미국 내 펀딩 받은 것을 외국어로 번역하여 국외 수혜를 지원함
경제적 이해상충 관계 비공개	• NIH 펀딩을 12개월 동안 받은 과학자가 같은 기간 동안 외국 기업과 20백만 달러 수준의 특허, 상품 등을 기술이전 • 해당 특허, 상품의 원천기술이 NIH 펀딩으로부터 발전된 경우였지만 NIH에 해당 사실을 알리지 않음
인재양성 프로그램에 대한 부정직한 보고	• NIH의 수혜를 받으면서 해외의 인재양성 프로그램으로부터 지원을 받았지만 해당 사실을 NIH에 공지하지 않은 경우
외국과 계약관계를 밝히지 않은 사례	• NIH 수혜를 받으면서 외국 대학과의 종일 계약을 맺고 있었으나 이러한 사실을 NIH에 밝히지 않은 사례

* 출처: NIH Foreign Interference: General Principles, Case Studies, Publicly Available Information on Specific Cases, and Oversight Reports(2023), From the NIH Office of Extramural Research (OER), NIH

❑ (영국) NSPA는 연구관계자들이 국외 연구를 추진할 시 연구 파트너 선정·계약체결, 연구자의 국외활동을 염두한 체크리스트를 제공하였으며 관련 내용을 학계 및 기업으로 맞춰 제시하므로 이해관계자들의 현장 적용을 지원함

6) NIH(2023). Brief Summary of NIH Foreign Interference Cases.,

○ 학계가 국제협력 관계에서 연구 파트너와 원활한 협업을 추진하기 위해서는 '파트너, 연구과제에 대한 정보, 기존 협력 관계에 대한 정보'에 대한 부분이 선행되어야 한다고 안내하고 있으며, 국외 체류에 대한 사안도 제시[7)]

- 국외 출장은 연구자가 '문제발생 시 보고대상 담당자를 파악하고 있는지, 해당 국가가 영국 수출통제 대상인지, 해외기관에 대한 정보 등을 파악하고 있는지에 대한 사안임

〈표 3-24〉 **NSPA 학계를 위한 신뢰할 수 있는 연구 체크리스트 주요 내용**

구분	주요 내용
협력 대상(파트너) 정보	• 파트너에 대한 실사(확인)을 통해 적대국 군·경찰 등을 대신하여 연구에 참여한 사실을 알게 되었는가? • 당신이나 소속기관 평판, 윤리 등에 위협이 있는가? • 협력에 문제는 없는가, 결정을 소속 부서 또는 기관에 보고하여 검토할 필요는 없는가?
연구 관계 정보	• 프로젝트에 연구데이터, 기밀 또는 개인 식별 가능한 데이터가 포함되는가? 보호계획은 있는가 • 지적 재산은 누가 소유하는가? • 협력 대상자가 소속기관 IT 네트워크 접근권을 갖는가? 어느 정도의 권한을 갖는가? • 소속기관의 이익 보호를 위한 계약 요건이 있는가?
기존 협력 대상 관련 정보	• 새로운 프로젝트가 기존 연구 파트너와 이해상충을 일으킬 가능성이 있는가? 협의한 적이 있는가? • 비공개 계약조건을 검토하고 기존 파트너들에게 알려야 하는 내용이 있는가?

* 출처: 과학기술정보통신부 및 KISTEP(2023.6). 국제연구협력 시 연구자산 유출 방지를 위한 주요국 정책사례집

○ 산업계에 대해서는 TRL 수준을 기준으로 민감한 연구에 대해서 판단하게 하고 지식재산보호, 데이터의 권리 이전 등 기업의 매출과 연관될 수 있는 연구개발성과에 대한 보호를 강조하고 있음[8)]

〈표 3-25〉 **NSPA 산업계를 위한 신뢰할 수 있는 연구 체크리스트 주요 내용**

구분	주요 내용
제안 관련 정보	• 연구의 기술성숙도(TRL)은 어느 정도인가? • 협력 과정에서 공유되는 데이터나 지적재산은 얼마나 민감한 이슈인가? • 연구성과가 나온 경우 파트너는 어느 수준까지 지식재산권 접근권한을 갖게 되는가?
기관 고려사항	• 프로젝트 간의 네트워크 분리 계획은 무엇인가? • 지적 재산권에 대한 합의 조건은 무엇인가? • 상대 기관의 다른 협력 관계는 어떠한가? • 직원 이탈 시 연구보호 절차는 어떠한가?

7) · https://www.npsa.gov.uk/trusted-research-academia
8) · https://www.npsa.gov.uk/trusted-research-academia

구분	주요 내용
프로젝트 내용 관련 정보	• 프로젝트의 데이터 저장서버는 어디 있는가? • 비공개 계약조건을 검토하고 기존 파트너들에게 알려야 하는 내용이 있는가, 데이터의 국외 이전 위험요소가 있는가?

* 출처: 과학기술정보통신부 및 KISTEP(2023.6). 국제연구협력 시 연구자산 유출 방지를 위한 주요국 정책사례집

❑ (일본) 문부과학성은 2021년 연구 국제화 및 개방화에 따른 위험에 대학 및 연구기관이 대응할 수 있도록 관련 체크리스트 양식을 제공함(2023년 추가개정)[9)]

○ 일본의 경우 연구기관이 스스로 위험을 감지하고 평가할 수 있는 조직체계가 구성되어 있는지, 연구자를 지원해줄 수 있는 헬프데스크 등 시스템이 있는지 등을 강조함

〈표 3-26〉 **일본 국제공동 연구시 위험성 진단 위한 체크리스트(대학 및 연구기관용)**

구분	주요 내용
일반사항	**〈이해상충 및 위험에 관련한 소속기관의 대응체계〉** • 소속 연구자가 위험에 빠졌을 때 이를 상담지원해 줄 수 있는 컨설팅 헬프데스크가 존재하는가? • 소속 연구자와 스탭이 위험에 관한 교육을 받을 수 있는 기회가 존재하는가? • 소속 기관에 위험에 대한 정보를 파악할 수 있는 시스템이 마련되어 있는가? **〈연구자의 이해상충 보고를 축적/확인할 수 있는 정보 시스템〉** • 연구자 및 소속직원이 제출한 이해상충 보고사항을 재확인할 수 있는 메커니즘을 보유하고 있는가? • 연구자 및 소속직원이 협력하고자 하는 국외 기관에 대한 위험성을 판단할 수 있는 수단을 보유하고 있는가
외국정부, 기관과 협력시에 대응방안	**〈MOU, 국제공동협력 연구를 할 시 규칙 존재 여부〉** • 적절한 양식이 존재하는가? • 국제협력 대상자에 대한 위험을 평가하고 있으며, 타 경로로 정보를 획득하여 정보를 비교하고 있는가? • 위험에 대한 우려가 존재할 시 이를 평가하고 대응할 수 있는 체계가 존재하는가? • 연구원들이 협약을 진행하기 전에 조언을 구할 수 있는 헬프데스크가 존재하는가? **〈국외수혜정보를 보고받을 수 있는 체계가 존재하는지 여부〉** • 연구자들이 국외수혜를 받을 시 이를 지원해 줄 수 있는 헬프데스크와 관련 정보를 재검증할 수 있는 시스템이 존재하는가? **〈연구자의 국외출장에 대해 대처할 수 있는 규정, 체계가 존재하는지 여부〉** • 수출통제 국가에 해당하는 곳에 연구자가 방문하였을 시 위험성을 판단할 수 있으며 관련하여 다른 경로로 정보를 재확인 할 수 있는가?

9) https://www8.cao.go.jp/cstp/english/doc/checklist_for_univ_en.pdf

구분	주요 내용
외국정부, 기관 등 파트너 정보에 대한 사안	• 해외 파트너 및 최종 사용자 등에 대한 위험성 정보를 평가할 수 있는 목록을 보유하고 있는가? • 소속 기관이 어떠한 위험에 대처해야 하는지에 대해 파악하고 있는가?

2 국내 연구보안 지침 사례

❑ 선행문헌 분석 및 한계 파악을 통한 시사점 도출

○ (방법) 기존 연구·산업보안 지침, 출연연 규정 등에 대한 분석으로 기존 지침의 구조적 한계 식별 및 지침 고려항목 도출

〈표 3-27〉 선행문헌의 검토범위

구분	분석대상 지침
연구보안 지침	• 국가R&D표준관리 표준매뉴얼('14·미래부) • 연구보안 이해('15·KIRD) • 연구보안길라잡이('21·NST 및 정보원)
산업보안 지침	• 산업보안 안내서('21·산업부) • 중소기업 기술보호('19·대중소협력재단) • 영업비밀 표준서식('17·특허청) • 기술 해외유출 방지('22·지재위)
기타 규정	• (내부규정) 보안등급이 높은 출연연의 내부 규정 검토 • (기타) 국가정보원 정보보안 지침, 인터넷진흥원 통신기반시설 가이드 및 정보보호 대책 요구사항

○ (한계점) 기존 지침은 법제도 준수, 5대 보안영역 등 보안관리 관점에 치우치거나 보안개념 미비, 독자층 설정 오류 등으로 가독성이 낮다는 한계를 가지므로 이를 개선하기 위한 구조 필요

〈표 3-28〉 연구보안 관련 현장 관계자의 현장지침 수요

◦ “연구현장에서 참고할 수 있는 보안 매뉴얼 부재”(’23.4.혁신본부장님 주재 연구보안 간담회)

◦ “기존 연구보안 지침은 발행기관 분산, 홍보 부족으로 혼란이 유발”
“‘미래부(2014)’ 지침이 연구보안 관계자 활용성이 높았던 편이며 이를 참고해서 여러 기관에서 기반을 구축” (’23.12. 연구보안 관련자 인터뷰)

○ (지침적용) 정책 현장착근·연구현장 적용 실질성, 연구자 가독성 등을 고려한 지침 작성 방향 필요

- R&D 전주기와 보안영역 결합, 구체성 높은 사례구성, 간결한 원칙을 제시하는 안내서 등으로 연구자 가독성 제고
- 연구보안(연구윤리 강조, 산업보안과 차이)·보안주체·대상·보안조치 등 관련 개념과 범위에 대한 안내
- 법제도 구현의 실질성을 위해 보안·민감과제 관리 관점 부여
- 규정 및 절차 준수 과정을 반영한 체크리스트

〈표 3-29〉 **선행 연구보안 지침의 한계분석 요약**

구분	국가연구개발사업 보안관리 표준매뉴얼 ('14·미래부)	연구보안의 이해 ('15·KIRD)	연구자를 위한 연구보안관리 길잡이 ('21·국정원·NST)	연구보안 현장지침 ('24)
성격	· 규정준수 위한 지침 – 보안담당자 관점	· 연구자(대학원생) 교육자료	· 연구자 대상 연구보안 소개	· **국가R&D 과제 수행 연구(책임)자, 기관** 대상 안내서 – **연구(책임)자 눈높이에 초점**
연구 보안 개념	· 연구보안 정의, 지켜야 할 자산에 대한 제시미흡 · 보안·일반과제 관리의 개념	· R&D 전주기에서 연구자의 정보·성과물 유출 방지 위한 활동 · 연구정보-보안연계	· 연구자·기관의 R&D전주기 상 연구산출물 무단 유출 방지 활동 – (주체)연구자·기관 – (대상)연구원, 시설,자료,성과 – (방법)규정,장치, 시스템	· **R&D 전주기 관점**필요 · 기존 **연구보안에 연구진 실성 강조, 산업보안 차별화 된 개념제시**
구성	· 과제종류 및 이행대상자 별 5대 보안영역 준수사항 제시 · 피상적 체크리스트(결과중심) · 구체성이 낮은 사례 제공	· 법제도 소개 · R&D 단계별 연구자 추진사항 · R&D 제도 교육 전반	· [연구자] R&D전주기 보안영역 안내 · [연구기관] 보안항목 준수사항	· 법제도 구현의 실질성을 위해 **보안·민감과제 관리 관점 필요** · **과제종류, 이행대상자 고려** · 5대 보안영역과 규정점검 결합 · 연구자와 기관의 인위적 역할 구분은 실효성이 낮음 · **규정·절차준수 과정 반영한 체크리스트** · **구체성 높은 사례구성**

○ 선행 산업보안 관련 지침은 주로 기업을 대상으로 자체적으로 보안수준을 진단하고 대응할 수 있는 체크리스트를 제시함과 동시에, 사고처리 방법, 사고사례 등에 대하여 상세하게 안내하고 있음

- 주로 기업대상, 완제품 기술유출을 대상으로 하고 있어 연구보안과 범위가 다르지만 현장에 오랫동안 적용되어온 지침이므로 현장의 실정을 다수 반영

〈표 3-30〉 **(참고) 선행 산업보안 관련 지침**

구분	산업보안 안내서('21) (산업기술보호지침)	중소기업 기술보호 지침('19)	기술의 해외유출과 탈취 방지를 위한 연구자 가이드 라인('22)	꼭 알아야 할 영업비밀 관리 표준서식 활용서('17)
작성 주체	산업기술보호협회 (산업부)	대중소기업농어업 협력재단 (중소기업부)	지식재산위원회 (부처 공동)	영업비밀보호센터 (특허청)
관련법	「산업기술의 유출방지 및 보호에 관한 법률」 제8조 「산업기술보호지침」 제43조(산업보안 안내서)	중소기술보호법 중소기업기술 보호지침	산업기술/국가핵심기술 유출 외 다양한 관련법	영업비밀보호법 등
목적	• 국가핵심기술 유출 방지를 위해 필요한 방법/절차를 관련 기관이 활용할 수 있도록 작성	• 보호역량이 영세한 중소기업에게 보호 지침을 구체화하여 사고예방 • 사고구제/정부지원 안내	• 기술유출 사례를 기반으로 기업 관계자의 경각심 제고/교육	• 기업 경영 시 필요한 영업비밀 관련 표준서식 망라
주요 독자	• 산업보안 관리 담당자 (기업/출연연)	• 중소기업 산업보호 담당자	• 기업 관계자 • 기업 내부 국가핵심기술 연구자	• 기업 규모/업종, 영업비밀의 특성 등의 다른 불특정 다수의 기업 등
목차 구성	**제1장 산업기술 유출·침해 예방 및 보호 조치** **제2장 산업기술 유출·침해 대응 및 복구** **제3장 산업기술 계약 시 유출 방지 및 보호 조치**	**제1장 보호 지침 개요** **제2장 기술분류/ 중소기업 성장 단계별 기술 보호** **제3장 기술보호 수준 자가진단** **제4장 기술 유출 예방/관리/운영 방안** **제5장 기술 유출과 사후 구제**	**1. 서론** **2. 보호대상 기술 및 유출 사례** - 보호대상 기술 - 기술유출 유형/ 피해사례 **3. 연구자가 알아야 할 법령** **4. Q&A** **5. 기술유출 방지 체크 리스트**	**제1장 활용 가이드 소개** **제2장 표준서식 및 해설** - 내부관계용(인력/물리) - 외부관계용(비밀유지/분쟁) **제3장 영업비밀보호규정 (부록) 표준서식**
특징	• 법률에 따른 충실한 내용 • 예방-사고 관점, 기업의 주요 활동에 따른 보호조치 등 안내 • 관리자를 위한 것으로 보이며 산업핵심기술 연구자가 관련 내용 숙지 어려움	• 보호범위/영역 명확한 구분 • 중소기업의 성장단계에 따른 안내와 자가진단 가능 • 예방,사고 조치 방법 동시 제시 • 기술유출 사후구제와 정부 보호제도 안내 • 연구에 대한 관점은 부족 • 중소기업 전용 내용 다수	• 해외기술유출으로 범위를 좁혀 긴박성 존재 • 유출경로/사례를 종합해 유형화해서 알기 쉬움 • 기술유출의 책임성 강조 • 독자층, 보호대상을 구체화하지 않음 • 적용법률이 포괄적이어서 범위가 넓은 형태도 있음	• 보안과 관련된 각종 서식이 망라되어 있어 업무에 참고하기 쉬움 • 기업대상이어서 연구와 다른 부분 존재 • 서식 현행화 필요

제4절 연구현장 이해관계자 정책소통 기반 현황 파악

1 연구보안 이해관계자 대상 심층 인터뷰 추진

◻ 연구현장 FGI 기반 작성 시사점 발굴

○ (방법) 다양한 연구현장 이해관계자를 대상으로 한 정책피드백·선행 지침 의견·보안사고 사례를 취합하여 지침구성 시사점 도출

〈표 3-31〉 **연구현장 FGI 기반 작성 시사점 발굴 방법**

이해관계자		수요발굴 취지		인터뷰내용
연구자	· 학제 분야 및 산학연을 고려한 연구자 면담 ※학제(기계·정보·생명·기초·에너지), 대학·출연연·기업, 수도권·지방대	· 연구보안에 대한 현장 인식 파악과 지침 고려 필요사항	▶	· 정책필요성 · 보안·자산 개념 · 보안현황 · 해외수혜 · 민감과제 · 성과공개 · 유학생 · 지침 활용성
지원인력	· 과제관리(연구지원팀) · 보안담당팀 · 성과관리(TLO·기술지주사)	· 과제운영 및 보안조치 관점에서 연구보안 체계 구축을 위한 실무자 필요사항 확인		
전문기관	· 국책연구 기획·운영 관리자(연구재단 단장급)	· 중앙행정기관장(전문기관) 관점의 연구보안 관리 조치		

○ (연구자) 연구보안 정책 본격화에 공감하나 연구자가 위축되지 않도록 연구계를 설득*해 가며 장기적·순차적 도입 필요

* 사례제시, 시범사업, 인식조사 결과 기반 설득

〈참고〉 연구보안 정책 인식에 대한 현장 인터뷰 中 연구자 논의사항

◦ "미국 등 우방국가의 연구 보안 강화 움직임이 있다면 외교적 마찰을 피하기 위해서라도 정책의 틀을 갖춰 나가는 것은 공감. 국내 연구자들도 천인계획 참여 요청 연락 등을 받고 있고 실제 K대 사고 사례 등 필요성에 공감대"

* (예1) 미 하원 중국특위는 20년간 미중 관계 분석을 기반으로 중국과 경쟁에 승리하기 위해서는 '연구보안을 강화하여 미국 기술의 중국 공산당 유출을 막고 우방과의 기술협력을 강화하여 경쟁우위를 점해야 한다고 제언'('23.12)[10]

* (예2) 미국 NIH가 관계 연구기관의 불법해외 접촉사례 255건('18~'23.11)을 조사한 결과 176건(69%)의 사례에서 연구자들이 외국 정부로부터의 금전 지원을 은폐하였다고 밝혔으며 이로 인해 전체 사례 중 111건(43.5%)에서 해임 등 발생('23.11)[11]

* (예3) '19년 중국이 인류 최초로 달 뒷면에 창어4호를 착륙시킨 사건은 미국의 우주 국제협력 정책에 변화를 촉발, 미 정부 관계자들은 10여년에 걸친 미-중 협력 과정에서 자국 원천기술의 유출이 발생했다고 간주하고, 안보 관점에서 견제로 태세 전환[12]

◦ "우리나라의 원천·기초 분야는 해외 대비 열위로 기술 유출 여지는 희박하다고 생각되며 무조건적인 보안보다는 개방과 보안 간 균형이 필요. 특히 전체 정부R&D 예산이 조정된 여건에서 국제협력과 보안을 동시적으로 활성화하는 접근은 부담스러움"

* (예) '21년 미국 물리학회는 연구보안 정책에 대한 학계 설문조사 결과 연구보안 정책이 국제협력 및 연구 개방성을 저해한다며 정책 개선 요구[13]

◦ "극소수의 보안사고를 예방하기 위해 전체가 불편해지는 상황임. 고액과제 운용 연구자 중심 접근, 사례제시, 시범사업, 인식조사 결과 등을 들어 설득 필요"

※ FGI에 참여한 현장연구자 의견이며 KISTEP 및 과기정통부 의견과 다를 수 있음

- (공통) 치명적인 자산 유출은 인력이동이며 연구보안 관리 주체는 결국 일선 연구책임자이기에 관련자 인식 교육 필요

10) The Select Committee on the Strategic Competition between the US and CCP (2023). *A strategy to win America's Economic Competition with the Chinese Communist Party*, United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party.

11) https://grants.nih.gov/policy/foreign-interference/data, accessed on Feb 14 2024.

12) Carrai, M. A., Randolph, J. and Szonyi, M. (Eds.) (2022). *The China Questions 2: Critical Insights Into Us-China Relations*, Harvard University Press.

13) APS (2021), *Impact of US Research Security Policies : US Security and the Benefits of Open Science and International Collaborations*, American Physical Society.

〈참고〉 인력을 통한 자산유출에 대한 현장 인터뷰 中

〈외국인 유학생이 기술을 유출하는 경우〉
◦ “지방대의 대학원생 인력 수급은 심각하여 방학마다 학생 유치를 위해 홍보하는 실정, 향후 유학생은 국가에 없어서는 안될 인적 자원으로 자리매김 할 것이며 관리 필요”
◦ “민감과제라도 지방대는 유학생이 과제를 수행하게 될 확률이 높음. 같은 실험실 내에서 교수가 학생을 차별하기도 어려워서 차라리 민감과제에 대한 행동 강령을 지정해 주었으면 좋겠음”
◦ “대학연구실 교류로 온 연구원(학생)이 실험 데이터의 일부를 취득해 본국으로 돌아가 해외학회에 논문을 발표한다던지, 유료로 다운로드 받을 수 있는 자료를 본국에 보내준다던지 하는 상황도 존재”
◦ 출연연의 UST 학생들은 원자력연 등 주요 출연연에 5~6년에 머무르며 출연연의 동향을 파악할 수 있음. 유학생에 대한 연구자들의 의견이 천차만별이라 지침 필요함”
◦ “해외 선진국가들은 유학생들의 연구테마를 달리하는 등의 방법으로 민감과제 보호 조치를 취하고 있음”

〈퇴사·이직·휴직자〉
◦ “A연구원에서 퇴사자(국립대 교수로 이직)가 본인이 쓰던 연구기자재를 늦은 밤에 무단 반출하는 상황이 CCTV에 찍혔음”
◦ “우리나라의 원자력, 국방관련 수출이 증대되며 이를 따라 퇴직자가 수출국가로 가는 사례도 빈번하게 발생. 기술을 파는 것이 정책 방침이므로 사람이 따라가는 것을 막을 수 없으나 퇴직자들의 두뇌에는 기밀 사항이 있을 수 있음을 생각해야 함”
◦ “출연(연)의 연구자나 대학의 박사후연구원이 대학교 교수로 임용되어 가면서 기존의 소속 연구소나 대학교의 연구데이터 및 연구장비를 절도하는 사례는 종종 발생함”
◦ “연구 연가시 해외 연구기관과 공동연구를 위해 연구 중이던 주요 연구자료를 별도 신고 없이 유출하고, 해외기관과 연구내용 및 데이터 공유”

〈창업자〉
◦ “실험실 창업자의 경우 투자가 간절한 반면 보안은 취약한 경우가 많음. 중국 투자자들은 손쉽게 투자해 주거나 M&A 제의를 함. 또한 NASDAQ 진출 전에 싱가폴 시장을 거치는 경우가 많으므로 중국 자본에 노출이 많을 수 있음. 불법은 아니지만 중국 영향력이 국내 과학계에 침투하는 경로가 될 수 있으므로 주의 필요”
◦ “실험실 창업 교수 중 일부는 인식 부재로 NDA 없이 해외 기관과 공동연구와 기술실용화를 하는 경우도 있으며 본교에 알리지 않고 해외 용역을 받기도 함. 실질적으로 본교 담당자는 창업 연구자에 대한 관리를 하지 못함”

- (대학) 학제 별 개방성 수준이 달라 일괄 적용하기보다 학자들의 합의가 이뤄지는 분야* 위주 관리 필요

* 원천기술 유출 시, 글로벌 기술선점·신산업 태동에 악영향을 줄 수 있는 분야가 학제별 존재
※ 단, 인적관리·IT·시설보안 등 인프라 전반 개선 필요성은 미흡 사항 인정

〈참고〉 대학의 실험실 보안환경 관련 현장 인터뷰 中

◦ “대학은 학생들이 실험실을 오고 가며 배울 수 있는 지점이 많아서 실험실 개방 다수”
◦ “대학의 정보통신망 관리는 출연연에 비해 자유로운 것이 사실, 지메일·드랍박스·개인 컴퓨터 사용 등 전반적으로 관리 미비. 또한 학교마다 관리 수준이 다름”

- (출연연) 보안정책 대부분 기구축, 국부 창출을 위해서는 국제적 협력·경쟁이 동시 공존하는 분야에 뛰어들 수밖에 없으며 이때 개방성-보안 간 균형감각 필요

  ※ 일부 원천기술 보안은 출연연에서 이미 관리하고 있는 현황, 그 외 비밀사항은 대부분 산업비밀과 연계

〈참고〉 출연연 관계자의 연구보안 정책 관련 인터뷰 中

◦ "출연연은 그간의 사이버공격, 인력유출, 평가 등 경험이 누적되어 보안 수준이 상대적으로 높아 민감한 기술은 별도로 관리하고 있음. 즉 연구보안 제도에 대한 거부감은 낮은 편"
◦ "원자력 분야의 경우 국제협력과 함께 보안이 중요한 대표적인 분야로, 연구발전을 위해 국제협력을 하는 것이기에 서로가 가진 것을 보여주기도 하고 경쟁도 하므로 공동연구에 따른 기술 유출이라는 단점을 최소화하면서 기술 제고라는 장점을 극대화할 수 있도록 하는 접근이 중요. 한편, 원자로 운용에 관한 지식은 국가별로 고도의 보안등급의 산업기밀로서 관리"

- (기업) 민감·보안과제 성과공개 지연 시 '미래가치 실현'을 포함한 보상 검토 필요하며 규제로 작용하지 않도록 해야 함

  ※ 대중소 기업 역량에 따라 보안정책이 천차만별

〈참고〉 기업 연구보안 정책 관련 인터뷰 中

◦ "보안, 민감과제 설정으로 성과활용이 지연되거나 기업의 경영성과가 위축되는 경우가 발생한다면 투입 연구비가 아니라 예상 미래가치 등을 기준으로 피해보상 필요"
◦ "기업의 경우 연구성과를 비공개로 하고 싶어서 보안과제로 과제분류를 요청하는 경우가 있으나, 해외출장 신고조치 등 행정적 부담이 커서 보안과제 분류를 후회하는 경향"
◦ "보안대책에 기술이전에 대한 판단주체와 기준이 제시되어 있지만 여전히 절차 등이 불명확하다고 관계자들은 생각하는 경우가 많음. 국가핵심기술 경우에도 이전이 가능하지만 위원회를 열어서 이전을 결정해야 하기 때문에 위원회를 열어주지 않으려고 하여서 기업의 불만이 큼"

○ (지원인력) 연구보안-과제관리-성과관리 부문 간 협업이 미약하여 보안 전주기 관리는 어려운 현황이며 규정 사문화된 상황

  ※ 지침 발행기관 다수여서 혼란, 대학의 경우 내부적으로 보안업무가 '과제관리·시설관리·정보 등'으로 산재 되어 지침적용 쉽지 않음

〈참고〉 지원인력 대상 인터뷰 中

◦ “대학의 경우 연구보안 규정은 존재해도 담당 인력이 없는 경우가 많은 상황. 최근 연구지원 인력들이 교육 수강을 통해 관련 업무를 겸직으로 추진하고 있으며 전문성 및 경험이 없는 상태. 만약 기관 단위 책임이 강화된다면 사고가 났을 때 이들이 피해보는 것이 아닌지 우려되므로 사고가 났을 때 누가 책임질 것인지 명확히하는 것이 필요”
◦ “연구자-연구기획처-연구관리-성과관리 담당자 간에 보안 관련 소통은 없는 상태, 보안과제에서 창출된 성과인지 모르고 관리하는 경우도 많음 ”
◦ “보안심의위원회는 규정 상 ‘총무-시설-정보-연구처’ 등이 모여 추진하거나 또는 단과대별 학장들이 모여 추진하는 경우 등 학교별로 다름. 한편 실무 수준에서 보안담당자가 구심점이 되어 시설, 연구지원, 연구처의 보안관리를 추진하는 것은 어려움”

○ (전문기관) 관리과제 수가 많기에 전문위원이 과제 관련 보안 위반 사항을 파악하기 어려운 실정이며 시스템적 접근 통한 관리 필요

- 기존 지침 활용성이 낮고 현장 피드백을 받기 어려운 구조, R&D 전주기 체계 관리는 미흡

〈참고〉 전문기관 대상 인터뷰 中

◦ “NSF의 경우 PO(사업 담당자)가 관리하는 과제수가 많지 않고 개별 연구자에 대해 면밀히 파악하고 있기에 관리감독이 가능(Human Oversight)하지만 국내의 경우 개별 사업 담당자가 관리하는 과제수가 지나치게 많고 순환직으로 연구자에 대해 잘 알지 못하는 경우가 많아 시스템적 관리에 의존할 수 밖에 없음”
◦ “대부분 전문기관의 경우 연구보안에 대해 관심을 가지고 있지 않다고 생각하면 됨”
◦ “연구보안은 규제 성격이 강하며 규제를 다루는 기관은 다양한 사건 사례를 취합해야 함. 하지만 국민의 불안감이 높아질 수 있기 때문에 모든 사례를 공개하는 것은 지양해야 함”

○ (지침적용) 연구보안을 R&D전주기와 결합하여 관계자 실행가능성을 제고하고 기관 자율성 존중, 연구환경 여건 변화 등 참고 필요

〈참고〉 민감과제 설정에 대한 현장 인터뷰 中

◦ “기술수준이 높으면서도 대규모 인력, 비용이 들어간 과제, 성과를 비공개한 과제 Pool에서 민감과제를 고를 수 있을 것으로 보이나 예외 사항도 많아 정성적인 고려도 필요”
  - 예외적으로 요소수 분야의 경우 기술 수준도 낮고 과제 규모가 크다고 말할 수 없지만 정책적으로 필요성이 높아 민감과제로 지정될 필요성이 있을 수 있음. 그 외 종자분야 또한 과제규모는 작지만 인건비가 싼 개도국으로 기술이 유출되었을 경우 국내 농업계에 파장을 불러올 수 있는 등 문제점이 있음
◦ “정량적으로 민감과제가 지정된다면 해당 기준을 피해 가기 위한 방법들이 생겨날 것임. 현재에도 보안과제로 지정되는 것을 피하고자 연구계획서를 모호하게 작성하는 연구자도 다수”
◦ “민감보안과제 선정 시 중요한 것은 ‘예측가능성’이라고 생각됨. 자유공모 시 공고문에 민감보안과제 지정이 가능하다고 사전에 알렸더라도 실제로 협약 시 민감보안과제로 지정된다면 연구자들의

불만이 커질 수 있으며 가장 파장을 적게하는 방법은 기획단계에서부터 민감보안과제가 결정되어 지정 등으로 연구개발기관을 선정하는 것임"

◦ "만약 민감과제 선정으로 성과활용과 공개가 지연된다면 젊은 교수의 경우 실적 및 승진 등에 영향을 받을 수 있는 가능성도 생길 수 있으며 불이익을 받지 않을 수 있도록 배려해 주길 바람"

〈표 3-32〉 **연구자 주요 의견 요약**

구분	대학	출연연	기업	비고
연구보안 정책인식 (방향성)	· 장기적, 자율적 접근 필요 · 사례중심, 시범사업 등으로 현장설득	· 정책추진 공감 · 관리주체 다양화로 혼선 · 감사 대비 우려	· 규제로 인식될 수 있어 조심스러운 접근 필요	· 자율적 연구보안 문화 형성 필요성 · 부처 간 역할 분담 명확화하여 현장 안내
개념/범위	· 자산 다각화, 보안개념 차별성 등 고민 · 자산유출 중 인력 이동 치명적	· 보안 범위가 방대, 범위정립 필요 · 경제적 가치 산출을 주요 자산 인식	· 과제-성과물-시설 등 보안영역을 구분하지 않음 · HR, 영업비밀 중요	· 연구자산·보안에 대한 개념 구체화
보안관리 현황	· 실험실 개방, 자유로운 IT 환경, 유학생 등 자율추구로 보안관리 미비 · 사례위주로 설명 필요함	· 그간 다수 경험과 국정원 평가 존재하여 안정적 관리	· 퇴직자, 협력 회사를 창구로 기술 유출 · 대기업은 자체 관리	· 산학연 입장이 달라 고려 필요 · 사례분석·시나리오 개발로 현장체감 개선
민감과제	· 학제별 민감 기술분야 존재 · 예측가능성 위해 초기부터 지정 필요	· 기술수준 우위 분야만 민감과제 지정	· 자체 보안등급 따라 민감분야 관리	· 연구기획부터 평가까지 연구자 예측가능성 감안한 민감과제 지정 · 민감분야에 대한 분야별 논의 필요성 존재
해외수혜신 고제도	· 김영란법 유사 · 실제 연구사항만 관리 필요	· 김영란법 유사 · 기관 규정상 상세부지침 미흡함	· 해당 사항이 많지 않다고 예단	· 제도운영 홍보 (산학연 FAQ)
성과공개/ 평가	· 연구실적평가 불이익 우려	· 연구실적평가 불이익 우려	· 성과공개 지연 시 경영 타격 우려 · 인지도 미흡	· 평가 관련 현장 논의 고려
인센티브	· 제재감시 요인 등을 적게 해야 인센티브도 작동	· 행정부담 증가시 인센티브 매력 저하	· 큰 관심 없음	· 동기부여 가능한 인센티브 부여
사고처리	· 사고 피해 입증 어려워 사고 대처 힘듦	· 기관규정 통한 처리	· 징벌적 손해배상 형식의 처벌	· 보안제재 규정 실제화 등 고민

구분	대학	출연연	기업	비고
인력관리	· 유학생 증가 추이로 지방대로 갈수록 관리 어려움	· UST외국인 근로자 장기근속으로 유출 우려 · 퇴사자 통한 유출 존재	· 실무인력 관리는 철저 · 스타인력 관리는 느슨한 편 · 퇴사자 기술 유출 다수	· 민감 과제 이상 유학생 접근 제한 행동강령 등 안내 필요 · 보안과제 연구자 인력 Pool 관리
사업화	· 중국 자본의 유혹 존재 · 창업 시 보안관리 미비	· 창업,기술이전 시 유출 가능성 있음	-	· 기존 지침에 창업분야 등 추가
교육	· 연구진실성과 결부되기에 교육 필요	· KIRD 교육이 구체성 낮음	· 교육보다는 사내 보안체계 고도화에 의존	· 현장 활용 가능한 교육콘텐츠 필요

〈표 3-33〉 **연구지원인력 및 전문기관 주요 의견 요약**

구분	연구개발기관 내 연구지원인력			전문기관	비고
	보안담당	과제관리	성과관리		
기존지침 활용성	· 미래부(2014) 지침 다수 활용	· 기존지침상 과제관리 과정 모호	· 발행기관분산 · 홍보 부족, 독자층 파악 어려움	-	· 지침 가독성, 활용성에 대한 고민
보안현황/ 규정적용	· 기존지침대비 환경변화 다수 · 규정 존재하나 담당자 부재 · 보안업무가 산재 (과제관리, 시설, 보안담당)	· 일목요연한 법정리 필요 · 국정원 실태 점검이 대학현실 미반영 · 보안위원회의 실질적 운영 미흡	-	· 내규에 따른 운영 · 운영위원회 활동 통한 지속 피드백 필요	· 법제도 준수 체크리스트 · 기관 내 거버넌스 활성화 고민
전주기 관리	· 보안 업무 관련 현장 적용성 제고 필요	· 민감과제 확대 시 행정부담 우려	· 과제-성과관리 간 소통부재로 보안성과 알 수 없음	· 전략기술은 기획부터 보안 필요 · 전문위원의 관리과제가 다수, 인적 노력 한계, 시스템적 접근 필요	· 보안·민감과제 위주 R&D 전주기 관리
사고처리	· 기관 단위 책임을 지게될 시 보안담당자 피해 우려 (대부분 겸직인원)	-	-	· 별도 처분사항 부재	· 현장 기반 보안 사고 처분 사례 연구 필요

2 연구보안 체계 내실화 토론회 개최

❑ 연구보안 체계 내실화 토론회 주관('23.11.14.)을 통한 공론화 착수

○ (목적) 글로벌 R&D 활성화와 함께 국제사회가 신뢰할 수 있는 연구생태계 조성을 위해 국제표준에 맞는 연구보안 체계 내실화를 추진할 필요

○ 토론회 개요(안)

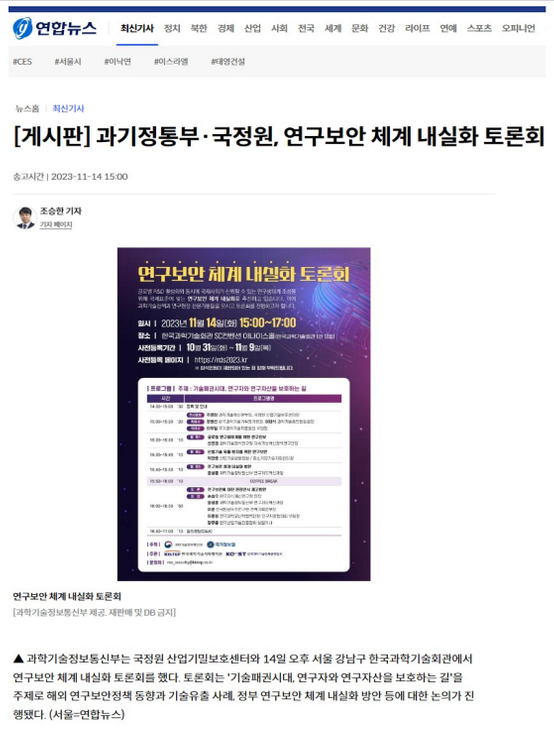
- (일시·장소) 11.14(화) 15:00~17:00 / 한국과학기술회관 12층
- (참석자) 과기정통부 과기혁신본부장, 국정원 산업기밀보호센터장, 과기자문회의 부의장, 과학기술단체총연합회장, 과학기술기획평가원장, 연구보안 전문가, 일반 연구현장 등
- (논의주제) 기술패권시대, 연구자와 연구자산을 보호하는 길

※ (주최) 과학기술정보통신부, 국가정보원 (주관) 한국과학기술기획평가원, 한국과학기술단체총연합회

〈표 3-34〉 **연구보안 체계 내실화 토론회 일정**

시간	프로그램명	발표자
14:30~15:00 ('30)	등록 및 안내	
15:00~15:20 ('20)	인사말씀	**주영창** 과기혁신본부장
		국정원 산업기밀보호센터장
	개회사	**정병선** 한국과학기술기획평가원장
		이태식 한국과학기술단체총연합회장
	격려사	**이우일** 과기자문회의 부의장
15:20~15:30 ('10)	**발제 1** : 글로벌 연구생태계를 위한 연구안보	**선인경** 과학기술정책연구원 지속가능혁신정책연구단장
15:30~15:40 ('10)	**발제 2** : 산업기술 유출 방지를 위한 연구보안	**박찬준** 산업기술보호협회 중소기업기술지킴센터장
15:40~15:50 ('10)	**발제 3** : 연구보안 체계 내실화 방안	**윤성훈** 과기정통부 연구제도혁신과장
15:50~16:00 ('10)	COFFEE BREAK	
16:00~16:50 ('50)	**패널토론** 주제 : 연구보안에 대한 현장인식 제고방안 (국외 수혜정보관리, 인센티브 확대방안 등)	**손승우** 지식재산연구원장 (좌장) (토론자: 한국항공우주연구원 이준, 전국대학교산학협력단장 이준성, 한국산업기술진흥협회 장무훈 외)
16:50~17:00 ('10)	질의응답(Q&A)	사전 및 현장 질의

토론회 자료집



연합뉴스 기사('23.11.14.)

토론회 현장

토론회 패널토의

[그림 3-2] 연구보안 체계 내실화 토론회 개최

제5절 현장 연구자 중심의 연구보안 인식조사

1 설문조사 개요

개 요

○ 현장 연구자*들을 대상으로 「체계 내실화 방안(안)」 인식 등에 대한 설문조사를 수행하였으며, 세부 사항은 다음과 같음

* 국가연구개발사업 세부과제 연구책임자(PI) 경험이 있는 연구자에 한함

- (설문기관) 한국갤럽조사연구소
- (표본크기) 유효응답 410인*

* 층화표본추출을 적용하여, 소속기관유형(산·학·연) 및 연구분야(기초과학·농생명의·공학)별 비율이 국가연구개발사업 조사·분석 결과와 일치하도록 통제

- (설문기간) 2024.1.4.~1.15.*

* 2023.12.22.~12.29. 사전설문(유효응답 40인)을 통한 설문지 정제 후 본설문 실시(사전설문 유효응답자는 본설문 응답자에서 배제)

2 응답자 특성

인구통계학적 특성

○ (연령 및 성별) 40대(50.0%)와 50대(36.6%)가 다수*이며, 남성(89.0%)이 여성(11.0%)에 비해 압도적으로 많은 비율을 차지

○ (학위 및 전공) 최종 학위 기준, 박사 학위자(63.7%)* 및 기계 전공자(18.0%)**가 가장 높은 비율을 차지

* (학위) 박사(63.7%), 석사(18.3%), 학사(18.0%)

** (전공) 기계(18.0%), 생명과학(12.7%), 전기/전자(11.5%), 보건의료(9.0%), 정보통신(8.5%), 재료(8.3%) 등

※ 학위 취득 후 평균 14.81년 경과

○ (소속 기관) 중소·중견기업(40.2%)과 대학(원)(38.3%)의 비율이 높으며, 대기업(0.5%)의 비율은 낮음*

* (소속 기관) 중소/중견기업이 40.2%, 대학(원) 38.3%, 국공립/정부출연연구기관 10.7%, 기타공공기관 5.1%, 민간연구소(사단법인, 기업부설 등) 5.1%, 대기업 0.5%

※ 근속 기간 평균 11.33년

- (근무부서 규모) 평균치 기준 Post-Doc(2.3명) 및 박사(7.3명) 등 박사급 연구원 10여 명을 포함하여 박사과정(2.6명), 석사(5.5명), 석사과정(3.5명), 학사 이하(7.8)로 구성

〈표 3-35〉 **응답자 인구학적 특성**

항목		표본수(명) (백분율)
연령대	30대 이하	29 (7.1%)
	40대	205 (50.0%)
	50대	150 (36.6%)
	60세 이상	26 (6.3%)
성별	남성	365 (89.0%)
	여성	45 (11.0%)
최종학위	학사	74 (18.0%)
	석사	75 (18.3%)
	박사	261 (63.7%)
최종학위 취득연차	5년 미만	32 (7.8%)
	5년 ~ 10년	75 (18.3%)
	10년 ~ 15년	118 (28.8%)
	15년 이상	185 (45.1%)
전공분야	기초과학	41 (10.0%)
	의생명과학·농학	115 (28.0%)
	공학	254 (62.0%)
현재 소속 기관별	학	157 (38.3%)
	연	86 (21.0%)
	산	167 (40.7%)
합계		**410 (100%)**

❑ 연구과제 수행 실적

○ (연구관리) 최근 5년간 국가R&D 과제 수행시 한국연구재단(48.8%) 및 중소기업기술정보진흥원(31.7%)등 연구관리 전문기관의 심사·평가 및 연구비 관리 경험*

* (연구관리) 연구재단(48.8%), 기정원(31.7%), 산기평(24.9%), KIAT(15.4%), 보산원(11.7%), IITP(9.8%), 에기평(8.8%), 농기평(7.3%), KAIA(6.8%), NIPA(4.9%) 등

〈표 3-36〉 **응답자 연구과제 수행실적**

주관 부처	연구관리 전문기관	경험수(건) (백분율)
과기정통부	한국연구재단(NRF)	200건 (48.8%)
	정보통신기획평가원(IITP)	40건 (9.8%)
	정보통신산업진흥원(NIPA)	20건 (4.9%)
중기부	중소기업기술정보진흥원(TIPA)	130건 (31.7%)
산업부	한국산업기술기획평가원(KEIT)	102건 (24.9%)
	한국산업기술진흥원(KIAT)	63건 (15.4%)
	한국에너지기술평가원(KETEP)	36건 (8.8%)
복지부 식약처 질병청	한국보건산업진흥원(KHIDI)	48건 (11.7%)
농식품부	농림식품기술기획평가원(IPET)	30건 (7.3%)
국토부	국토교통과학기술진흥원(KAIA)	28건 (6.8%)
…	…	…
산림청	한국임업진흥원(KOFPI)	4건 (1.0%)

○ (과제 수행) 최근 5년간 국가R&D 과제 약 2.28건, 7.69억원 규모 수행 (연평균)

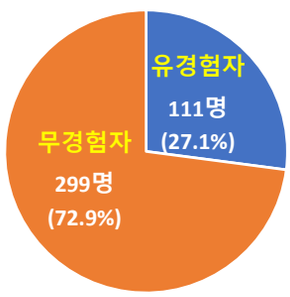
- (논문) 주저자(1.97건), 교신저자(3.26건), 공동저자(2.77건) (연평균)
- (특허) 국내 특허(1.88건), 해외 특허(0.93건) (연평균)
- (사업화) 사업화 상용화 경험(1.22건) (연평균)

〈표 3-37〉 **응답자 과제수행 실적**

구분	항목	조사 결과
과제 수행 실적	과제 건	약 2.28건/년
	과제비 규모	약 7.69억원/년
	과제 수행기간	약 3.01년
연구 실적	논문 주저자	약 1.97건/년
	논문 교신저자	약 3.26건/년
	논문 공동저자	약 2.77건/년
	국내 특허	약 1.88건/년
	국외 특허	약 0.93건/년
	상용화	약 1.22건/년

❑ 국제연구협력 경험

○ (협력 여부) 전체 응답자 410명 중 국제협력 유경험자는 111명(27.1%)이고 무경험자는 299명(72.9%) 으로 집계

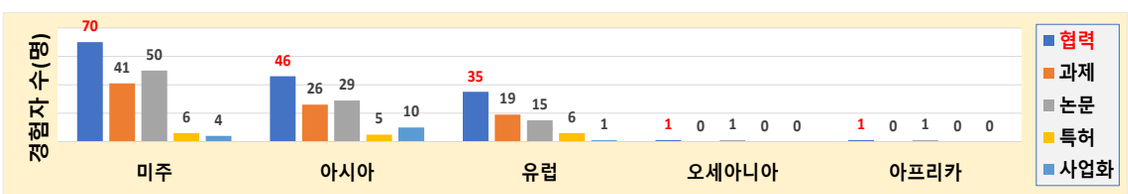


[그림 3-3] **국제연구협력 경험 여부**

〈표 3-38〉 **국제연구협력 경험 여부**

	유경험자	무경험자
협력 경험	111명 (27.1%)	299명 (72.9%)

- (협력 지역) 전체 응답자 중 미주(17.1%) 지역과 협력한 연구자가 가장 많았고 아시아(11.2%), 유럽(8.5%), 오세아니아(0.2%), 아프리카(0.2%) 순으로 나타남



[그림 3-4] **국가별 국제연구협력경험 및 실적 경험자 통계량**

〈표 3-39〉 **국가별 국제연구협력경험 및 실적 경험자 통계량**

		미주	아시아	유럽	오세아니아	아프리카
협력 경험		70명 (17.1%)	46명 (11.2%)	35명 (8.5%)	1명 (0.2%)	1명 (0.2%)
성과	과제	41명	26명	19명	0명	0명
	논문	50명	29명	15명	1명	1명
	특허	6명	5명	6명	0명	0명
	사업화	4명	10명	1명	0명	0명

❑ 응답자 최근 5년간 국제연구협력경험 상세

○ 미주 전체 응답자 중 70명(17.1%) 미국, 캐나다와 협력

〈표 3-40〉 **미주 지역 국제연구협력 과제수행 및 성과산출 경험 (최근5년)**

지역	구분	국제연구협력 과제수행 및 성과산출 경험 (최근5년)					
		평균(건)	없음(%)	1회(%)	2회(%)	3회(%)	4회(%)
미주 (미국, 캐나다 등)	과제	1.4	90.0	7.8	1.2	0.7	0.0
	논문	2.8	87.8	3.9	3.9	1.5	1.2
	특허	1.5	98.5	1.2	0.0	0.0	0.2
	사업화	1.0	99.0	1.0	0.0	0.0	0.0

○ 아시아 전체 응답자 중 46명(11.2%)의 응답자가 중국, 일본, 동남아시아 등과 협력

※ 국제 연구협력 한정으로, 한국 제외

〈표 3-41〉 **아시아 국제연구협력 과제수행 및 성과산출 경험 (최근5년)**

지역	구분	국제연구협력 과제수행 및 성과산출 경험 (최근5년)					
		평균(건)	없음(%)	1회(%)	2회(%)	3회(%)	4회(%)
아시아 (중국, 일본 등)	과제	1.6	93.4	4.9	1.0	0.2	0.0
	논문	2.5	92.7	2.7	2.0	0.7	0.7
	특허	1.3	98.5	1.0	0.5	0.0	0.0
	사업화	1.5	97.3	2.2	0.2	0.0	0.0

○ 유럽 전체 응답자 중 35명(8.5%)의 응답자가 EU, 비EU 회원국 등과 협력

〈표 3-42〉 **유럽지역 국제연구협력 과제수행 및 성과산출 경험 (최근5년)**

지역	구분	국제연구협력 과제수행 및 성과산출 경험 (최근5년)					
		평균(건)	없음(%)	1회(%)	2회(%)	3회(%)	4회(%)
유럽 (EU, 비EU 등)	과제	1.4	95.4	3.2	1.2	0.2	0.0
	논문	3.5	93.9	2.4	1.2	1.0	0.2
	특허	2.0	98.5	0.7	0.2	0.2	0.2
	사업화	2.0	99.8	0.2	0.0	0.0	0.0

○ 기타 전체 응답자 중 각 1명(0.2%)씩 오세아니아 · 아프리카와 협력

〈표 3-43〉 **기타지역 국제연구협력 과제수행 및 성과산출 경험 (최근5년)**

지역	구분	국제연구협력 과제수행 및 성과산출 경험 (최근5년)					
		평균(건)	없음(%)	1회(%)	2회(%)	3회(%)	4회(%)
오세아니아	논문	2.0	99.8	0.0	0.2	0.0	0.0
아프리카 및 기타	논문	1.0	99.8	0.2	0.0	0.0	0.0

3 「체계 내실화 방안(안)」에 대한 IPA 분석 결과

❑ 개 요

○ IPA(Importance-Performance Analysis)를 활용하여 연구자 인식을 토대로 「체계 내실화 방안(안)」의 연구현장 수용도 분석

- 현장연구자 설문 결과에 근거하여 「체계 내실화 방안(안)」에서 제시한 6개 정책이슈들*을 정책 필요도와 정책대안의 만족도를 기준으로 분석

* ①국외수혜사항 신고, ②범부처 규정마련, ③보안등급 세분화, ④분류절차 명확화, ⑤보안과제연구자 보상, ⑥연구현장 인식제고

※ 각 정책이슈별 필요도와 정책대안 만족도는 7점 리커트 척도(1~7점)로 조사

❑ 분석 결과

○ 각 정책이슈를 정책대안의 만족도(x축)와 정책의 필요도(y축)에 따라 4사분면에 전개*하였으며, 사분면별 위치에 따른 해석은 다음과 같음

※ x축 및 y축 평균값을 기준으로 4사분면 구분

〈참고〉 사분면별 해석

(1사분면) 유지강화영역으로, 정책의 필요성과 정책대안의 만족도 **모두 상대적으로 높음**
☞ 현 정책대안(체계 내실화 방안(안)) **지속 유지**

(2사분면) 중점개선영역으로, 정책의 **필요성은 높으나** 정책대안의 **만족도가 상대적으로 낮음**
☞ 현 정책대안(체계 내실화 방안(안)) **빠르게 수정·보완 필요**

(3사분면) 장기개선영역으로, 정책의 필요성과 정책대안의 만족도 **모두 상대적으로 낮음**
☞ 현 정책대안(체계 내실화 방안(안)) **장기적으로 개선 필요**

(4사분면) 과잉노력영역으로, 정책의 **필요성은 낮으나** 정책대안의 **만족도가 상대적으로 높음**
☞ 현 정책대안(체계 내실화 방안(안))이 필요성에 비해 **과하게 설계된 상태**

○ (분석결과1) 전반적으로 정책 필요도*와 정책대안 만족도**가 비례

* 평균 5.14로 보통(4.00)을 상회하여 정(+)의 필요도를 나타냄 (필요하다고 인식)

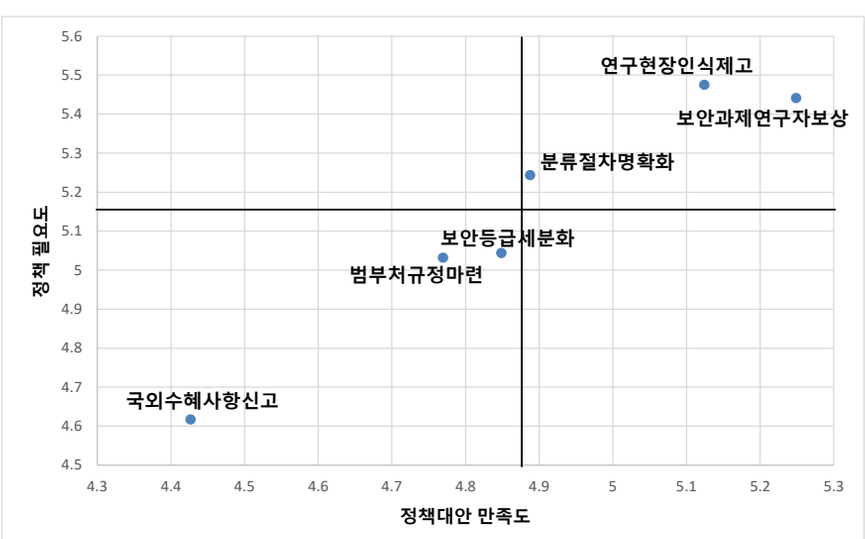
** 평균 4.88로 보통(4.00)을 상회하여 정(+)의 만족도를 나타냄 (만족스럽다고 인식)

- 필요도가 높은 이슈일수록 정책대안 만족도가 높아, 정책대안의 품질이 연구현장의 수요를 잘 반영하고 있는 것으로 해석 가능

○ (분석결과2) 총6개 이슈 중 3개 이슈*는 유지강화영역(1사분면)에 위치하고, 나머지 3개 이슈**는 장기개선영역(3사분면)에 위치하는 것으로 나타남

* 연구현장 인식제고, 보안과제연구자 보상, 분류절차 명확화

** 국외수혜사항 신고, 범부처 규정마련, 보안등급 세분화



[그림 3-5] IPA 결과 종합 (n=410)

〈표 3-44〉 IPA 결과

정책이슈	정책 필요도	정책대안 만족도	사분면 영역	해석
연구현장 인식제고	1위(5.48)	2위(5.12)	유지강화영역(1사분면)	현 정책대안 유지
보안과제연구자 보상	2위(5.44)	1위(5.25)	유지강화영역(1사분면)	현 정책대안 유지
분류절차 명확화	3위(5.24)	3위(4.89)	유지강화영역(1사분면)	현 정책대안 유지
보안등급 세분화	4위(5.04)	4위(4.85)	장기개선영역(3사분면)	현 정책대안 장기적으로 발전 필요
범부처 규정마련	5위(5.03)	5위(4.77)	장기개선영역(3사분면)	현 정책대안 장기적으로 발전 필요
국외수혜사항 신고	6위(4.62)	6위(4.43)	장기개선영역(3사분면)	현 정책대안 장기적으로 발전 필요

- 유지강화영역(1사분면)에 위치한 정책이슈는 「체계 내실화 방안(안)」에서 제시한 정책대안*의 연구자 만족도가 높아 장·단기적으로 유지가 필요한 것을 의미

* ①연구현장 인식제고, ②보안과제연구자 보상, ③분류절차 명확화 방안의 연구자 만족도가 높아 장·단기적으로 유지 필요

- 장기개선영역(2사분면)에 위치한 정책이슈는, 「체계 내실화 방안(안)」에서 제시한 정책대안* 중 장기적 관점에서 개선이 필요한 것을 의미

* ①보안등급 세분화, ②범부처 규정마련, ③국외수혜사항 신고 방안은 당장 수정·보완이 필요하지는 않으나, 향후 지속적 의견수렴 등을 통해 장기적 관점에서 발전시켜나갈 필요

- 중점개선영역(2사분면)에 위치한 정책이슈는 없으며, 이는 「체계 내실화 방안(안)」에서 제시한 정책대안 중 시급하게 수정·보완이 필요한 사항은 없는 것을 의미*

* 이는 「체계 내실화 방안(안)」이 단기적 관점에서 만족스럽게 설계된 것을 의미

- 과잉노력영역(4사분면)에 위치한 정책이슈도 없으며, 이는 「체계 내실화 방안(안)」에서 제시한 정책대안 중 필요성에 비해 과하게 설계된 정책대안 역시 없는 것을 의미*

* 이는 「체계 내실화 방안(안)」이 현장 필요성에 비례하여 효율적으로 설계된 것을 뜻함

○ (분석결과3) 국제협력 유경험자와 무경험자를 구분하여 분석한 결과유경험자는 전체 분석결과와 유사하나, 무경험자는 다소 차이를 보임

- (유경험자) 3개 이슈*는 유지강화영역에 위치하고, 나머지 3개 이슈**는 장기개선영역에 위치하는 것으로 나타나며, 이는 전체 분석결과와 동일함***

* 연구현장 인식제고, 보안과제연구자 보상, 분류절차 명확화

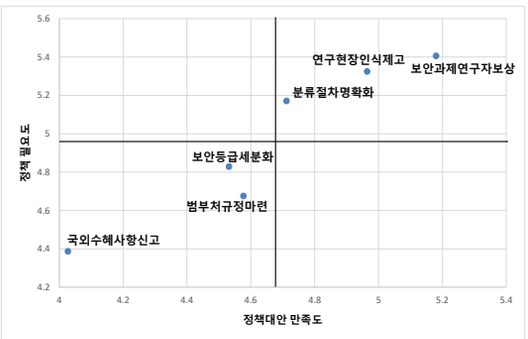
** 국외수혜사항 신고, 범부처 규정마련, 보안등급 세분화

- (무경험자) 분류절차명확화를 중점개선영역*으로, 보안등급 세분화를 과잉 노력영역**으로 인지하나, 두 이슈 모두 x축 기준선에 매우 가까운 관계로 정책대안의 상대적 만족도는 보통(평균적)이라고 보는 것이 타당

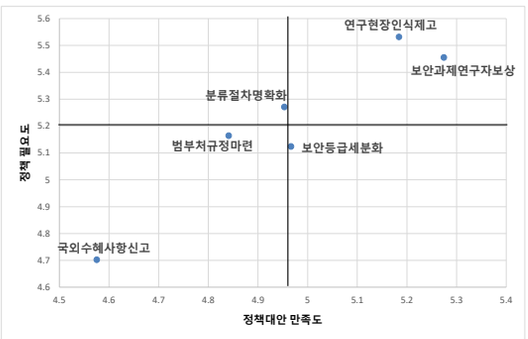
  * 시급한 개선이 필요한 영역

  ** 필요도에 비해 과잉 노력이 투입된 영역

  ※ (제언) 국제협력 유경험자와는 달리 무경험자는 분류절차명확화(안)과 보안등급 세분화(안)을 비판적 · 비효율적으로 인식할 소지가 있어 향후 추진방안에 대해 보다 상세한 설명 필요



[그림 3-6] **국제협력 유경험자 IPA 결과 (n=111)**



[그림 3-7] **국제협력 무경험자 IPA 결과 (n=299)**

❑ 결론 및 시사점

○ 전반적으로 「체계 내실화 방안(안)」이 연구현장의 필요성을 잘 반영하고 있으며, 일부 정책대안들은 우선적으로 추진하되 타 정책대안들은 장기적 관점에서 지속적 의견수렴 및 발전 필요

- (우선 추진) ①연구현장 인식 제고, ②보안과제 연구자 보상, ③분류절차 명확화 순으로 연구현장의 필요성이 높아 「체계 내실화 방안(안)」 집행 시 우선적으로 추진 필요

  ※ 특히 연구현장 인식 제고를 최우선 과업으로 추진 필요

- (장기 개선) 향후 ①보안등급 세분화, ②범부처 규정 마련, ③국외수혜사항 신고 순으로 정책대안에 대한 지속적 수정·보완 추진 필요

  ※ 충분한 숙고를 통해 장기적 관점에서 제도의 수정·보완이 필요한 바, 향후 제도개선 시 시범운영에서 나온 피드백을 적극 반영 고려할 필요

○ 국제협력 경험 유무에 따른 정책대상 세분화 고려 필요

- 6개 정책이슈의 사분면 위치가 국제협력 경험 유무에 따라 다소 차이를 보여, 향후 정책 홍보활동 등 추진 시 정책대상을 구분하여 진행하는 것이 효율적

  ※ (예) 국제협력 유경험자/무경험자를 구분하여 각 집단을 대상으로 맞춤형 홍보를 추진하는 것이 효율적이며, 예를 들어 무경험자를 대상으로 홍보·컨설팅 수행 시 분류절차명확화와 보안등급세분화 추진방안에 대해 보다 상세히 설명 필요

4 「체계 내실화 방안(안)」에 대한 컨조인트 분석 결과

※ 개략적인 분석결과 요약이며 전체 분석결과는 보고서 등으로 제출 예정

❑ 조사 개요

○ 진술선호분석* 기법 중 컨조인트 분석을 활용하여 현장연구자의 연구보안 성과관리 정책 방향에 대한 기호도를 정량적으로 분석

* 非시장적인 재화나 용역에 대한 지불의사 평가방법으로, 잠재선호를 직접 질문(예 : 얼마나 지불하시겠습니까? 다음 중 어떤 대안을 선택하시겠습니까? 등)하여 얻은 답변으로부터 해당 재화나 용역의 가치를 추정하고 계량화하는 방법의 총칭

- (설문 구성) 응답자 본인이 최근 수행한 국가R&D 과제 수행 현황을 기준선(status quo)으로 삼아, 연구보안 체계 내실화에 따른 ① 제약(의무)*과 ② 보상**을 비교·검토하여, (이러한 제약과 보상을 감안할 때) ③ 수용 가능할 수 있는 과제 규모까지 정량적으로 답변

* 성과활용 시 사전승인 필요(민감과제) 또는 금지(보안과제)

** 보안수당, 연구보안 우수 연구자(기관) 정부표창, 해외출원 불가에 대한 손실보상 등

〈표 3-45〉 **컨조인트 설문의 항목별 속성수준**

구분		속성			설명
		속성 항목	속성값	#	
과제	의무사항	A. 성과활용	① 제한없음 ② 사전승인 필요 ③ 금지	3	
	지원규모	**1. 연평균 과제비**	① 1억/년 ② 5억/년 ③ 30억 원/년	3	- 해당 과제의 연평균 과제비
		2. 기간	① 3년 ② 5년 ③ 10년	2	- 해당 과제의 수행기간
보상	연구자	가. 금전적 인센티브 (보안수당)	① 기존유지 ② 인건비 10% 수준으로 확대지급 ③ 인건비 20% 수준으로 확대지급	3	- 보안과제 수행 시 지급
		나. 정부표창	① 없음 ② 표창	2	- 보안과제 수행자에 대한 과기정통부 장관표창
		다. 손실보상	① 해외출원 불가하며 보상 없음 ② 정부연구개발비만큼 보상	2	- 보안과제 수행 시 발생하는 산출물(성과) 중, 특허를 정부가 비밀로 관리하여 해외출원을 제한받게 되는 경우 보상

- (설문 예시) 응답자는 위 항목별 속성수준에서 무작위로 조합된 가상의 과제 2개를 본인이 최근까지 수행한 과제 현황을 기준선으로 총 3개의 대안카드에 대해 선호하는 순위*를 부여

* 가장 선호하는 대안이 1순위, 가장 기피하는 대안이 3순위

구분	항목	귀하의 현수준	가상의 과제 A	가상의 과제 B
제약	A. 성과활용	제한없음	제한없음	금지
투입	1. 연평균 과제비	8.8억 원	5억 원/년	1억 원/년
	2. 기간	2.5년	10년	5년
보상	가. 금전적 인센티브 (보안수당)	기존 유지	인건비 10% 수준	인건비 20% 수준
	나. 유공자 정부표창	없음	없음	없음
	다. 손실보상	없음	없음	없음
선호 순위		□위	□위	□위

[그림 3-8] **컨조인트 설문의 대안카드 예시**

- (본 설문의 특징) 대안 선택 시, 응답자는 본인의 현수준을 비교분석의 잣대로 활용하므로 가상의 대안을 사용하는 컨조인트 설문의 단점을 저감하고 상대적 선호도를 보다 명확하게 할 수 있음

○ (설문조사) 국가R&D 과제 연구책임자(PI) 경험이 있는 현장연구자를 모집단으로 하고 410인에 대해 온라인 설문 유효응답 수집

※ 유효응답자의 소속기관유형(산·학·연) 및 연구분야(이학·농생명의학·공학) 비율을 모집단과 동일하게 유지(산:학:연 = 9:8:2, 이:농생명의:공 = 4:3:10, 층화표본추출법)

- (기간) 2024.1.4.~1.15.
- (설문기관) 한국갤럽조사연구소(주)

❑ 분석 결과

○ (현장연구자 반응) 설문조사에 응답한 현장연구자들은 제시한 보상수준이 무색한 수준으로 성과활용 제약에 강한 거부감을 나타냄이 확인됨

- (과제규모 무관) 응답자들은 연구보안 체계 내실화 제도 도입에 따른 성과활용과 보상에 방점을 두고 있으며, 결과적으로 수행하는 과제의 규모(예산, 기간)에 크게 개의치 않는 양상

※ 추정결과에서 성과활용의 상대적 중요도(partworth)는 전체의 0.2% 수준에 불과

- (성과활용 제약 민감) 응답자들은 보안등급에 따른 성과 활용 금지에 격렬하게 반발하는 것으로 나타났으며, 상대적으로 1/3 수준이나 승인 후 활용 가능한 경우에 대해서도 반발이 심한 것으로 나타남

※ 추정결과에서 성과활용의 상대적 중요도는 전체의 85%여에 달해 현장연구자들이 국가R&D과제의 성과활용 여지에 중점을 두고 있음을 확인 가능

- (보상 수용성 확인) 응답자들은 정부표창과 연구비 보상 등 인센티브 제도에 대해서는 대체로 우호적인 편이나, 보안수당 제도에 대해서는 별다른 메리트로 받아들이지 않는 것으로 조사됨

※ 추정결과에서 보상의 상대적 중요도는 전체의 15% 미만이나, 대부분 연구비보상과 정부표창에 집중되어 있으며 인건비의 일부를 인센티브로 지급받는 보안수당에 대해서는 사실상 관심이 없는 것으로 조사됨

〈표 3-46〉 **설문조사 중 컨조인트 설문결과 요약**

항목		단위	계수 추정결과*	상대적 중요도	지불의사비용 (WTP)**
성과 활용	승인후 활용가능	여부(1/0)	-0.7209***	14.0%	-36.0
	활용 금지	여부(1/0)	-2.0113***	71.2%	-100.6
과제규모	(연간)정부연구비	억원/년	0.02000***	0.0560%	
	수행기간	년	0.02403	0.127%	1.2
보상	보안수당	인건비%	0.05139***	0.139%	2.6
	정부표창	여부(1/0)	0.5867***	6.44%	29.3
	(정부)연구비보상	여부(1/0)	0.3075***	8.04%	15.4

* 유의수준 1%에서 유의함을 *** 로 표기

** Willingness-to-pay : 해당 항목 단위별로 얻기 위해 지불하고자 하고자 하는 비용

○ (시사점) 정책홍보 필요성 및 정책설계 시 착안점이 식별되므로, 지속적으로 현장연구자들의 이해를 돕는 홍보 방안의 도입과 현장연구자들이 선호하는 인센티브 유형에 대한 정책 집중 필요

- (제도 홍보 지속 필요) 보안등급별 성과활용 제약에 관한 사항을 곡해하지 않도록 충분한 홍보 지속 필요

※ 현장연구자들이 연구보안 체계 내실화를 규제 강화로 인식하는 경향이 재확인된 만큼 보안등급별 제약사항에 대한 다각적인 홍보방안 마련 필요

※ 보안등급별 성과활용 제약수준에 대한 문구 조정 등 인지적 측면에서 연구자 친화적인 접근 방안 마련 필요

- (인센티브) 현장연구자에게 직접 체감 가능한 정책수단의 선호도가 입증됨을 감안한 보상방안 고려 필요성 시사

※ 정부표창과 연구비보상 방안의 구체화 및 홍보 등 연구의지(동기부여)에 부정적인 영향은 지양하면서 제도의 취지를 살릴 수 있는 정책수단 고안 필요

제6절 연구보안 현장지침 작성방향 및 구성(안)

1 현장지침 작성방향

▣ 연구보안 체계 내실화('23.9.22) 방안 안건의 충실한 현장 구현
- 연구보안의 개념·관점에 대한 상세 안내
- 보안등급·연구개발기관 주체를 고려한 보안조치

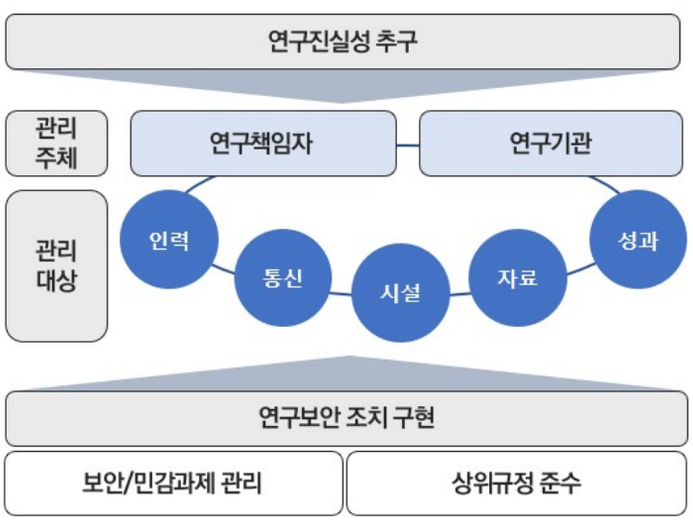
▣ 연구현장의 자율적 규범준수를 위한 자가 진단도구 제공

❑ 연구보안의 개념·관점 재정립

○ (개념범위) 보호의 근간이 되는 연구자산 정의·보호범위를 명확화하며 연구보안의 개념을 구체적으로 안내

○ (예방관점) 사후규제에 집중하는 산업보안과 달리 보안사고 예방을 위한 절차 준수와 기준 제시

※ 연구보안에서 절차는 단순 절차가 아닌 실질적 연구보안 규범 형성 실체



[그림 3-9] **연구보안 개념에 대한 안내 예시**

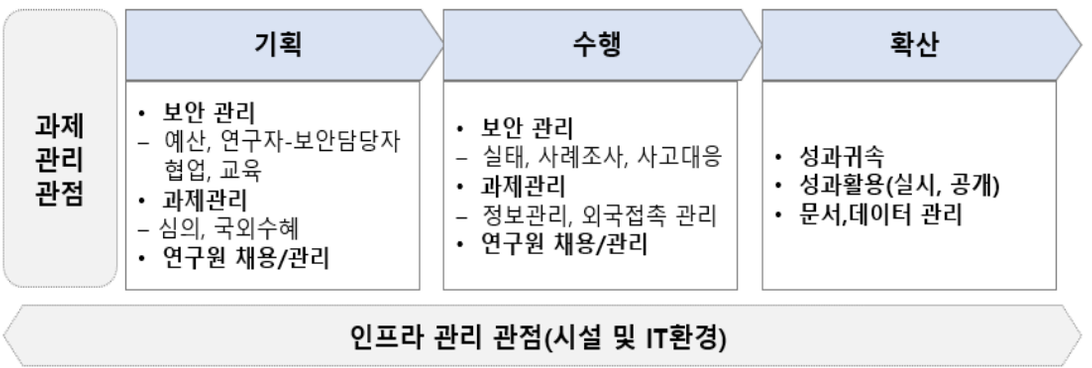
❑ 보안등급·연구개발기관 주체(산·학·연)를 고려한 보안조치

○ (관리영역) R&D 전주기 관점에서 보안영역 및 과제등급 별 차별화된 보안 조치를 안내하여 현장 적용성을 제고

- (보안영역) 연구보안 주요 영역*에 대한 연구현장 준수사항

* 참여연구원 관리, 성과물·기술이전, 정보통신망 관리, 시설보안 관리, 실태점검
(기존 지침 대비 연구원, 사업화, 데이터 관리 영역 등에 대한 강조)

- (과제등급) 3단계 분류(보안·민감·일반과제) 대한 정의 및 기준 설명, 보안 관리 활동 권고를 위한 방안



[그림 3-10] **R&D 전주기 별 연구보안 영역 추진체계 예시**

○ (주체) 산학연의 연구보안 위험인식, 규정순응 정도, 보안 조치 필요사항이 상이하므로 주체 입장을 고려해 실행 가능성을 높일 필요

❑ 자율적 규범준수를 위한 자가 진단도구 제공

○ (구성가독성) 이해관계자의 이해를 돕기 위하여 주요 항목 별 '기본원칙-주요내용-실행지침' 순서로 상세 설명

○ (체크리스트) 기관 차원에서 연구보안 자율적 규범 준수를 유도하고 보안 수준을 자가 진단·측정하는 도구 제공

- (수준진단) 연구기관이 스스로 현재 수준과 취약한 부분을 파악할 수 있는 지표를 제공하여 연구보안 리스크를 자가 점검

※ 원칙-실행지침을 체크리스트로 구현 또는 핵심적 영역만 체크

- (절차준수) 관련 안건·법을 종합 정리하여 연구개발기관의 충실한 제도준수 지원

[참고] **본문구성 예시**

3.1 연구결과물 관리

과제등급		
모든과제	민감과제	보안과제
○		

기관유형		
대학(학)	연구소(연)	기업(산)
	O	

원칙 (법소개 또는 행동 지침 구성)

- [연구개발기관] 보안과제에서 산출되는 문서, 자료, 데이터에 대한 보안 등급을 정해야 한다.
- [연구개발기관] 보안과제 산출물의 보안 등급을 정하는 절차를 마련해야 한다.
- [연구자] 연구자는 보안 등급 추진 절차 시 내부위원회에 출석해 보안등급을 부여해야 한다.
- [연구자] 연구자는 보안등급 확정 시 등급에 따른 내부 지침 등을 따라야 한다.

내용

- 보안과제에서 산출되는 문서, 자료, 데이터는 다음과 같은 내용을 말한다.
- 보안 등급을 정하는 절차 마련에는 아래와 같은 내용이 포함되어야 한다.

실행항목

1. 연구개발 성과물의 보안등급 분류 기준 수립
   ....관련내용...
2. 연구성과물의 보안등급 부여 절차 수립
3. 보안등급별 보안 대책 수립

❑ 현장지침 사례구성

○ 기존 보안사고 사례 분석을 기반으로 연구기관 또는 연구자들이 즉시 활용 가능 상황별 시나리오 개발 등을 검토(24.3월 이후~)

- 주요 보안영역 또는 R&D 전주기 단계에 대한 '유형 별 시나리오'를 제작하고 '시나리오 구성*' 체계화

* 사건개요-결론 및 조치-쟁점사항

※ 실제 연구보안 사고사례를 수집·참고하되 사례 공개 시에는 과학계에 대한 국민 신뢰도 저하가 우려되므로 지양하고 가상의 시나리오 각색

- 산업보안과 구별되는 연구보안의 특징을 연구자들이 쉽게 이해할 수 있도록 연구자 인터뷰·해외 사례 등 참고해 가상의 스토리텔링 작업 추진

※ '24년 하반기, 현장에서 즉시 활용 가능한 상황별 시나리오 개발

〈참고〉 외국인 유학생이 허가 없이 자료를 유출하는 현장 가상 사례

(사례1)

◦ 지방국립대 반도체 연구실 박사과정의 A 외국인 학생은 연구실에서 보안과제를 포함하여 여러 과제를 동시에 연구하고 있다. 외국인의 경우 보안과제 허가를 사전 승인받아야 하지만 상황이 워낙 바쁘다 보니 어느 순간 자연스럽게 보안과제 일부를 맡아서 하게 되었다.

◦ A학생은 본국에서 석사과정을 마쳤는데 한국에서 연구를 하다 보니 본국의 친구들에게 참고 자료를 보내주면 좋을 것 같아서 실험 데이터의 일부를 정리해서 보내주었다. 그 과정에서 부지불식간에 보안과제에서 창출된 연구데이터 일부를 전송하게 되었다.

◦ 담당 교수는 우연히 실험실에 들렀다가 이 장면을 목격하게 되었고 결국 해당 학생을 연구실에서 내보내기로 하였다.

연구보안 Check Point	- 외국인이 보안과제에 참여할 경우 중앙행정기관장의 사전 승인이 필요하다. - 외국인 연구자가 보안과제에 참여할 시에는 제한된 업무범위 설정이 중요하다. - 보안과제 관련 성과의 경우 데이터 유출 제한 방침이 필요하다.

(사례2)

◦ 지방국립대 반도체 연구실의 B교수는 보안과제를 수행하면서 학생들에게도 보안관리에 대해 강조하고 있으며 외국인 학생들은 연구에서 배제하고 있다. 또한 성과를 외부에 비공개 하려고 노력하였다.

◦ 그러던 어느 날 중국의 C교수로부터 B교수의 보안과제 연구성과와 관련하여 천인계획에 함께 참여하자는 메일을 받게 되었다. 성과를 비공개하고 있었는데 C교수가 B교수의 보안과제 연구성과에 대해 알고 있어서 큰 충격을 받았다.

◦ B교수는 연구실 내에 중국 공산당원 학생들에 대해 의심했지만 20명 가까이 되는 중국 학생들 중 누가 연구성과 정보를 유출한 것인지 알 수가 없었다. 연구실 내 컴퓨터에 비밀번호가 몇 년간 동일해서 사실상 누구라도 마음먹으면 정보에 접근할 수 있는데 이 사실을 간과한 것이었다.

연구보안 Check Point	- 보안과제 관련 데이터 이용 내역의 기록 및 보관, 시스템 구축 등이 중요하다. - 보안과제 수행 연구실의 경우 보호구역 별도 설정과 출입제한이 필요하다. - 보안과제 관련 업무용 컴퓨터의 경우 강화된 암호 조치가 필요하다.

〈참고〉 실험실 창업 기업이 해외 기업의 투자를 받은 경우에 대한 현장 가상 사례

◦ S대의 A교수는 국가연구개발사업의 장기적인 지원으로 기초연구의 상업화 단계에 이르게 되었다. 사업성이 있다고 판단하여 S대로부터 기술을 양도받고 정부의 지원을 받아 창업도 하게 되었다. 하지만 사업 과정은 연구와 매우 달라 경영이 쉽지 않았고 사업을 진행할수록 끊임없이 돈이 들어 포기하고 싶어졌다. 또한 국내 시장이 예상보다 빠르게 성장하지 않아 미래를 장담하기 어려웠다.

◦ 마침 중국의 C기업이 M&A를 제시해 왔고 A교수는 협상을 진행하기로 마음먹었다. 그 과정에서 국정원, 연구개발특구 등의 관계자가 찾아와 해당 기술이 보안과제, 국가핵심기술에 해당하는지 판정하게 되었고 판정 결과 해당 사항이 없어 M&A 허가가 떨어졌다.

◦ 국가연구개발사업에서 투자된 기술을 M&A 해도 되는지 마음에 걸렸지만 A교수의 기술은 국내 시장이 형성되지 않은 단계라 선택지가 없다는 결론을 내렸다. A교수는 기술료를 통해 정부에 보답해야겠다고 생각했다.

연구보안 Check Point	- 연구개발기관 연구보안심의회의는 실험실 창업 허가 시, 창업 대상기술의 보안 및 민감과제 해당 여부에 대해 검토해야 한다. - 연구개발기관은 보안·민감과제 관련 실험실 창업자에게 '국가연구개발사업 보안대책'에 대한 관리 현황 자료 제출을 요구할 수 있다. - 해외수출 시 보안과제·전략물자·국가핵심기술 해당 여부를 확인하고 중앙행정기관장의 허가를 받아야 한다.

〈참고〉 현직자가 자산을 유출하는 현장 가상 사례

◦ D교수는 학계에서 촉망받는 학자로 다양한 국가연구개발과제를 수행하고 있다. 연구연가 중 기회가 찾아서 해외 유수 대학의 우수학자로 초빙받게 되었고 생활비와 급여 등을 지원받을 수 있게 되었다.
◦ D 교수는 해외 저명한 학자들의 그룹에 참여하고 조언을 구하기 위해서 그간에 쌓은 지식과 데이터를 해외 학자들에게 발표하기 시작했다. 그 중 일부는 국가전략기술과 관련성이 높은 사안도 있긴 했지만 관련하여 별도의 신고 절차가 있는지 몰랐기 때문에 D교수는 꺼림직한 마음에도 불구하고 규정을 어기는 것은 아니라고 생각했다.

연구보안 Check Point	- 국가전략기술 관련 해외에서 정보 공개 요청을 받은 경우 이에 대해 연구개발기관은 전문기관 등에 알려야 한다. - 민감과제 수행 재직자의 해외 출장 시 연구개발기관의 연구보안심의회의는 발표 자료 등을 사전 검토해야 한다.

〈참고〉 퇴사자가 자산을 유출하는 현장 가상 사례

◦ E출연연에 오랫동안 근무해 온 B씨는 오랫동안 원자로에 대한 기술을 연구하다가 은퇴 시점에 현지에 기술을 수출하는 업무를 도맡아 했다. 국가 수출 역군이라 인정도 받고 개도국의 기반을 다지는 일이라서 뿌듯하기도 하였다.
◦ 은퇴 후 해외 한 국가에서 이전에 수출한 원자로 운용과 관련하여 일자리를 제안받았다. B씨 입장에서는 은퇴 후 생계가 막막해지기도 하였고 국가적으로 권장된 수출이라 일자리 제안을 받아들이는 데에는 크게 망설임이 없었다.
◦ B씨는 A출연연 퇴사 시에 관련 영업비밀을 유출하지 않기로 서약하였고 데이터도 최대한 활용하지 않기로 교육받았다. 하지만 해외 원자로 운용이 긴급하기도 하고 또 머릿속에 이미 지득한 지식이 많아 B씨는 자연스럽게 해외에 지식을 이전하게 되었다.

연구보안 Check Point	- 연구개발기관은 민감과제 수행 퇴사자의 해외 이직에 대한 정보를 관리해야 한다. - 연구개발기관 등은 퇴사자가 보안기술 유출 관련 상담과 교육을 받을 수 있도록 해야 한다.

〈참고〉 보안과제 관련 기술이전 가상 현장 가상 사례

◦ 중견규모인 K기업 관계자는 국방 연관 분야의 보안과제를 수행하게 되었다. 해당 성과와 관련하여 국가적으로 수출 붐이 일어나고 있기에 K기업도 해당 보안과제에서 창출된 성과를 수출할 수 있을 것이라는 희망이 생겼다.
◦ 이에 전문기관에 수출을 진행해도 되는지 문의했지만, 전문기관 담당자로부터 중앙부처의 답을 기다리고 있다는 답이 돌아왔다. 알고 보니 중앙부처에서 위원회를 열어서 수출 여부를 승인해야 하는 상황이었는데 위원회 개최가 계속 지연되는 중이었다.
◦ 답답한 K기업 관계자는 전략물자원의 검증 시스템을 이용하여서 수출 가능 여부를 자가 확인하였다. 이 결과를 가지고 전문기관과 부처에 재차 문의한 결과 그제야 일부 성과에 대해서만 수출이 가능할 것이라는 답변을 겨우 듣게 되었고 제품화 계획을 일부 축소하여 수출을 준비하고 있다.

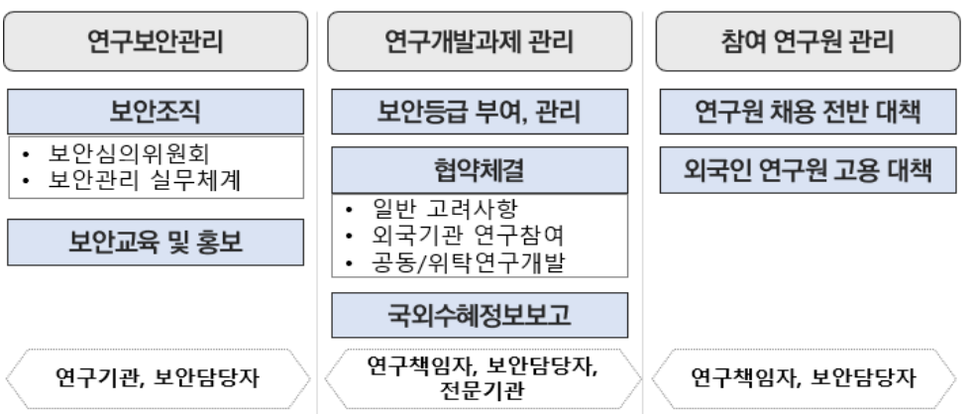
연구보안 Check Point	- 보안과제 기술이전 시 중앙행정기관 장의 사전 승인이 필요하다. ※ 참고) 보안과제가 대외무역법에 따른 전략물자이자 산업기술보호법에 따른 국가핵심기술에 해당하는 경우 '산업기술보호법, 대외무역법'을 모두 따라야만 행정처분 대상이 되지 않음[14]

14) 법제처 법령해석 사례(2020-09-17),

2 현장지침 목차설계(안)

○ (서론) ① 연구보안 체계 내실화 방안 배경 및 취지, ② 지침의 목적 및 위상, 관련 법령 체계, ③ 연구보안 개념 및 범위, 보안조치 영역, 용어 등 소개

○ (연구보안과 연구개발과제의 준비)는 과제선정~협약을 말하며, ① 연구기관 입장에서 준비해야 하는 연구보안 관리 전반 ② 연구책임자가 숙지해야 할 보안과제 관리 필요사항 안내



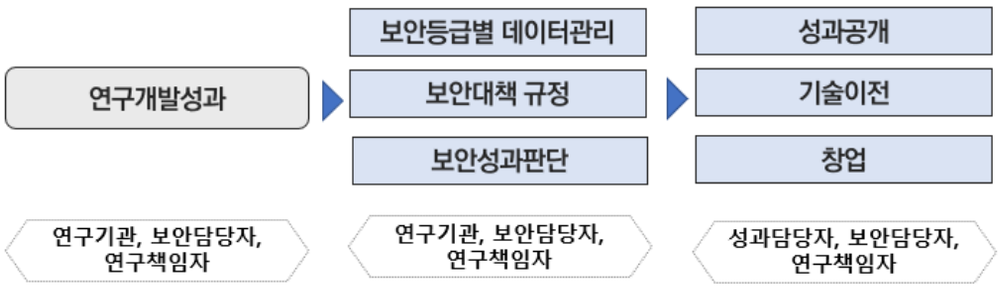
[그림 3-11] **연구보안과 연구개발과제의 준비 구성**

○ (연구보안과 연구개발과제의 수행) ① 연구기관의 실태점검, 사고대응 등 보안 관리 전반 ② 연구책임자가 고려해야 하는 외국인 접촉, 데이터 관리 등

[그림 3-12] **연구보안과 연구개발과제 수행 구성**

https://moleg.go.kr/lawinfo/nwLwAnInfo.mo?mid=a10106020000&cs_seq=424259&currentPage=1&keyField=&keyWord=&sort=date

○ (연구보안 연구개발과제의 성과 · 기술이전 관리) 연구개발 성과를 성과공개·기술이전·창업 등으로 연계할 시에 지켜야 할 보안관련 사항



[그림 3-13] **연구보안 연구개발과제의 성과 · 기술이전 관리 구성**

○ (연구인프라 보안관리) 연구기관의 물리적·정보통신 보안 추진 시 고려해야 할 사안

[그림 3-14] **연구개발기관의 연구인프라 보안 구성**

〈표 3-47〉 **연구보안 현장지침 구성(안)**

장	절	목	보안등급
I. 서론	1-1 연구보안 체계 내실화 방안		공통
	1-2 관계 법령 체계와 제도개선 방향		
	1-3 유관 지침 및 본 지침과의 관계		
	1-4 용어 정의		
II. 과제 수행 준비 : 과제 선정부터 협약까지	2-1 관계 법령 및 규정 체계		
	2-2 연구보안 관리	① 연구보안심의회의 구성 및 운영	
		② 연구보안 관리 실무체계	
		③ 보안관리 규정 교육 및 보안서약	
	2-3 연구개발과제 관리	① 보안등급 부여체계	
		② 보안등급 관리체계	
		③ 국제협력 조치사항	
		④ 국외수혜정보 보고체계	
		⑤ 협약 체결 시 기타 고려사항	등급별 상이
		⑥ 공동연구개발 및 위탁연구개발 시 절차	등급별 상이

장	절	목	보안등급
	2-4 참여연구원 관리	① 참여연구원의 참여 가능 범위	등급별 상이
		② 채용 시 유의사항	등급별 상이
		③ 외국인 참여연구원 관리	등급별 상이
III. 과제의 수행	3-1 관계 법령 및 규정 체계		공통
	3-2 연구보안 관리	① 보안관리 실태점검	등급별 상이
		② 보안사고 대응 및 조치	등급별 상이
		③ 규정별 사례 관리	공통
	3-3 연구개발과제 수행 관리	① 해외에서 외국기관·외국인과 접촉하는 경우	등급별 상이
		② 국내에서 외국기관·외국인과 접촉하는 경우	등급별 상이
		③ 문서 및 데이터 관리(연구노트, 데이터 등)	등급별 상이
	3-4 참여연구원 관리	① 재직, 계약 갱신 및 퇴직	등급별 상이
		② 일시 출입자 및 파견자 관리	등급별 상이
		③ 외국인 참여연구원 관리	등급별 상이
IV. 과제의 성과 및 기술이전	4-1 관계 법령 및 규정 체계		공통
	4-2 연구보안 관리	① 연구개발성과의 귀속·이전	등급별 상이
		② 연구개발성과의 활용	등급별 상이
		③ 연구개발성과 문서 및 데이터 관리	등급별 상이
V. 연구개발기관의 연구인프라 보안관리	5-1 시설관리	① 접근통제	등급별 상이
		② 주요시설 및 시설물 관리	등급별 상이
		③ 보호구역 별도 관리	등급별 상이
	5-2 정보통신망 관리	① 업무용 정보기기 및 저장매체 시스템 관리	공통
		② 정보시스템 데이터 관리	등급별 상이
		③ 통신망 네트워크 관리	등급별 상이

3 연구보안 현장지침 작성 추진체계

❑ (전문가협업) 주요 보안영역*의 전문가 그룹과 현장지침 상세 내용 집필에 대한 협업 추진

* 참여연구원 관리, 성과물·기술이전, 정보통신망 관리, 시설보안 관리

- 보안영역 별 실무진 및 연구자가 원고 초안 작성

※ 보안 우수·사고 사례에 취합과 시나리오 개발 등 참여

❑ (현장자문위) 현장 연구자·과제관리·보안담당자·전문기관 관련자로 구성된 자문그룹이 현장지침 원고에 대한 감수 추진

※ (예정) 1차('24.2월), 2차(6월). 3차(11월)

❑ (시범운영) 특정 실험실 대상 보안영역 및 보안등급별 보안조치를 시범 적용하여 가이드라인 고도화

○ 시범대상 실험실에 연구현장 가이드라인·보안등급 분류 지침을 적용하여 실효성이 떨어지는 부분, 반영 필요사항 도출

〈표 3-48〉 **연구보안 현장지침 작성체계**

제7절 연구보안 시범운영 및 국외수혜정보보고 제도설계

❑ 국외수혜정보보고 제도설계

○ 국가연구개발과제를 수행하는 연구책임자(공동·위탁연구개발기관의 책임자 포함)는 국외로부터 지원받는 행정적 · 재정적 지원 및 노무 또는 자문 등을 제공하고 받는 대가에 관한 사항을 관계 중앙행정기관의 장에게 보고하여야 함*

* 영 시행일('24.2.6.) 이후 ①공고된 공모 과제 또는 ②지정 등 공모 외의 방법으로 연구개발기관이 지정된 과제의 연구개발계획서 제출을 요청하는 경우부터 적용

※ 법 제3조에 따라 법 제9조부터 제18조까지의 사항을 적용받지 않는 국가연구개발사업은 보고 대상에서 제외

국가연구개발혁신법 시행령 제9조제3항

제9조(연구개발과제 및 연구개발기관의 공모 절차) ③ 연구개발계획서에는 다음 각 호의 사항이 포함돼야 한다.

8. 연구책임자가 연구개발기간 동안 외국의 정부 · 기관 · 단체 등으로부터 받는 행정적 · 재정적 지원이나 노무 또는 자문 등을 제공하고 받는 대가에 관한 사항

- (보고 주체) 국가 R&D과제를 수행 중이거나 수행하고자 하는 주관 연구개발기관의 연구책임자 및 공동·위탁 연구개발기관의 책임자*

  * 협약 변경 시에도 해당

- (보고 대상) 외국의 정부 · 기관 · 단체 등으로부터 받는 행정적 · 재정적 지원*이나 노무 또는 자문 등을 제공하고 받는 대가**

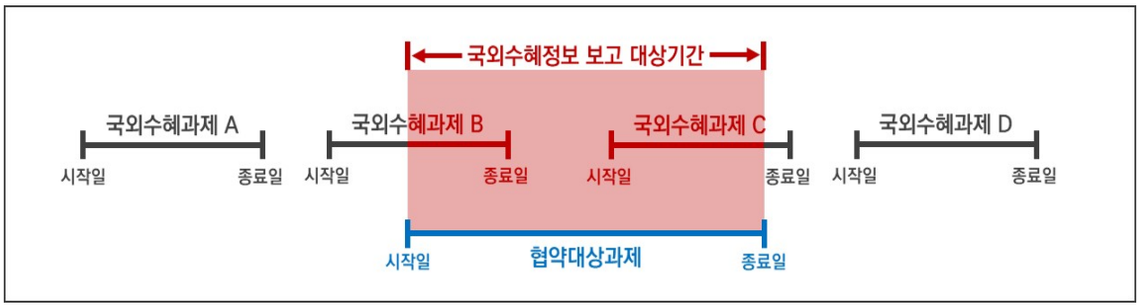
  * 연구과제(용역)·인력·장비·시설 지원 등을 포함하며, 지원이 확정되지는 않았으나 협약 시점에서 지원이 예상되는 사항(외국과제 신청 현황 등)도 포함

  ** 각종 컨설팅(자문) · 세미나 · 강연 · 겸직 등 포함. 단, 순수 학술활동(강의, 학회참석 · 발표, 논문 · 학술서적 기고 등)의 경우 동일 기관으로부터 연간 미화 5,000달러(USD)를 초과하는 경우에만 보고

※ 연구과제(용역)의 경우, 신청·선정·지정·협약·계약 등을 포함하며 단순 문의·제안·논의 및 종료사항은 미포함

- (보고 범위) 협약 대상 국가R&D과제의 수행기간과 중첩되는 행정적 · 재정적 및 노무 또는 자문 등에 관한 사항만 보고

※ 아래 예시 그림의 경우, 협약 대상 국가R&D과제 기간과 중첩이 있는(있을 예정인) 국외수혜과제 B와 C가 보고 대상이며, A와 D는 기간 중첩이 없어 보고 대상이 아님



[그림 3-15] **국외수혜정보 보고 대상 기간 범위(예시)**

- (보고 시기·방법) 국가 R&D과제 협약 시 제출하는 연구개발계획서* 내 국외 수혜현황 정보 보고를 포함하고, 과제 수행 중 발생일로부터 30일 이내(권고) 이를 현행화(IRIS 활용**)

  * 국가연구개발혁신법 시행규칙 별지 제1호서식 연구개발계획서(협약용) 중 '연구책임자 등 현황'

  ** 연구자책임자가 IRIS 국가연구자정보시스템(NRI)에 국외수혜정보를 입력 및 관리하고, 이를 협약 시 활용

- (보고 항목) 지원·지급 출처, 사유, 기간, 내용, 연구개발과제와의 관련 여부

〈표 3-49〉 **국가R&D과제(과제수행기간 : '24.2.15.~'27.2.14.) 연구책임자의 국외수혜정보 보고 예시**

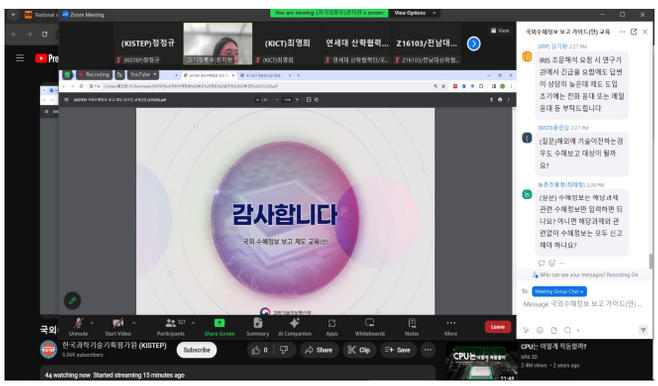
보고 시기	지원 · 지급 출처 (외국정부/ 기관/단체 등)	지원 · 지급 사유 (연구 수행/노무 · 자문 제공 내역 등)	지원 · 지급 기간	지원 · 지급 내용 (인력/시설/ 보수 등)	연구개발과제와의 관련 여부
협약시	○○국 ○○기업	○○○에 관한 연구 수행	'22.4.1~'24.3.31.	총 5만불(USD)	연구개발과제 선행연구
	○○국 ○○대학	○○○ 연구인력 지원	'24.3.1~'25.2.28.	박사급 2명	연구개발과제 참여예정
수행중	○○국 ○○연구소	○○○ 주제로 강연	'24.5.1.	1,000만원	연구개발과제 무관

❑ 국외수혜정보보고 교육('23.12.13, '23.12.20) 지원을 통한 「내실화 방안」 시범운영 저변 확대

○ 「국외 수혜정보 보고제도」의 원활한 제도 착근을 위해 부처(전문기관) 및 연구개발기관 연구관리부서 관계자 대상 온오프라인 교육·홍보 추진

〈표 3-50〉 **국외수혜정보보고 교육추진**

구분	교육 상세내용
일시	• '23.12.13(수) KIRD 교육 • '23.12.20일(수) 온라인 교육(ZOOM 및 유튜브중계)
대상자	• 부처, 전문기관 및 연구개발기관 연구관리부서 담당자



[그림 3-16] **국외수혜정보제도 온라인 교육 현황**

제8절 소결

❑ 연구보안 체계 내실화 방안을 현장에서 실천하기 위한 필드매뉴얼의 작성 방향을 수립하고 연구보안 시범운영 정책설계 등에 시사점을 도출하기 위한 기초 연구를 진행함

○ 선행문헌(산업·연구보안)에 대한 연구를 통해 기존 지침의 구조적 한계를 식별함과 동시에 향후 R&D 전주기 관점과 결합한 연구보안 관점 제시에 대한 방향성을 설정함

- (기존 문헌 한계) 법제도 준수, 5대 보안영역 등 보안관리에 매몰되거나 개념화 미비, 지침 사용자 범위 적절성 미흡 등으로 인해 효용성이 제한적
- (시사점) 연구보안 이행 사항을 R&D전주기와 결합하여 연구보안 지침 접근성을 제고하고 정책 현장착근 및 연구현장 적용 실질성, 연구자 가독성 등을 고려할 필요성 확인

※ 개념과 범위 구체화*, 구체성 및 가독성 제고 필요

* 연구보안·연구윤리·산업보안 구분, 보안주체(기관유형)별 보안조치 등 차별화

○ 연구보안 현장지침의 주 독자층인 연구자, 연구보안 업무 관계자를 대상으로 심층 인터뷰를 도출함

- (연구자) 연구보안 정책 본격화에 공감하나 연구자가 위축되지 않도록 연구계를 설득해 가며 장기적·순차적 도입 필요

※ (공통) 치명적인 자산 유출은 인력이동이며 연구보안 관리 주체는 결국 일선 연구자이기에 관련자의 연구진실성 교육 필요

※ (대학) 학제 별 개방성 수준이 달라 일괄 적용하기보다 학자들의 합의가 이뤄지는 분야 위주 관리 필요

※ (출연연) 보안정책 도입과 운영 경험이 상대적으로 많아 제도 거부장벽 자체는 낮은 편이나, 분야별 국제공동연구 특성 등을 고려할 필요

※ (기업) 민감·보안과제 성과공개 지연 시 '미래가치 실현'을 포함한 보상 검토 등이 결부되어 기업 연구개발활동의 위축을 초래하지 않도록 고려 필요

- (전문기관) 관리과제 수가 많아 전문위원 수준에서 개별적으로 과제 관련 보안 위반 사항을 파악하기 어려운 실정을 감안한 시스템적 접근 통한 관리 필요

○ 이해관계자 의견을 종합한 연구보안 현장지침 작성방향 제시

- (개념·관점 정립) 보호의 근간이 되는 연구자산 정의·보호범위를 명확화하며 연구보안의 개념을 구체적으로 안내
- (전주기 관점 도입) R&D 전주기 관점의 보안영역 및 과제등급 별 차별화를 통한 활용도 제고

- (기관유형 및 보안등급 차별화) 연구개발기관 유형(산학연), 보안등급(보안/민감/일반)별 현장지침 수립 및 자가진단도구 제시를 통해 활용도 향상

❑ 현장 연구자 중심의 연구보안 인식조사

- (개요) 국가연구개발사업 세부과제 연구책임자 경험이 있는 연구자 410인을 대상으로 설문 추진함(2024.1.4.~1.15)
- IPA(Importance-Performance Analysis) 등 분석방법론 활용한 결과 '연구현장 인식제고, 보안과제 연구자보상, 분류절차 명확화 등에 대한 정책집행 우선순위가 높음
- 컨조인트 분석결과 연구자는 성과활용제약에 거부감이 많은 것으로 나타남

❑ 연구보안 시범운영 사전협의 실무지원을 통한 연구현장 환류 체계 기초 확보

- (실무협의) 후보기관의 참여의사 확인 및 후보기관 유형 특정을 통한 현장지침 우선적용 가능성에 따른 환류체계 구축
- (국외수혜정보보고) 제도의 기초를 설계하고 관련 교육 추진

❑ 향후 일정

- 현장지침 초안 마련 : '24.3월
- 시범사업 운영 환류 및 현장지침 초판 발간 : '24.3월~12월
- 현장지침 홍보 확산 : '24.11월~'25.2월

제4장 보안등급 분류체계 설계를 위한 탐색적 연구

제1절 연구의 배경

❑ 보안등급 세분화* 제도화에 대비한 연구관리 전문기관 중심의 등급분류 가이드 수요제기

○ (필요성) 「연구보안 체계 내실화 방안」 및 「세계를 선도하는 글로벌 R&D 추진 전략」 세부 추진방안 이행 및 연구현장 착근을 위해서는 보안등급 세분화* 제도 도입에 대비한 보안등급 분류기준의 가이드라인 수립 필요

* 「연구보안 체계 내실화 방안」('23.9), 「세계를 선도하는 글로벌 R&D 추진 전략」('23.11) 공히 기존의 보안과제와 일반과제 사이에 민감과제 등급 신설 추진을 명시

○ (목적) 연구관리 전문기관이 「연구보안 체계 내실화 방안」 의 취지를 충족하면서 국가R&D과제 보안등급을 효율적이고 탄력적으로 분류할 수 있는 가이드 제시

1 선행연구

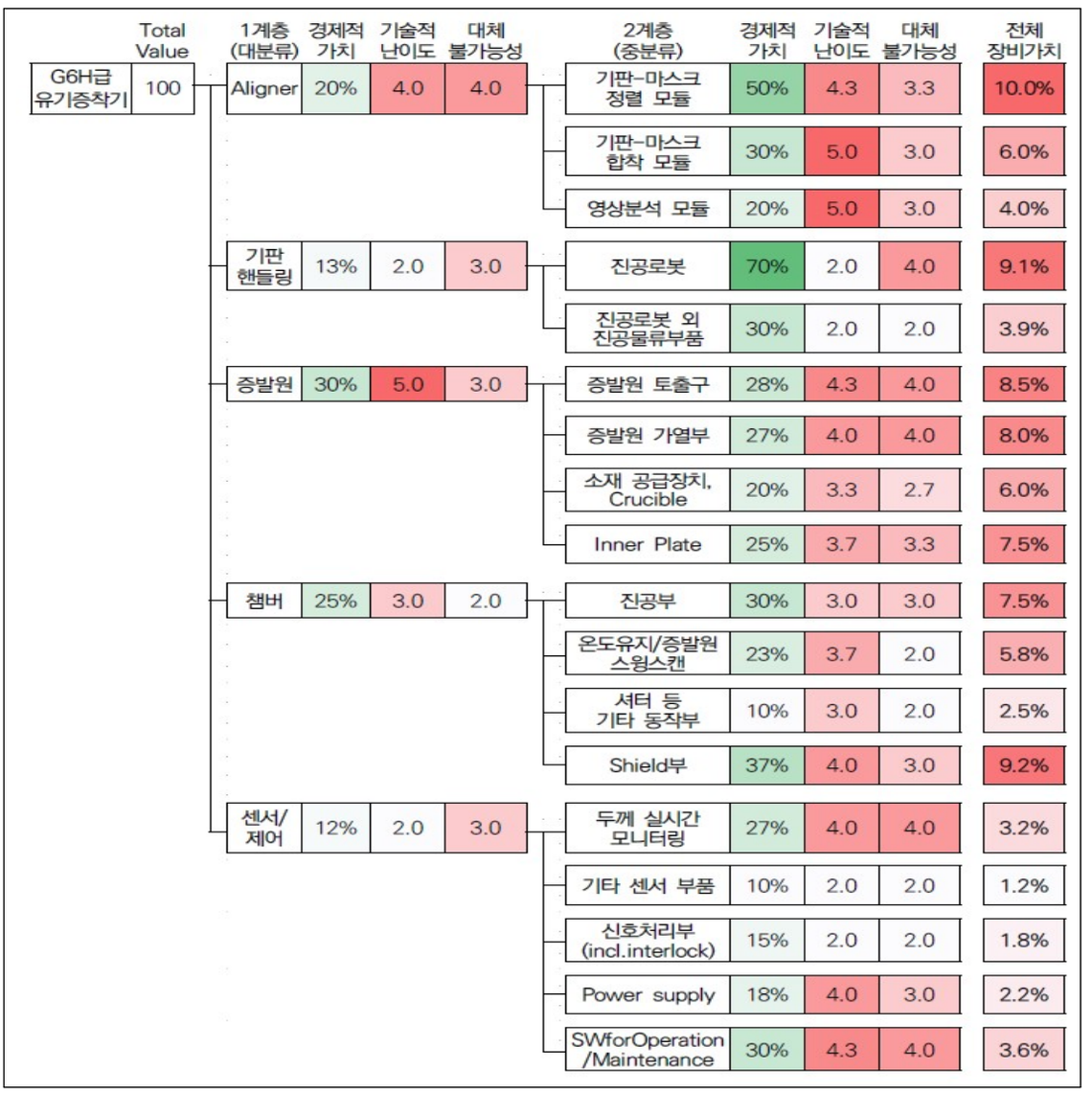
❑ 국가안보와 직결되는 소재·부품·장비(소부장) 산업기술 가치평가 항목 검토(조용래 외, 2020)

○ 조용래 외(2020)는 국가 산업기술 안보와 국민경제를 대변하는 속성을 아래와 같이 조작적으로 정의하고 계량점수와 전문가 5점척도 평가를 종합하여 우리나라 산업 특히 소재·부품·장비(소부장) 부문별 강점과 약점을 직관적으로 파악하는 평가체계를 제시

- (경제적 가치) 국민경제 파급효과를 시장성(시장점유율, 성장전망 등) 그리고 산업가치사슬상 가치(가격비중)가 상호 필요충분관계라는 관점에서 “경제적 가치”로 지칭
- (기술난이도) 소부장 핵심전략품목의 “기술수준”을 다르게 표현한 개념으로 산업가치사슬상 구성요소별 구현의 난이도를 기술수준으로 본 경우에 해당
- (대체불가능성) 소부장 핵심전략품목의 “대체가능성”으로 해당 산업부문 가치 사슬에서 해당 산업부문이 사라진다면 기업 또는 국가 단위에서 대체재가 존재하는지, 있다면 대체재의 수준은 어느 수준인지(바로 투입 가능한 대안인지 여부 등)를 의미

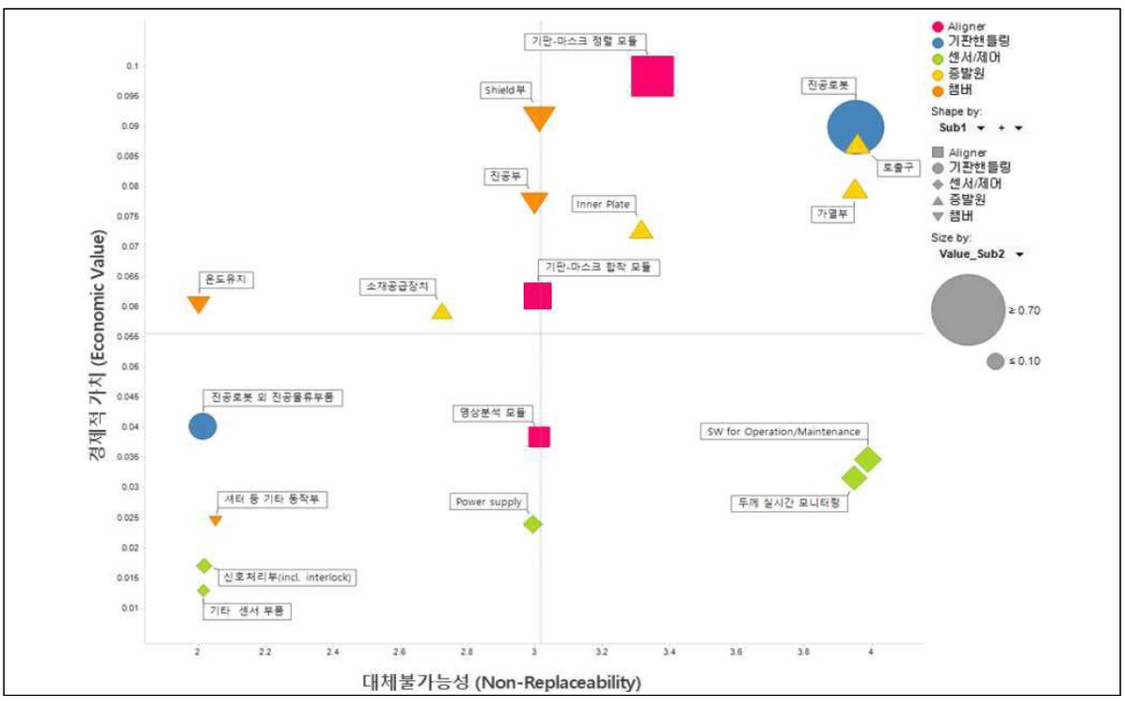
○ 평가대상 기술을 가치사슬 관점에서 계층화를 포함하여 복합적으로 구조화하고 해당 요소기술별로 상기 경제적 가치와 기술난이도, 대체불가능성을 유관 전문가들을 대상으로 FGI 평가를 수행

- (기술트리 구성 및 분석) 평가대상 기술의 가치사슬 관점 요소기술을 정의하고 구조화한 후 전문가 대상으로 FGI를 통해 요소기술별 중요도를 계량화

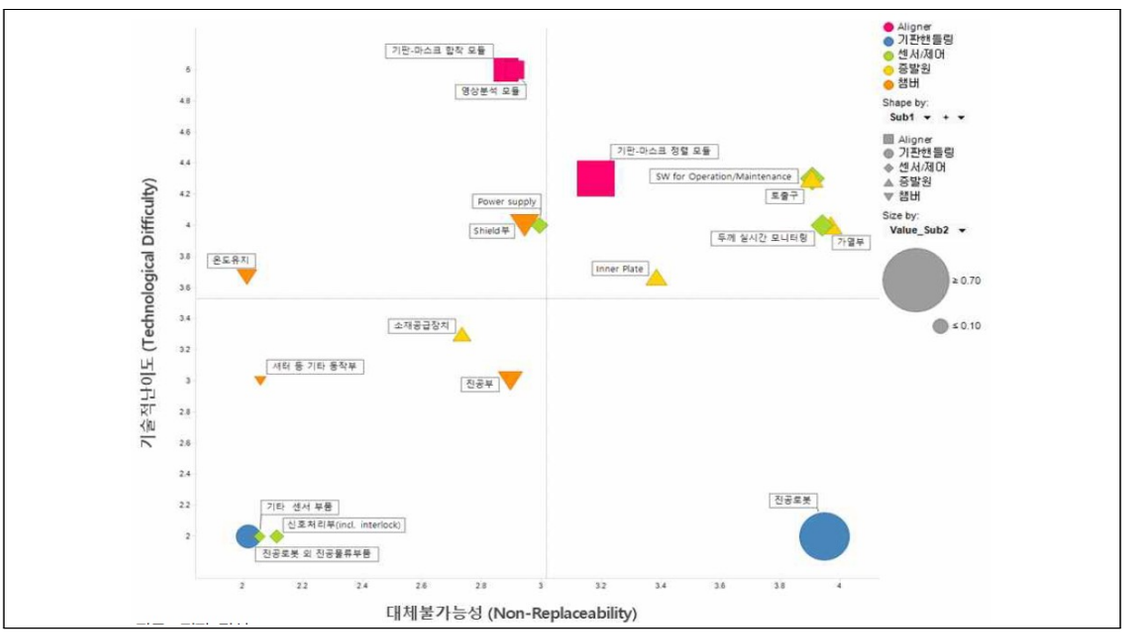


[그림 4-1] OLED용 대면적 증착기 가치사슬 요소기술별 지표 정량화의 예시(조용래 외, 2020)

- (사분면 분석) 기술난이도 대 경제적 가치, 대체불가능성 대 기술난이도를 사분면 기준으로 분석하여 각각 우리나라가 자체적으로 보유한 핵심역량과 외국의 제재조치에 가장 취약한 기술을 식별



[그림 4-2] 요소기술별 대체불가능성 대 경제적 가치 식별의 예(조용래 외, 2020)



[그림 4-3] 요소기술별 대체불가능성 대 기술적 난이도 식별의 예(조용래 외, 2020)

※ 각 1분면에서 우상단 끝으로 갈수록 중요도가 높음을 의미(조용래 외, 2020)

○ (의의) 조용래 외(2020)가 제안한 분석방법은 평가 대상기술의 산업적 가치와 리스크를 정량적으로 식별할 수 있다는 장점을 지니나, 근본적으로 과제분석이 아닌 기술분석이라는 범주적 한계를 지님

- (장점) 기술트리 분석을 활용한 요소기술의 식별과 전문가집단의 활용을 통해 평가 결과가 상대적으로 객관적이고 계량화된 분석 결과를 제시할 수 있음
- (단점) 분석 결과가 평가에 참여한 전문가집단의 구성에 좌우되는 경향을 지니며, 기술분류 분석에 적절할 수 있으나 평가 대상이 상대적으로 현저하게 미시적인 과제분석에 적용하기에 어려움이 존재

※ 기술 단위 분석에 참여 가능한 전문가집단의 모집단 크기와 과제 단위 평가에 참여 가능한 전문가집단의 모집단 크기 자체가 현저하게 차이가 존재함

❑ 국가연구개발과제의 보안등급 평가기준 검토(나원철·장항배, 2020)

○ 나원철·장항배(2020)는 내용타당성 기반으로 평가항목을 도출하고 선정된 평가항목별 AHP를 통해 가중치를 부여하는 2단계 전문가 설문 기반의 과제별 보안등급 부여방안을 제시

- (평가항목의 도출) 연구진이 도출한 평가항목 후보군에 대해 설문을 통한 내용타당성* 검증을 실시하고 구조방정식 기반의 요인별 상관분석을 통해 일관성과 신뢰성까지 검정하여 평가항목을 도출

* Content validity : 평가대상을 고려하여 제시한 평가항목의 적절성과 대표성의 수준을 대변하는 개념(강동석·유시형, 2009)

- (평가항목별 가중치 도출) 평가항목의 도출과 별도의 전문가집단 대상 AHP 설문 및 분석을 통해 앞 단계에서 도출한 평가항목별 평가 가중치를 산출

※ 과제기초정보 5%, 과제수행유형 10%, 기술성 50%, 사업성(경제성) 35% 가량(Ibid.)

- (평가항목별 평가기준 제시) 평가항목별 점수를 합산하여 과제별 보안등급을 판정하는 체계를 제시

※ 예를 들어, 과제 기초정보에는 과제비와 과제수행기간을 구간별로 차등 점수를 부여하며, 기술성과 사업성(경제성)은 평가위원별 점수를 5점 척도를 활용하여 점수화하는 방안을 제시

○ (의의) 나원철·장항배(2020)가 제안한 방법은 과제정보와 평가자들의 5점척도 기반 점수체계를 복합적으로 활용한 입체성에서 의의를 지닌다고 볼 수 있으나, 제안한 점수화 방안의 근거가 없어 임의적인 한계를 지님

평가기준		평균	표준편차	요인분석				신뢰도
평가요인	평가항목			요인적재량	공통성	고유값	분산설명	Crobach 알파
1. 과제 기초 정보	1-1 연구 규모	3.55	1.15	0.979	0.993	2.01	14.36	0.991
	1-2 연구 기간	3.6	1.15	0.976	0.991			
2. 과제 수행 유형	2-1 연구 수행 주체	3.86	0.75	0.894	0.891	2.68	19.143	0.939
	2-2 연구 개발 단계	3.93	0.78	0.905	0.886			
	2-3 공동 연구	3.83	0.76	0.952	0.922			
3. 과제 기술성	3-1 필요성	3.98	0.98	0.944	0.907	4.566	32.617	0.975
	3-2 구체성	3.95	1.01	0.931	0.914			
	3-3 혁신성	3.98	0.92	0.937	0.899			
	3-4 차별성	4.02	0.87	0.941	0.908			
	3-5 지식재산권 창출 가능성	4.07	0.97	0.962	0.972			
4. 과제 사업성	4-1 경제성	3.86	1.03	0.94	0.938	3.718	26.558	0.972
	4-2 시장성	3.81	1.04	0.95	0.939			
	4-3 기대효과	3.74	1.04	0.934	0.916			
	4-4 파급효과	3.81	1	0.923	0.898			

[그림 4-4] 국가연구개발과제 보안등급 평가기준의 도출 예(나원철·장항배, 2020)

국가연구개발과제 보안등급 평가기준 점수화			
점수화 시점	보안등급 평가요인	보안등급 평가항목	점수화 방안
과제 공고 시 점수화	1. 과제 기초 정보 (5점)	1-1 연구 규모 (1점)	- 2억 미만 : 0점 - 2억 이상 : 1점
		1-2 연구 기간 (4점)	- 2년 미만 : 1점 - 2년에서 4년 : 2점 - 4년 이상 : 4점
	2. 과제 수행 유형 (10점)	2-1 연구 수행 주체 (2점)	- 대기업 : 2점 - 정부연구소 : 1.6점 - 대학 : 1.2점 - 중소기업 : 0.8점 - 중견기업 : 0.4점
		2-2 연구 개발 단계 (1.5점)	- 기초연구 : 0.5점 - 응용연구 : 1점 - 개발연구 : 1.5점
		2-3 공동 연구 (6.5점)	- 공동연구 : 6.5점 - 단독연구 : 0점
과제 선정 평가 시 점수화	3. 과제 기술성 (50점)	3-1 필요성 (5.5점)	- 국가연구개발과제 선정평가 시 점수화 방식은 각 선정평가 평가항목마다 5개 척도로 책정(매우 우수 ~ 우수 ~ 보통 ~불량 ~ 매우 불량) - 기존 5개 척도를 본 연구의 평가항목 보안등급 점수로 환산하여 판정하고자 함
		3-2 구체성 (4점)	
		3-3 혁신성 (10.5점)	
		3-4 차별성 (10점)	
		3-5 지식재산권 창출 가능성 (20점)	
	4. 과제 사업성 (35점)	4-1 경제성 (13점)	
		4-2 시장성 (13점)	
		4-3 기대효과 (4.5점)	
		4-4 파급효과 (4.5점)	

[그림 4-5] 국가연구개발과제 보안등급 산정체계 방안(나원철·장항배, 2020)

2 보안등급의 판단기준

❑ (현행) 「국가연구개발혁신법」은 보안과제를 정의하고, 해당 법 및 동법 시행령에서 보안과제의 분류·관리 및 기관의 책임범위를 명시

〈표 4-1〉 **국가연구개발혁신법 제21조(국가연구개발사업 등의 보안)**

제21조(국가연구개발사업 등의 보안) ① 관계 중앙행정기관의 장 및 연구개발기관의 장은 소관 국가연구개발사업 및 연구개발과제와 관련하여 연구개발성과 등 대통령령으로 정하는 중요 정보가 유출되지 아니하도록 보안대책을 수립·시행하여야 한다.

② 중앙행정기관의 장은 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 보안이 필요한 연구개발과제를 보안과제로 분류할 수 있다.

③ 제2항에 따라 보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는 보안관리 조치를 하여야 한다.
⋮

⑥ 제1항에 따른 보안대책의 내용, 제2항에 따른 보안과제의 분류 기준, 제3항에 따른 보안관리 실태 점검 및 조치 사항은 대통령령으로 정한다

[시행 2023. 9. 22.] [법률 제19235호, 2023. 3. 21., 일부개정]

〈표 4-2〉 **국가연구개발혁신법 시행령 제45조(연구개발과제에 대한 보안과제의 분류)**

제45조(연구개발과제에 대한 보안과제의 분류) ① 중앙행정기관의 장은 다음 각 호의 연구개발과제를 법 제21조제2항에 따른 보안과제(이하 "보안과제"라 한다)로 분류할 수 있다.

1. 「방위사업법」 제3조제1호에 따른 방위력개선사업과 관련된 연구개발과제

2. 다음 각 목의 어느 하나에 해당하는 기술과 관련된 연구개발과제
   가. 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술
   나. 중앙행정기관의 장이 보호의 필요성이 있다고 인정하는 미래핵심기술
   다. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호에 따른 국가핵심기술
   라. 「대외무역법」 제19조제1항에 따른 수출허가 등 제한이 필요한 기술

② 중앙행정기관의 장은 제1항 각 호의 어느 하나에 해당하는 연구개발과제를 법 제9조제4항 본문에 따라 연구개발기관을 공모하기 전까지 보안과제로 분류해야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 연구개발기관이 선정된 이후에 지체 없이 보안과제로 분류해야 한다.
⋮

③ 중앙행정기관의 장은 제10조에 따라 선정된 연구개발기관이 외국에 소재한 기관·단체 또는 외국인과 공동으로 연구를 수행하는 경우에는 해당 연구개발과제가 「대외무역법」 제20조제2항에 따라 전략물자에 해당하는지에 관한 판정을 신청하여 그 결과에 따라 그 연구개발과제를 보안과제로 분류할 수 있다.

[시행 2023. 12. 14.] [대통령령 제33899호, 2023. 12. 5., 타법개정]

〈표 4-3〉 **국가연구개발사업 보안대책 제3조(연구개발과제 보안과제 분류)**

제3조(연구개발과제 보안과제 분류) ① 중앙행정기관의 장은 법 제21조제2항에 따라 소관 연구개발과제를 보안과제로 지정·해제하는 등 분류가 필요할 때에는 검토를 위하여 해당 연구개발 분야 및 보안업무 전문가 등으로 구성된 보안과제분류위원회를 설치하여 운영하여야 한다. 단, 다음 각 호에 해당하는 경우 보안과제분류위원회의 검토를 생략한다.
1. 연구개발과제 발굴을 위한 사전 기획을 통해 보안과제로 분류될 수 있는 경우
2. 자유공모 과제에 대하여 연구개발과제평가단을 통해 보안과제로 분류될 수 있는 경우
3. 다른 법령에 의한 절차를 통해 보안과제로 분류될 수 있는 경우

② 연구개발기관의 장은 수행 예정이거나 수행하고 있는 보안과제에 대하여 재분류가 필요하다고 판단하는 경우에는 보안과제분류위원회에 보안과제 여부를 재분류해줄 것을 요청할 수 있다.

③ 연구개발기관의 장은 수행 예정이거나 수행하고 있는 연구개발과제에 대하여 보안과제로 분류가 필요하다고 판단되는 경우에 보안과제분류위원회에 보안과제로 분류해 줄 것을 요청할 수 있다
⋮

[시행 2023. 11. 20.] [과학기술정보통신부고시 제2023-39호, 2023. 11. 20., 일부개정]

❑ (제도개선 방향) 「연구보안 체계 내실화 방안」은 보안과제 등급을 보안과제와 민감과제로 분리하고 관리수준 등을 이원화하는 제도개선 방향을 제시

〈표 4-4〉 **연구보안 체계 내실화 방안이 제시한 보안등급 세분화 방안(안)**

구분		보안과제	민감과제(가칭)	일반과제
정의(안)		국가안보와 관련되거나, 국민경제에 중대한 영향을 미칠 수 있는 과제	유출시기술적·재산적 가치의 상당한 손실이 예상되어 국민경제에 영향을 미칠 수 있는 과제	보안과제·민감과제로 분류되지 않은 과제
보안 조치 (예시)	국외수혜 정보	보고(공통 사항)		
	외국접촉	사전승인 (3년 이내 수행자)	사후보고 (1년 이내 수행자)	-
	외국인 참여 공동연구	사전보고·승인	-	-

* 「연구보안 체계 내실화 방안(안)」(국과위 심의회의 본회의, '23.9.26.)

○ (판단기준) 사례지정에 가까운 현행 법령과 달리, 제도개선(안)은 국가안보와 국민경제 영향으로 판단기준을 명시

〈표 4-5〉 **「연구보안 체계 내실화 방안」의 보안등급 세분화 주요인자 구분**

구분	보안과제	민감과제(가칭)	일반과제
국가안보	유관	무관	무관
국민경제 영향	영향 중대	영향 있음	무관

- (국가안보) 유관/무관으로 명시되어 있어 상대적으로 명료한 판정이 가능하나, “국가안보”의 범주가 명시되어 있지 않고* 구체적인 사례제시 역시 부재**한 한계가 존재

* 종래에 군사안보와 필요충분조건으로 인식되던 것과 달리(Grizold, 1994; Hameiri and Jones, 2013) 최근에는 경제안보, 환경안보 등 개념 확대 경향(이효영, 2022)

** 현행 혁신법 시행령은 국가핵심기술(산업기술보호법) 및 EL(대외무역법) 등 보안과제의 대상범위를 한정하고 범주 이해를 돕는 사례를 제45조제1항2목에서 명시

- (국민경제) “국민경제” 자체가 포괄적인 개념이며, 개별 연구개발 과제의 국민경제 영향을 수준화하여 판단하기 어려운 한계

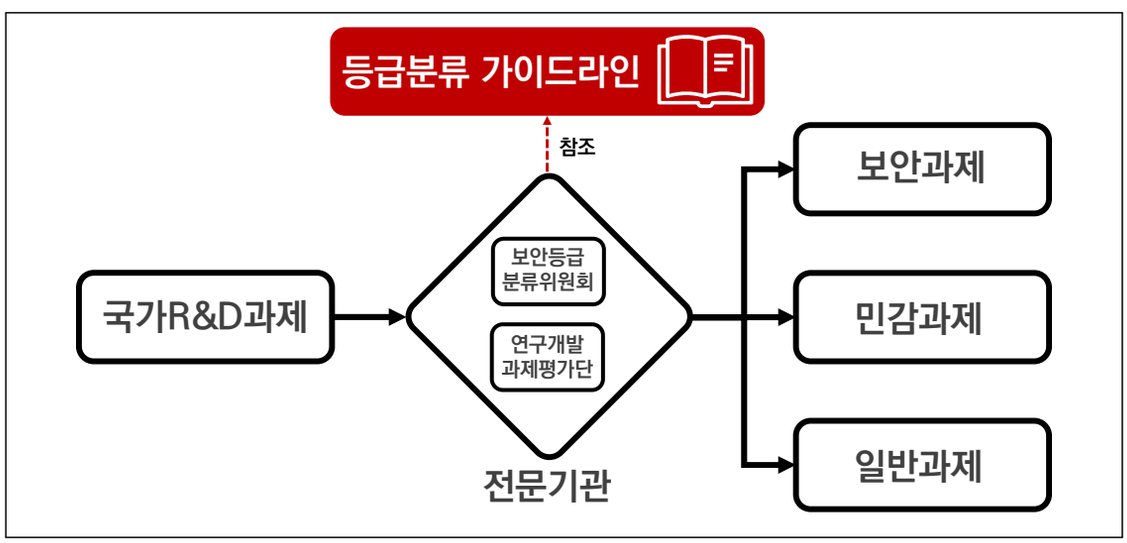
제2절 보안등급 분류 가이드 수립 방향(안)

1 보안등급 분류 가이드의 범주와 기능 정의

❑ 보안등급 분류 가이드의 역할과 활용 범위

○ (역할) 연구관리 전문기관의 자율적 판단에 활용 가능한 고려사항 제시

- (레퍼런스) 등급분류 가이드라인은 보안등급 판단의 참고자료(reference)로, 과제별 보안등급은 전문기관이 최종 판정



[그림 4-6] 국가R&D과제 보안등급 분류체계에서 등급분류 가이드라인의 역할 도식

○ (활용) 국가R&D과제 생애주기 전 단계에서 연구현장의 수시 참조용

- (관계기관) 연구기관, 연구관리 전문기관 등
- (관계자) 국가R&D 수행 현장연구자, 국가R&D 과제 기획자 및 과제평가* 참여자(선정평가 포함), 연구개발지원인력 및 보안등급 관리자** 등

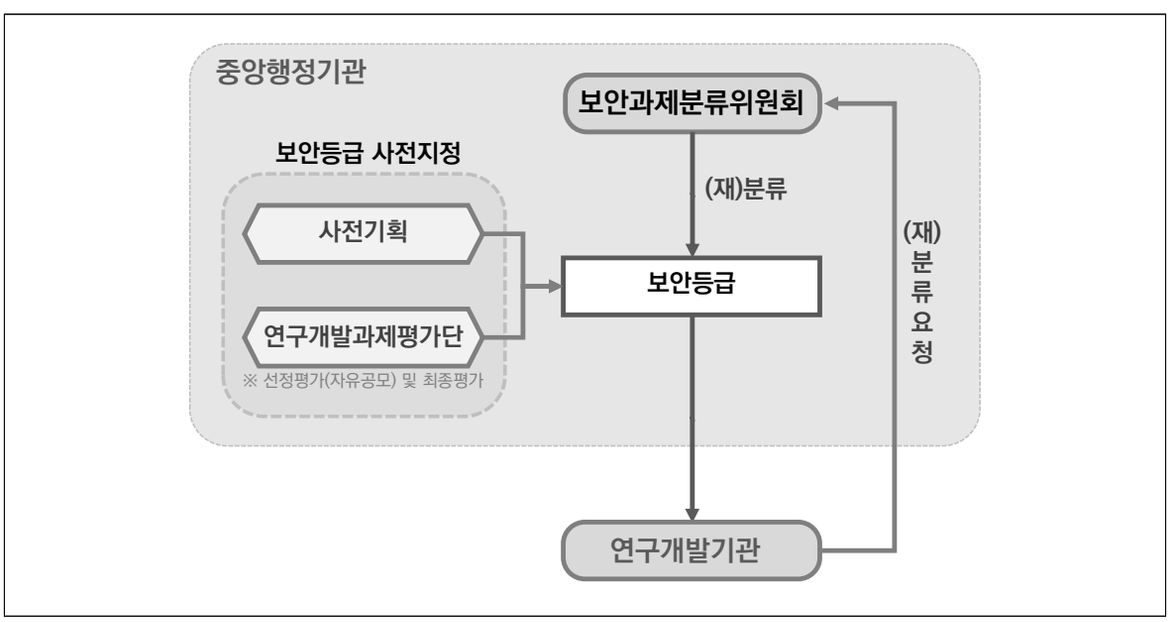
* 「국가연구개발혁신법」의 연구개발과제평가단

** 연구기관 및 전문기관 소속의 연구개발지원인력(연구보안 또는 연구관리 담당자 포함) 및 「국가연구개발사업 보안대책」에 따른 보안등급분류위원회 등 포함

❑ 보안등급 분류 절차 해설 제공

○ (등급분류 의사결정 체계) 현행 제도 상 과제별 보안등급분류에 관한 최상위 의사결정기구인 보안과제분류위원회 중심의 분류체계 명시

- (기준) 보안과제분류위원회(중앙행정기관)를 과제별 보안등급 분류 주체
- (예외) 사전기획 시 지정, 연구개발과제평가단의 지정 시 등



[그림 4-7] 국가R&D과제 보안등급 분류 의사결정 체계

❑ 전주기적 대응체계 수립 추진

○ 「국가연구개발사업 보안대책」 등 현행 제도와 제도개선 방향을 복합적으로 감안하여 기획 단계부터 활용 가능한 체계 수립을 모색

2 과제 생애주기별 보안등급 분류 방안(안)

❑ 선정평가 이전과 선정평가 후속조치를 구분하는 단계별 접근 채택

○ 기획연구진의 자의적인 판단과 자유공모형 사업의 보안등급 분류까지 지원하는 방안 제시

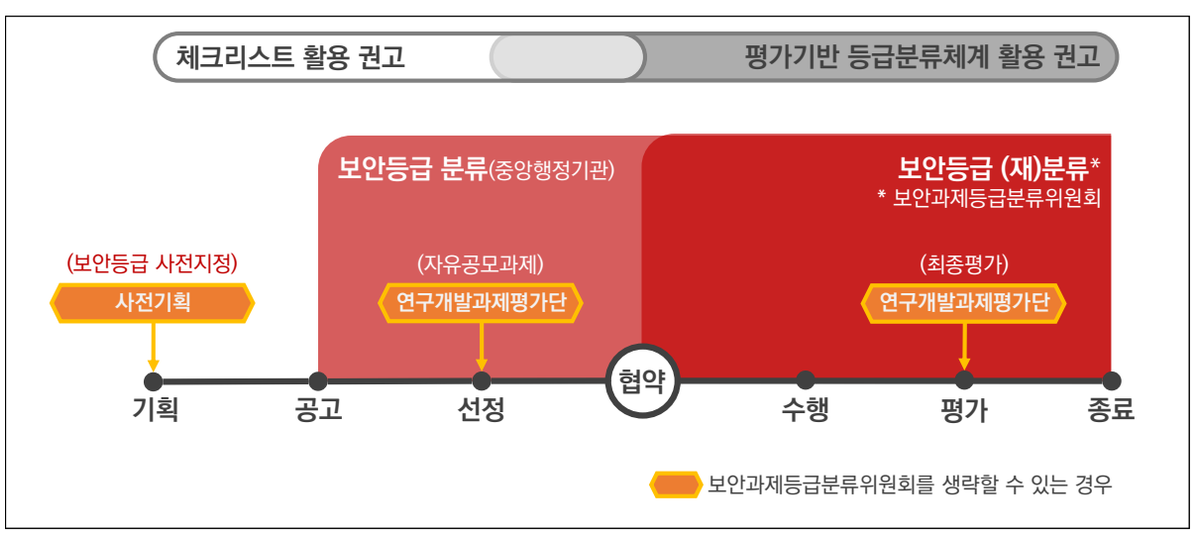
① (기획-공모 단계) 기획연구진(과제 기획 단계)과 연구개발과제평가단(선정평가 단계)은 대상 기술 및 연구활동 특성(수행 예상 기관유형별 여건 등)을 감안하여 보안등급(민감과제/보안과제)을 사전 분류*

* 현행 「국가연구개발사업 보안대책」은 사전기획 및 공모형 과제의 경우 보안등급 사전 설정으로 인해 보안등급분류위원회의 별도 검토를 생략할 수 있음을 명시(제3조제1항)

- (등급분류 가이드의 역할) 기획연구진 또는 연구개발과제평가단의 보안등급 사전 분류를 돕는 체크리스트 제공*

* 특히, 기획연구진은 수행기관을 알 수 없고 과제의 기술적 · 경제적 가치를 판단하는 데에 한계가 있으므로 보안등급의 분류에 참고할 가이드가 필요

* 국가전략기술(국가핵심기술, 국가첨단전략기술, 수출통제)로서 관리대상 기술인지에 대한 판단은 과기정통부 과학기술전략과(산업부 기술안보과, 전략물자제도과 등)의 검토 및 지정 사항을 원칙으로 함



[그림 4-8] **국가R&D과제 생애주기에서 연구보안 등급분류 및 재분류 시점**

〈표 4-6〉 **보안등급 분류 체크리스트 예시 : 산업체가 연구개발기관인 경우**

① 해당 과제정보의 유출이 해당기업 경영실적에 직접적·즉시적 악영향을 미치는가?	
설명	■ 수행기관(기업) 경영에 부정적 영향의 즉시성이 있는지를 확인하기 위한 질의 - 해당 과제 정보*가 유출되는 순간 경쟁사(또는 경쟁국)가 즉시적으로 기술 대등 또는 우위에 도달할 수 있는지 검토 - R&D 회임기간(time lag) 등으로 경쟁사(또는 경쟁국) 유출의 직접적·즉시적 영향*은 상대적으로 미흡하나, 주가 및 내부인력의 동요(이탈) 등 기업자산 또는 기업가치 하락 등 심각한 규모의 악영향이 즉각적으로 발생할 정도의 R&D과제인지 검토
주의	■ 기획연구진 등 (해당 과제 수행기업이 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 즉시적으로 기술 대등 또는 우위에 도달할 수 있는 경쟁사가 국내에 한정되는 경우, 국민경제 영향성은 부재함(일반과제로 분류됨이 적절) ■ 영업비밀로 관리 중인 기술이 아닌, 해당 국가R&D과제 수행 정보에 한함에 유의 (예) ㅇ社가 ㅁ 분야 △ 기술을 X 나노미터 목표로 '25년 1월까지 과제 수행 중 : 해당 (예) ㅇ社가 영업비밀로 관리 중인 △ 기술의 공정조건(recipe) 유출 : 미해당
② 국내외 해당 산업에서 국내기업이 지배적인 혹은 독보적인 지위를 차지하고 있는가? 외국기업과의 경쟁 수준은 치열한가?	
의미	■ 기획연구진 등 (해당 과제 수행기업이 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 국내 기업이 세계 시장을 선도하고 국외 기업과 경쟁이 치열하며 그 격차가 크지 않은 경우 과제 정보의 유출도 경제안보에 영향을 줄 수 있음 - 해당 과제 정보*가 유출되는 순간 경쟁사(또는 경쟁국)가 즉시적으로 기술 대등 또는 우위에 도달할 수 있음 ■ 세계 시장에서 국내 기업의 점유율이 낮거나, 일반적으로 해당 산업부문에서 우리나라의 기술경쟁력이 취약한 경우 추격형 기술개발에 해당되므로 보안과제나 민감과제 해당사항이 없음
주의	■ 해당 과제 정보의 유출이 경쟁사(또는 경쟁국)에 즉시적·유의미한 영향을 주어야 함 - 영업비밀로 관리 중인 기술의 유출 자체는 해당 사항이 없으나, 과제 정보의 유출이 기술을 가늠하게 만드는 경우를 고려할 필요
③ 해당 과제가 국방R&D에 해당되는가?	
의미	■ 해당 과제가 무기체계 개발 등 국방R&D 해당 여부를 검토 - 단, 핵심기술개발사업 등 해당 과제 자체는 기초연구인 경우 미해당
④ 해당 과제가 특정 국가전략기술·국가핵심기술 또는 수출통제 기술 개발인가?	
의미	■ 해당 과제가 정부가 관리하는 주요기술 또는 수출통제 대상 기술인지 검토 - 국가전략기술 중 관리대상 범주는 과학기술전략과 지정 국가전략기술 연구개발사업에 한함 - 국가핵심기술·국가첨단전략기술 및 수출통제 지정 여부는 산업부 기술안보과 및 전략물자제도과의 판단을 준용함
⑤ 해당 과제에 외국기관이 공동연구개발기관 또는 위탁연구개발기관으로 참여하는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 국내 연구개발기관만 참여하는 연구 대비 유출 가능성이 상대적으로 높음을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 외국기관의 경우 소속 국가와 기관 특성에 따라 보안관리 수준이 다양하므로 이를 복합적으로 감안할 필요

⑥ 해당 과제에 외국인 참여연구원이 포함되어 있는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 내국인 참여연구원만으로 운영되는 연구 대비 유출 가능성이 높아짐을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 과제 정보에 참여사실이 포함되지 않은 외국인이 포함되는 경우 고려 - IRIS에 해당 과제 참여 내역이 입증되지 않은 외국인 참여연구원의 관리수준에 따라 연구기관(기업 등)이 자체 책임 하에 관리수준을 검토

〈표 4-7〉 **보안등급 분류 체크리스트 예시 : 대학이 연구개발기관인 경우**

① 연구책임자 또는 참여연구원이 세계적인 석학 또는 우수연구자를 포함하고 있는가?	
설명	■ 세계적인 석학이 수행하는 최첨단 연구개발과제의 정보가 유출되는 경우, 우리나라에 예상되는 학문적·기술적 타격을 검토 - 해당 과제 정보가 외국의 경쟁연구자에게 유출되는 경우 해당 과제의 참여연구원과 국가 기술수준에 심각한 타격을 줄 수 있는지 검토* * 유출 시 해당 연구자의 실험실 소속원들의 경력에도 심각한 악영향을 미치는 경우 등 포함
주의	■ 기획연구진 등 (해당 과제 수행연구자가 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 참여연구원 및 연구책임자에 관한 사항이기는 하나, 해당 R&D과제의 연구내용에 대해서도 고려필요 ※ (예) 세계적 석학이 학과장으로서 BK21플러스 사업의 연구책임자인 경우
② 해당 학문분야는 외국 연구자와 출판, 지재권 등 경쟁이 치열한가?	
의미	■ 국내 연구자와 외국 연구자 간 연구경쟁이 치열할수록 과제정보의 유출이 국내 연구자의 불이익으로 직결될 가능성이 높음 - 해당 과제 정보가 유출되는 경우, 외국 연구자가 즉시적으로 출판이나 지재권 등 연구성과에서 대등 또는 우위에 도달할 가능성이 있음
주의	■ 기획연구진 등 (해당 과제 수행기업이 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 세계적인 수준과 별도로 국내에서만 연구자 간 연구경쟁이 가열되어 있는 경우 해당사항이 없음
③ 해당 과제가 국방R&D에 해당되는가?	
의미	■ 해당 과제가 무기체계 개발 등 국방R&D 해당 여부를 검토 - 단, 핵심기술개발사업 등 해당 과제 자체는 기초연구인 경우 미해당
④ 해당 과제가 특정 국가전략기술·국가핵심기술 또는 수출통제 기술 개발인가?	
의미	■ 해당 과제가 정부가 관리하는 주요기술 또는 수출통제 대상 기술인지 검토 - 국가전략기술 중 관리대상 범주는 과학기술전략과 지정 국가전략기술 연구개발사업에 한함 - 국가핵심기술·국가첨단전략기술 및 수출통제 지정 여부는 산업부 기술안보과 및 전략물자제도과의 판단을 준용함
⑤ 해당 과제에 외국기관이 공동연구개발기관 또는 위탁연구개발기관으로 참여하는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 국내 연구개발기관만 참여하는 연구 대비 유출 가능성이 상대적으로 높음을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 외국기관의 경우 소속 국가와 기관 특성에 따라 보안관리 수준이 다양하므로 이를 복합적으로 감안할 필요

⑥ 해당 과제에 외국인 참여연구원이 포함되어 있는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 내국인 참여연구원만으로 운영되는 연구 대비 유출 가능성이 높아짐을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 과제 정보에 참여사실이 포함되지 않은 외국인이 포함되는 경우 고려 - IRIS에 해당 과제 참여 내역이 입증되지 않은 외국인 참여연구원의 관리수준에 따라 연구기관(기업 등)이 자체 책임 하에 관리수준을 검토

〈표 4-8〉 **보안등급 분류 체크리스트 예시 : 출연(연)이 연구개발기관인 경우**

① 연구책임자 또는 참여연구원이 세계적인 석학 또는 우수연구자를 포함하고 있는가?	
설명	■ 세계적인 석학이 수행하는 최첨단 연구개발과제의 정보가 유출되는 경우, 우리나라에 예상되는 학문적·기술적 타격을 검토 - 해당 과제 정보가 외국의 경쟁연구자에게 유출되는 경우 해당 과제의 참여연구원과 국가 기술수준에 심각한 타격을 줄 수 있는지 검토* * 유출 시 해당 연구자의 실험실 소속원들의 경력에도 심각한 악영향을 미치는 경우 등 포함
주의	■ 기획연구진 등 (해당 과제 수행연구자가 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 참여연구원 및 연구책임자에 관한 사항이기는 하나, 해당 R&D과제의 연구내용에 대해서도 고려 필요 ※ (예) 세계적 석학이 학과장으로서 BK21플러스 사업의 연구책임자인 경우
② 해당 학문분야는 외국 연구자와 출판, 지재권 등 경쟁이 치열한가?	
의미	■ 국내 연구자와 외국 연구자 간 연구경쟁이 치열할수록 과제정보의 유출이 국내 연구자의 불이익으로 직결될 가능성이 높음 - 해당 과제 정보가 유출되는 경우, 외국 연구자가 즉시적으로 출판이나 지재권 등 연구성과에서 대등 또는 우위에 도달할 가능성이 있음
주의	■ 기획연구진 등 (해당 과제 수행기업이 아닌) 해당 R&D과제를 수행하지 않는 외부의 판단을 의미함에 유의 ■ 세계적인 수준과 별도로 국내에서만 연구자 간 연구경쟁이 가열되어 있는 경우 해당사항이 없음
③ 해당 과제가 국방R&D에 해당되는가?	
의미	■ 해당 과제가 무기체계 개발 등 국방R&D 해당 여부를 검토 - 단, 핵심기술개발사업 등 해당 과제 자체는 기초연구인 경우 미해당
④ 해당 과제가 특정 국가전략기술·국가핵심기술 또는 수출통제 기술 개발인가?	
의미	■ 해당 과제가 정부가 관리하는 주요기술 또는 수출통제 대상 기술인지 검토 - 국가전략기술 중 관리대상 범주는 과학기술전략과 지정 국가전략기술 연구개발사업에 한함 - 국가핵심기술·국가첨단전략기술 및 수출통제 지정 여부는 산업부 기술안보과 및 전략물자제도과의 판단을 준용함
⑤ 해당 과제에 외국기관이 공동연구개발기관 또는 위탁연구개발기관으로 참여하는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 국내 연구개발기관만 참여하는 연구 대비 유출 가능성이 상대적으로 높음을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 외국기관의 경우 소속 국가와 기관 특성에 따라 보안관리 수준이 다양하므로 이를 복합적으로 감안할 필요

⑥ 해당 과제에 외국인 참여연구원이 포함되어 있는가?	
의미	■ 국제공동연구 장려와 상충되지 않는 수준의 유출 가능성을 검토 - 내국인 참여연구원만으로 운영되는 연구 대비 유출 가능성이 높아짐을 감안
주의	■ 기계적인 또는 무조건적인 협업이나 포함여부만으로 판단하는 것은 제도의 취지와 부합하지 않음 ■ 과제 정보에 참여사실이 포함되지 않은 외국인이 포함되는 경우 고려 - IRIS에 해당 과제 참여 내역이 입증되지 않은 외국인 참여연구원의 관리수준에 따라 연구기관(기업 등)이 자체 책임 하에 관리수준을 검토

② (협약 이후 단계) 기 설정된 보안등급의 변경은 보안과제분류위원회*의 의사결정을 따름

* 「국가연구개발사업 보안대책」 (제3조제1항)이 정의한 보안등급 분류 주체

- (보안과제 수시 등급분류) 연구기관은 수행 중(예정)인 국가연구개발과제의 보안등급에 대해 수시로 재분류 요청을 할 수 있음*

* 「국가연구개발사업 보안대책」 제3조제2항

- (기술성·경제성 판단) 검토 대상 국가연구개발과제의 선정평가 결과를 활용*하여 기술성과 경제성을 판단하는 것을 권고하되, 필요시 기술전문가** 및 경제성 전문가를 활용하여 기술성과 경제성을 판단 가능

* 위원별 평가결과 열람이 아니며 (위원별 최고점과 최저점을 제외한) 평가항목별 평가점수 또는 총점에 해당 평가항목 가중치를 곱한 값을 활용함을 의미

** 연구기관은 직접 판단에 참여하지는 못하더라도, 보안과제분류위원회 등 의사결정 주체를 대상으로 서면 또는 대면으로 의견 개진을 허용할 필요

- (수시 등급분류 시 기준선 설정) 일반과제에서 보안과제로 재분류 시, 재분류 시점을 명확히 하여* 연구현장 보안관리 부담을 최소화

* (예) 일반과제 → 보안과제 전환 시, 일반과제 단계에서 예정·기획된 국외출장 보고대상 시기 등

❑ 보안과제분류위원회 보안등급 재분류 의사결정 방안(안)

○ (목적) 보안과제분류위원회의 보안등급 재분류 시 점수체계를 도입하여 의사결정 부담을 경감하고 재현성과 객관성을 극대화한 체계 마련

- (범용성) 보안과제분류위원회의 보안등급 재분류뿐 아니라, 사전기획 및 공모 단계, 선정평가 단계의 보안등급의 분류 시*에도 본 방안을 참고하여 이행 가능

※ 기획연구진이나 연구개발과제평가단의 보안등급 판정 시에도 활용 가능

○ (개요) (각 위원회의) 위원들이 평가항목별로 점수를 부여하고 가중치에 따라 합산한 위원별 점수의 대푯값*에 따라 보안등급을 결정

* (예) 최저 · 최고치를 제외한 위원별 점수의 산술평균 등

- (2단계 판정) 국가안보 → 국민경제 영향의 순으로 평가
- (가중치 조정) 현재 평가항목별 가중치 배분 수준은 임의 제안된 것으로, 통계학적 방법*을 적용하여 공식적인 배분(안) 도출 필요

* 현장자문위원회에서 AHP 평가하는 방안 등

- (평가항목 수시개정) 현장자문위원회 의결에 따라 항목 가감

❑ 보안등급 분류 시 평가항목(안)

○ (국가안보) “국가안보” 개념을 전통적인 군사안보 범주로 한정하여 종래 보안과제의 무기체계와 직결되는 연구개발 활동을 보안과제로 분류

① (주관부처가 국방부·방사청) 국방부 또는 방사청 주관 국가연구개발과제는 원칙적으로 보안과제로 분류

- 무기체계 개발 및 시설운영과 연관되는 원천기술개발*은 제외

* 실제로 해당되는 사례는 방사청 핵심기술개발사업 소관 일부 세부과제에 한정됨

〈표 4-9〉 **국가연구개발과제 보안등급 판정체계(안)**

단계	항목	주요 검토 항목	배점
1	국가안보	주관부처 국방부/방사청 + 무기체계개발 여부*	100
		수행기관 항우연/원자력연 + 무기체계개발 여부*	100
2	국민경제	① 과제규모(정부연구비, 참여연구원) 상위 5%	25
		② 기관유형(대기업, 중견기업, 출연연)	10
		③ 국제공동연구*	15
		④ (기술성) 국가전략기술/국가핵심기술 등 해당	20
		⑤ (경제성) 선정평가 시 경제성 평가점수 우수	30
합계			

※ 점수 총합이 90점 이상이면 보안과제, 80점 이상이면 민감과제

〈표 4-10〉 **주관부처(국방부·방사청) 수행과제의 보안과제 판정 예시**

주관부처	세부사업명	내역사업명	과제명	보안과제
국방부	민군기술협력	전력지원체계개발	폭발물처리사 방염전투복	해당
방사청	국방기술개발	부품국산화지원사업	KF-21 AESA 레이더용 반도체송수신 모듈 등 5종	해당
		핵심기술연구개발	전술 군집 무인기 임무계획 및 자율 임무 재계획 기술	해당
			산화물기반 대전류 Thyristor 특화연구실	미해당

② (수행기관이 항우연·원자력연) 항우연(KARI) 또는 원자력연(KAERI) 수행 무기체계 개발 또는 국가전략기술 국가연구개발사업의 국가R&D과제는 기본적으로 보안과제로 관리

- 국가전략기술을 특정한 국가연구개발사업은 아니지만, 이에 준하는 성격의 기관고유 R&D과제도 포함할 수 있음*

* 항우연 및 원자력연은 기본적으로 국가R&D과제만 수행

- 인건비 등 일상적인 기관 운영활동은 제외

〈표 4-11〉 **수행기관(항우연·원자력연) 수행과제의 보안과제 판정 예시**

수행기관	주관부처	내역사업명	과제명	보안과제
항우연	과기정통부	다목적실용위성개발	다목적실용위성 7A호 탑재체 성능개선 연구개발	해당
		한국항공우주연구원연구운영비지원	액체엔진 고성능화 선행기술 연구	해당
	해수부	한국형위성항법시스템(KPS)개발사업	한국형 위성항법시스템(KPS) 지상시스템 개발	해당
원자력연	과기정통부	수출용신형연구로개발및실증	신형연구로 핵연료설계	해당
		한국원자력연구원연구운영비지원	양자정보통신 구현을 위한 기능성 양자자성 소재 개발	해당
			연구기획평가사업	미해당

○ (국민경제 영향) 현행 국가연구개발과제 선정평가 체계를 활용하여 국민경제 영향성에 대한 정성평가 위주로 전문기관이 판정[15)]

15) 국민경제 영향에 대한 연구개발활동의 계량적 판단은 아래와 같은 방안을 고려해볼 수는 있으나 분석 특성 상 현실성이 없으므로 정량적 판단은 원칙적으로 배제함
① 비용-편익 분석 : 연구개발활동의 직접적인 경제적 이익과 해당 기술개발 활동의 소요비용을 비교하는 방법.“직접적인 경제적 이익”의 범주 설정이 대부분의 연구개발활동 특히 과제 수준에서 현실성이 미흡하므로 일반론적으로 활용 가능한 방법이라고 볼 수 없음. 다만 해당 연구개발활동이 어느 정도 규모를 갖추고(대형 세부사업 수준) 일반 시민도 공감할 수 있는 수준의 성과물을 산출하면서 국민경제에 영향을 미치는 경우, 간접편익과 비용(환경에 미치는 영향, 사회적 변화 등) 추정을 조건부가치추정(CVM) 등 진술선호분석 기법 등을 활용하여 추정 가능
② 시장 파급효과 분석 : 특정 산업(시장)에 연구개발활동의 성과물이 미치는 영향을 분석하는 방법. ①과 마찬가지로“연구개발활동의 성과물”과“특정 산업(시장)”이 구체화된 경우에는 정량적인 분석도 가능하나 산업화 수준이 높을수록 세부 연구개발활동의 가치사슬과 파급효과를 특정하기 어려운 한계가 존재함. 다만 시장과 산업, 활동주체가 명확하게 특정되는 경우, 공급망에 미치는 영향이나 산업 내 경쟁구도 변화 등을 정성적으로 판단하는 접근은 대체로 유효한 편이므로, 과제보다 기술에 대해 적용하는 것이 적절
③ 경제적 영향 분석 : 특정 연구개발활동이 GDP, 고용, 수출 등 경제 주요지표에 미치는 영향을 분석하는 방법. 생산함수의 명료한 설계가 가능하다면, 이를테면 특정 연구개발활동의 결과물이 특정 기업 또는 산업 부문의 산업생산성을 향상시키거나 신시장을 창출하는 범위 및 수준을 알고 있다면 GDP 증가에 기여하는 정도를 추정할 수 있으나, 대부분의 경우 이러한 범위 및 수준을 특정할 수 없음
④ 산업연관분석 : 산업연관표를 활용, 생산유발계수 및 부가가치유발계수 분석 등을 활용하는 방법. 만일 특정 연구개발활동의 성과물로서의 해당 산업 생산물 및 타 산업 생산물 투입계수를 특정할 수 있다면 특히 국민경제 관점에서 적절한 분석방법이 될 수 있으나, 실제로는 ①-③과 동일한 한계를 지님

〈표 4-12〉 **국가연구개발과제 연구보안 등급분류 중 2단계(국민경제 영향성) 판단 기준(예시) 요약**

평가 항목			부연 설명	예시	가중치	
과제	규모	연구비(정부연구비 기준)	높은 연구비는 정부가 중요성을 인정한다는 의미	상위 5%(12억 초과) 여부	50	10
		참여연구원 수	참여연구원 다수일수록 유출 가능성은 증가	상위 5%(40명 초과) 여부		10
	수행 특성	연구수행주체	기관유형별 배점	대기업·중견기업·출연연 여부		10
		연구개발단계	기초연구 배제를 위한 항목	기초연구단계 미해당 여부		10
		공동연구여부	공동연구는 태생적으로 유출 가능성	공동연구 해당여부		10
기술성 (과제내용의 국가전략적 중요성)			국가핵심기술, 국가전략기술, 국가첨단전략기술, 수출통제 해당 ※ 과제의 성격에 따른 기간산업 해당여부 포함 ※ 또는 선정평가 결과 활용	해당 기술·산업 해당여부	20	
경제성			연구성과물의 경제적 파급효과 ※ 선정평가 결과 활용 ※ 정성판단, 3점 척도	3점 척도(0/10/20/30)	30	
합계					100	

〈표 4-13〉 **국가연구개발과제 연구보안 등급분류 중 2단계(국민경제 영향성) 판단 항목별 분석의도 및 판정 방법**

평가 항목			분석의도				판정 방법(기준)		가중치	
			범위 한정	유출 우려	기술적 가치	경제적 영향	자동판정*	기존활용**		
과제	규모	연구비(정부연구비 기준)	●		●	●	●		10	50
		참여연구원 수	●	●			●		10	
	수행특성	연구수행주체				●	●		10	
		연구개발단계	●				●		10	
		공동연구여부		●	●		●		10	
기술성 (과제내용의 국가전략적 중요성)					●	●		●	20	20*
경제성					●	●		●	30	30*
합계									100	

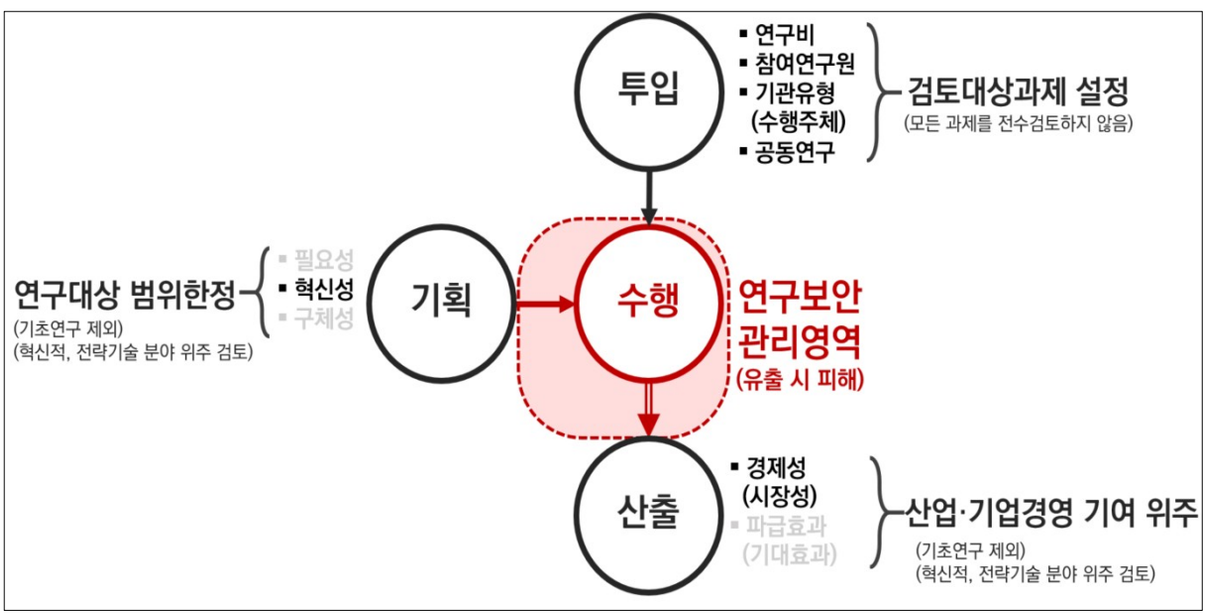
* 통합정보시스템에 등록되는 과제별 서지정보에 입각하여 자동 판정
** 필요시 보안과제분류위원회가 조정 가능

① (유출시 피해를 상정) 수행 → 산출 중간 과정에 관리 주안점

* 최종산출물 공보·공표 시점에서 “유출”은 무의미하다는 판단에 따름

② (선정평가체계 활용) 국가연구개발혁신법 및 동법 시행령이 명시한 선정평가 항목을 연구보안의 국민경제 영향평가에 (재)활용 권고

※ 법령 상 선정평가 항목은 전문관리기관 및 세부사업·내역사업별로 다양하게 적용 및 활용되므로, 평가항목의 세부적인 운영은 각 전문관리기관이 자율적관리 필요



[그림 4-9] **국민경제 영향 관점에서 연구보안 관리의 주요 고려 범위**

- (기술성·경제성 판단) 검토 대상 국가연구개발과제의 선정평가 결과를 활용하여 기술성과 경제성을 판단*하는 것을 권고하되, 필요시 기술전문가** 및 경제성 전문가를 활용하여 기술성과 경제성을 판단 가능

* 위원별 평가결과 열람이 아니며 (위원별 최고점과 최저점을 제외한) 평가항목별 평가점수 또는 총점에 해당 평가항목 가중치를 곱한 값을 활용함을 의미

** 연구기관은 직접 판단에 참여하지는 못하더라도, 보안과제분류위원회 등 의사결정 주체를 대상으로 서면 또는 대면으로 의견 개진을 허용할 필요

〈표 4-14〉 **국가연구개발과제 선정평가 항목과 연구보안 검토항목과 연관성**

항목		혁신법 및 시행령	연구보안
과제	학술적·기술적·사회적·경제적·지역적 파급효과	법 제10조제2항제3호	■ 혁신법 시행령 제45조제1항 ■ 연구보안 체계 내실화 방안
성과	활용 가능성	법 제10조제2항제3호	■ 연구보안 체계 내실화 방안

① (기술성) 연구대상의 국가전략적 중요성*에 따른 배점(20)

※ 국가전략기술, 국가핵심기술, 국가첨단전략기술, 수출통제기술 등 특정 세부기술의 연구보안 관점에서의 관리 필요성을 반영(20)

〈표 4-15〉 **기술성 지표별 배점(안)**

항목	기준	배점	비고
국가관리기술 여부	국가전략기술* 국가핵심기술* 국가첨단전략기술*또는 수출통제기술*	20	■ 기술분류 매칭여부 판단이 아님 ■ 해당 분야의 기술 또는 산업에서 분류 대상 과제 연구개발활동이 미치는 영향력을 판단한다는 의미 (부합성과 중요성/파급효과를 종합적으로 판단)
	해당 과학기술분류 없음	0	

* 중복 산정하지 않으며(예 : 국가전략기술과 국가핵심기술에 모두 해당되더라도 20점), 소분류 수준의 구체적 매칭 수준을 감안

※ 국가전략기술, 국가핵심기술 등은 과기정통부 과기전략과와, 산업부 기술안보과 및 전략물자제도과가 수시로 고시하는 사항을 고려하여 판단

※ 기술성은 전문기관의 과제 평가 총점(100점 만점 환산)에 기술성 해당 항목의 비중으로부터 유추하거나, 외부 기술전문가 의견 수렴을 통해서도 가능하도록 지원하고, 필요 시 연구기관 기술전문가가 의견을 피력할 수 있도록 배려

※ 단, 기술분류의 매칭만으로 판정이 이루어지는 것이 아니며, 보안등급 분류대상 과제가 해당 기술 · 산업 부문에서 지니는 영향력을 조합적으로 판단하여야 함

(예) EUV를 이용한 3nm 급 선폭 반도체 소자용 3D 게이트 기술개발 : 국가전략기술 및 국가핵심기술 등에 모두 부합할뿐 아니라, 해당 기술이 유출되는 경우 경쟁국의 기술수준을 급격하게 높일 가능성이 있음(20점)

(예) 5um급 선폭의 패널레벨 FOWLP 패키지 기술개발 : 국가전략기술 및 국가핵심기술 등에 모두 부합하나 우리나라는 아직 추격단계의 기술로 선도국 대비 월등한 열위에 있어 연구보안 관점에서는 관리대상으로 보기 어려움(0점)

② (경제성) 해당 국가연구개발과제 (연구)성과물의 국내 산업부문 기여도 및 경제적 파급효과의 예상 수준을 정성적으로 판단(30점)

- 가급적 해당 국가연구개발과제 선정평가 결과의 경제성 또는 경제적 파급효과 관련 평가항목을 가중치와 점수를 종합하여 준용*하도록 권고하되, 필요시 보안등급분류위원회에서 외부의견을 수렴하여 판정하는 옵션을 제시

* 가능한 경우 익명화된 평가위원별 배점의 활용을 권고하되, 현실적으로 평가참여자별·평가항목별 점수 활용이 곤란함을 감안하여 종합평점으로 대체

※ 경제성은 전문기관의 과제 평가 총점(100점 만점 환산)에 경제성 해당 항목의 비중으로부터 유추하거나, 외부 경제성 전문가 의견 수렴 등을 통해 판단

〈표 4-16〉 **국가연구개발과제 선정평가항목의 실례**

평가항목	세부항목 및 지표		배점
기술성 (70)	지원 필요성	RFP/품목과의 부합성	10
		선도적 IP 확보의 시급성 및 가능성	10
	도전성 및 창의성	개발 기술의 창의성 및 원천성	30
		개발 기술 목표의 구체성, 명확성	20
연구역량 (20)	책임자 등 조직 역량	연구팀 구성의 우수성 - (공통) 연구책임자 및 연구진 구성의 우수성 - (공동과제 구성시) 공동과제 구성의 타당성 포함	10
	주관기관 의지	연구기반 구축 및 주관연구기관의 지원 의지 - 인프라 및 지재권 출원 등록비 예산 지원 의지 등	10
파급성 (10)	파급효과	기대되는 기술의 파급성및 탁월성 - 사회·경제적 가치창출 가능성	10

(출처) 2022년도 PIM 인공지능반도체핵심기술개발(소자) 신규과제 공고문

〈표 4-17〉 **A과제가 100점 만점에 89점으로 과제선정된 경우**

- 기술성 : 89 × 70% = 62.3 → 보안등급 (재)분류 시 62.3/70 × 20 = 17.8

- 경제성 : 89 × 10% = 8.9 → 보안등급 (재)분류 시 8.9/10 × 30 = 26.7

※ 세부 평가항목 별 평균 점수를 알 수 없는 경우에 제한적으로 적용

- (과제 특성 고려) 보안과제분류위원회가 과제별 특성을 추가로 고려

① (과제규모) 상위 5% 수준 규모의 국가연구개발과제에 대해서만 검토(20)

※ 과제비 규모는 R&D 비정형성을 감안하더라도 과제의 사안적 중요성과 비례한다고 볼 수 있으며, 대형 과제의 수행은 다수의 참여연구원 투입을 필요로 하는 만큼 유출 가능성 또한 상대적으로 높을 가능성이 있음

※ 2022년도 국가연구개발사업 조사·분석 기준으로 연구비·참여연구원에 대한 대형과제의 판단 기준은 아래 참고 표와 같으며, 이를 바탕으로 예시적인 판정기준을 수립 가능

〈표 4-18〉 **국가연구개발과제 규모별 상위수준 판단지표**

항목	상위 % (과제건수기준)		
	5%	2%	1%
연구비(정부연구비 기준, 억원)	12.5	22	35
참여연구원(명)	42	70	95
연구기간(년)	7	10	13

(출처) 2022년도 국가연구개발사업 조사·분석

〈표 4-19〉 **과제규모별 배점(안)**

항목	기준*	배점	비고
연구비(정부연구비)	연 12억 이하	0	
	연 12억 초과	15	
참여연구원 수	연 42명 이하	0	Headcount 기준
	연 42명 초과	15	

* 상위 5% 기준이므로 매년 변동되며, 고시 등을 통한 기준선 변경 사항 안내 필요

② (기관유형) 공공부문과 민간부문 모두 기관 규모가 클수록 연구보안 유출 가능성은 낮으나, 유출 시 국민경제에 미치는 영향은 커짐(10)

※ 민간부문의 경우 대기업은 자체 관리가 우수한 편이므로 유출 가능성은 희박하나, 만일의 유출 발생 시 대규모 피해가 발생(예 : 삼성전자)하며, 유사하게 공공부문의 경우 (대학 대비 상대적으로) 출연연이 체계적이고 고강도로 관리하나 연구보안 유출 시 대학 대비 피해가 큼

〈표 4-20〉 **기업규모에 따른 유출 가능성과 유출 시 피해규모**

기업규모	보안 취약성	유출 시 피해규모	비고
대기업	소	극대	대기업은 우리나라 GDP의 60% 가량 점유
중견기업	중	중	
중소기업	대	소	

〈표 4-21〉 **기관유형별 배점(안)**

기관유형	대기업	중견기업	중소기업	출연연	대학
가점	10	10	0	10	0

〈표 4-22〉 **공동연구 여부에 따른 배점(안)**

항목	기준	배점	비고
공동연구	국제공동연구	15	연구 유출 가능성 관점
	국내공동연구	5	
	단독연구	0	

③ (공동연구) 유출 가능성의 측면에서 공동연구기관의 연구보안 관리수준과 주관·공동·위탁연구기관의 외국인 참여연구원 규모·관리 수준(10)

- 국제공동연구 진흥과 상충되는 관점이 아니며* 해당국 및 해당 외국기관의 성격과 연구관리 수준을 감안하여 필요시 배점한다는 취지

  * (예) 국제공동연구기관·국가가 체계적으로 연구보안 체계를 수립·운영 중인 경우 해당 사항이 없음

  ※ 상대기관의 관리 수준이 미흡할수록 점수가 높음

제3절 연구보안 등급분류 자동화 가능성 검토

❑ 국가연구개발 세부과제의 보안등급을 통합정보시스템 수준에서 예상·제안 가능성 탐색 필요

- (물리적 제약) 2019년 이후 국가연구개발사업 세부과제는 연 7만 건을 상회*하고 있어 한정된 인력과 전문가가 검토하기에 물리적인 한계

  * 2019년 70,327 → 2022년 76,052건 : 주관과제 한정, 공동·위탁과제 제외

- (현장지원) 보안등급의 예상 분류를 통합정보시스템 등을 통해 제공함으로써 전문기관 업무효율 향상 및 현장연구자 가이던스 제공*

  * 현장연구자 FGI 결과, 보안등급 예상 분류 제시 수요가 확인

❑ (탐색 방향) 활용 가능한 과제정보를 기반으로 보안과제 등급분류 자동화 가능성 모색

- (자료) 국가연구개발사업 조사 · 분석 데이터*를 활용한 보안과제 해당여부 판정 가능성 탐색

  * 현 시점에서 유일한 과제 데이터셋이며, 서지정보 위주로 수록

- (방법) 보안과제-일반과제*별 문서 유사도 분석을 통해 분석 가능성 및 유사도 영향인자 파악

  * 조사·분석 데이터셋은 비공개 과제를 보안과제로 표기하고 있으나, 일단 이를 준용하여 분석

❑ (분석 방법) 탐색에 적용한 유사도 분석 과정은 다음과 같음

- (과제별 텍스트 추출) 조사·분석 데이터의 과제별 요약문과 과제명에서 단어를 추출
- (과제 텍스트 벡터화) 추출한 단어를 이용해 과제를 단어공간 벡터화
- (유사과제 식별) 과제별 벡터를 학습시킨 AI로 하여금 과제별로 가장 유사한 과제를 검색
- (유사도 기준 비보안과제 식별) 각 보안과제를 대상으로 가장 유사한 비보안과제(“잠재보안과제”로 지칭) 10 개를 추출
- (분석결과 검토) AI가 제시한 보안과제와 잠재보안과제 간 차이 조사

❑ (데이터) 탐색적 연구 목적으로 2020년도 국가연구개발사업 조사·분석 데이터를 활용

- (기준) 연구기간 2020.1.1.~2020.12.31.인 국가연구개발사업 세부과제
- (규모) 총 73,501개
- (요약문 활용) 데이터 중 ‘연구내용’ 필드만 활용하고 탐색의 효율을 위해 요약문 중 ‘연구목표’와 ‘기대효과’ 필드는 활용하지 않음*

* '연구목표'와 '기대효과'를 포함하여 검토하는 경우 주제어 스펙트럼이 확장되므로 유사도 분석 결과의 정확도를 제고할 수 있으나(보안과제의 연구내용이 학문분야 특성상 특수한 경우에도 기대효과 등은 보편적인 단어를 주로 활용하므로 유사 비보안과제의 식별률 제고 효과가 존재), 실제로는 3개 필드의 어휘가 중복되는 경우가 많아 학습에 과도하게 많은 시간과 자원을 소요하는 등 효율성 측면을 고려

❑ **(비지도형 학습) 지도형(supervised learning)과 비지도형(unspervised learning)으로 구분할 수 있으며, 본 연구에서는 비지도형 학습을 적용**

○ (지도형 학습 이슈) 보안과제 여부를 식별자로 적용하는 지도형 학습은 보안과제와 잠재보안과제간의 표본 불균형* 가능성으로 인해 지양

* Sample Imbalance : 조사·분석 데이터 상 보안과제는 2022년 기준 557개로 모집단(73,501개)의 0.76% 수준에 불과하며, 이러한 비율은 대상연도를 넓히더라도 크게 달라지지 않아(2021년, 2023년 등 연도범위를 확대하지 않은 이유) 보안과제 여부로 접근하는 경우 과소추정(통계적 오류 중 1종 오류) 가능성이 높음

○ (비지도형 학습 적용) 각 과제별로 가장 유사한 과제를 모집단(전수 과제)에서 찾으므로, 표본 불균형 이슈에서 상대적으로 자유로움

❑ **(분석 결과) 557개의 보안과제가 5,427개*의 비보안 유사과제와 매치**

* 557×10=5,570개의 유사과제 중 보안과제 143개를 제외한 결과로, 이는 약 2.6% 정도의 중복률로 결과 오염에 크게 유의할 필요는 없음을 의미

❑ **(유사도) 보안과제와 잠재 보안과제 간 코사인 유사도*는 값 자체는 낮아 30% 수준****

* Cosine similarity : 내적공간의 문서 벡터 간 각도의 코사인값을 의미하며 0°(완전 동일한 문서)일 때 1, 90°(완전 상이한 문서)일 때 0의 값을 지님

** 유사도 최상위 10개 문서의 유사도가 30% 수준이라는 의미

○ (유사성 충분) 30% 어휘가 비슷한 맥락에서 사용되고 있으므로 차별성 검토를 필수로 시행하는 현행 혁신법 체계에서 충분한 유사성으로 간주 가능

❑ **(서지지표별 특성) 잠재 보안과제와 실제 보안과제는 규모(연구비, 참여연구원 수, 기간), 연구개발단계, 수행기관유형 등에서 유의할 만한 차이를 나타내지 않았으나, 융합연구 수준에서 다소 차이가 존재함**

○ (규모) 연구비, 참여연구원 수, 수행기간 모두 실제 보안과제와 잠재 보안과제 간의 차이를 히스토그램으로 비교하더라도 유의미한 차이를 발견하기 어려움

○ (연구개발단계, 기관유형) 규모와 마찬가지로 유의미한 차이가 존재하지 않음*

* 실제로는 연구개발단계의 경우 기초-응용-개발연구 이외에 '기타' 단계에서는 차이가 존재하나

‘기타’ 단계는 정책연구, 기관고유 인건비 등이 대부분이어서 의미를 부여하기 곤란

○ (융합연구) 융합연구*의 과제 비중은 실제 보안과제의 경우 상대적으로 잠재 보안과제 대비 통계적으로 유의하게 높음**

* 국가과학기술표준분류체계 상 2개 이상의 대분류가 동시에 지정된 과제

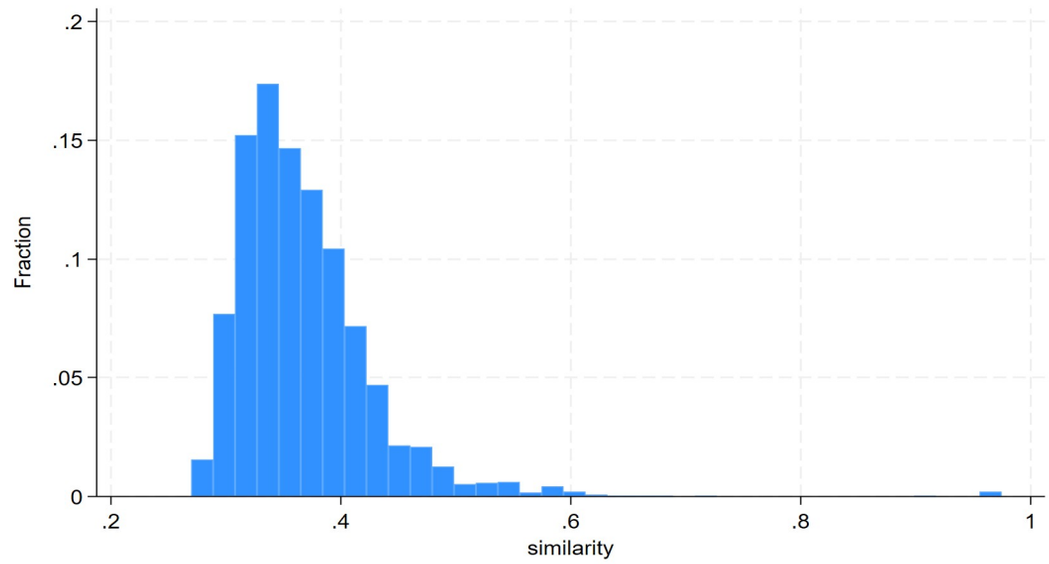
** 다만 융합연구의 비중은 실제 보안과제가 18.2%, 잠재 보안과제는 14.8% 가량으로 실질적인 정책적 함의를 부여하기에 큰 격차는 아님

```
df_simliars_secured_projects
```

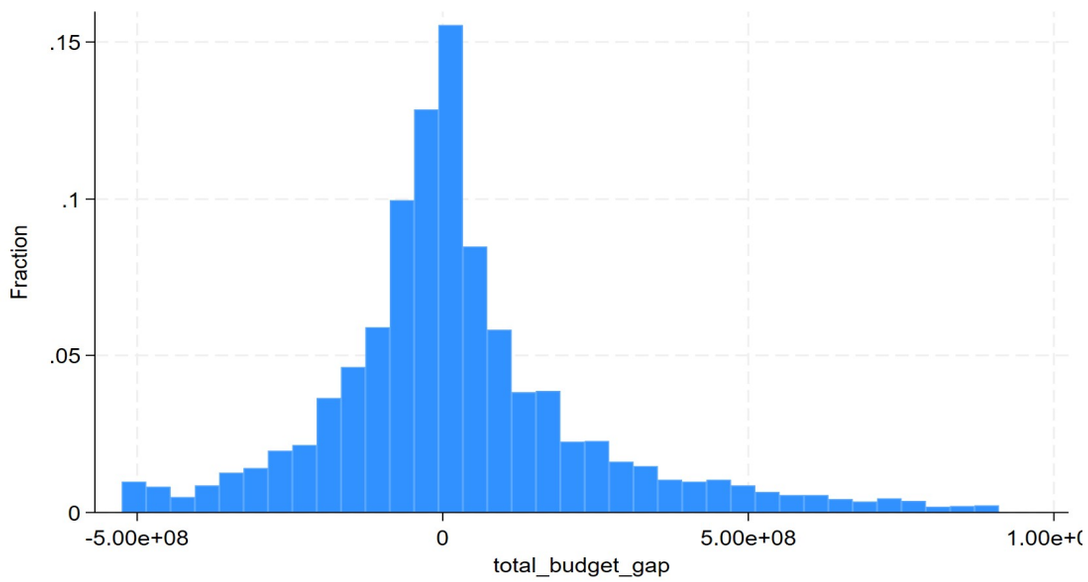
shape: (5_427, 6)

id	project_id	similar_project_id	similarity	classified	similar_classified
u32	str	str	f64	str	str
272	"1711124238"	"1711124231"	0.426191	"Y"	"N"
272	"1711124238"	"1425139831"	0.40117	"Y"	"N"
272	"1711124238"	"1345329780"	0.399949	"Y"	"N"
272	"1711124238"	"1345329770"	0.398162	"Y"	"N"
272	"1711124238"	"1345329731"	0.396306	"Y"	"N"
272	"1711124238"	"1395066203"	0.395733	"Y"	"N"
272	"1711124238"	"1345329689"	0.395136	"Y"	"N"
272	"1711124238"	"1345329684"	0.392392	"Y"	"N"
272	"1711124238"	"1345329725"	0.392366	"Y"	"N"
272	"1711124238"	"1345329808"	0.39204	"Y"	"N"
273	"1711124229"	"1711122690"	0.433824	"Y"	"N"
273	"1711124229"	"1425147832"	0.368872	"Y"	"N"
…	…	…	…	…	…
63900	"1345318958"	"1425141061"	0.315735	"Y"	"N"
63900	"1345318958"	"1485016839"	0.315158	"Y"	"N"
63917	"1711105769"	"1345316721"	0.341264	"Y"	"N"
63917	"1711105769"	"1711118955"	0.32401	"Y"	"N"

[그림 4-10] **비지도형 학습을 활용한 보안과제 분석 결과 예시**



[그림 4-11] 보안과제와 잠재 보안과제 간 유사도 분포



[그림 4-12] 보안과제와 잠재 보안과제 간 총연구비 분포

❑ **(분석결과 시사점) 서지정보에 국한된 문사 유사도 접근으로는 보안등급의 자동분류의 현실성 미흡**

○ 실제 보안과제와 유사한 과제(잠재 보안과제)의 식별은 비교적 용이하나, 도출된 실제-잠재 보안과제 간 서지정보 항목의 차별점을 발견할 수 없음

❑ **(향후계획) 이후 연구계획서 전문에 대한 접근이 가능해지면, 토픽모델 등 의미론적 접근을 시도해볼 수 있음**

제4절 소결

❑ 선행연구와 과업의 특성을 종합적으로 고려하고 전문가 의견을 수렴하여 국가연구개발사업 세부과제의 보안등급의 2단계 평가체계를 제시

- (전주기 대응) 국가연구개발사업 보안대책 등 기존 제도와의 일관성과 과제전주기 대응을 위해, 선정평가 이전에는 체크리스트를, 선정평가 이후 점수기반의 평가체계를 활용하는 방안을 제시
  - (기획·선정평가 단계) 과제가 의도한 연구수행기관의 기관유형에 기반한 체크리스트의 가안을 제시하고 이를 기반으로 보안과제 또는 민감과제로 분류하는 방안을 제시
  - (선정평가 이후 단계) 과제규모(연구비, 참여연구원) 및 수행 기관유형(대기업, 출연연 등), 공동연구여부 등 과제정보와 기술성과 경제성 등 연구개발과제평가단의 선정평가 결과를 전용한 점수기반의 평가체계를 보안과제등급분류위원회 등이 활용할 수 있는 방안을 제시
- (1단계) 보안과제 해당여부를 국가안보(무기체계개발) 연관성을 기준으로 판단하여, 제시된 항목에 부합하는 경우 보안과제로 판정하고 평가를 종료
  - (공통) 해당 국가연구개발사업 세부과제가 무기체계 개발에 직접적으로 활용되거나 체계개발의 일부인지 식별
  - (추가 검토요인) 해당 국가연구개발사업 세부과제가 국방부 또는 방위사업청이 국비를 부담하는지, 또는 특정 출연연(한국항공우주연구원, 한국원자력연구원 등)이 수행하는지 등을 확인
- (2단계) 과제규모(연구비, 참여연구원) 및 수행 기관유형(대기업, 출연연 등), 공동연구 여부 등 과제정보와 기술성과 경제성 등 연구개발과제평가단의 선정평가 결과를 재활용 또는 보안과제등급분류위원회의 5점척도 기준 평가결과를 조합하여 민감과제 판정 가능성을 검토
  - 평가 효율성과 공정성을 위해 가능한 경우 전문기관의 과제선정평가 결과를 준용할 수 있는 체계를 제시

❑ 향후계획(안)

- (의견수렴에 의한 항목 조정) 등급분류 전문가 및 현장연구자 대상 국가안보 및 국민경제 영향 고려인자별 검토의견 수렴

- (검토항목 조정) 필요시 국가안보 및 국민경제 항목 변경·수정*

  * (예) 현재 국민경제 영향성 인자로 설정되어 있는 국가전략기술·국가핵심기술 등 분류체계 해당여부 항목을 국가안보로 이동

- (가중치 조정) 조정된 검토항목의 배점 시나리오에 따른 보안과제 및 민감과제 규모 검토*를 통한 관리 예상수준 파악**

  * (예) 기술성 배점을 20점에서 30점으로 상향하고 경제성 배점을 30점에서 20점으로 감소

  ** (예) 보안과제 연 500건, 민감과제 1,500건 수준 등

○ (매칭 자동화 가능성 탐색) 과제요약문을 중심으로 보안과제 자동 판별 가능성을 탐색하고 추가로 도입 가능한 과제 서지정보가 있는지 검토

※ 외부 전문가 의뢰 및 검토 중(2월 중 적용 가능성 탐색 결론 도출 예정)

○ (향후일정) 시범운영 모의활용*('24.3월) → 시범운영 환류 및 가이드라인 수립(~6월) → 가이드라인 초안(6월) → 가이드라인 초판 발간(12월)

* 시범운영기관 모의적용 조직의 연구성격에 맞춘 가이드라인 우선 수립 예정

제5장 결론

1 연구보안 전담조직 설립방향 수립을 위한 사전조사

❑ (수립방향 제시) 연구보안 지원 역할을 중심으로 설정하되, 본격 연구보안 전담 집행조직의 해외 사례 추이와 국내 연구현장 의견을 감안한 설립 목적 및 세부 기능 등 조정 필요

- 연구현장의 연구보안 지원에 초점을 맞춰 ①정책 ②홍보 ③교육 ④가이드라인 개발 등을 중심으로 구성하되, 조직이 필수로 수행해야 할 기능을 추가하는 방향을 제시
  - 연구보안 관리 등 기관의 상세 직능은 근거법령의 검토와 필요시 개정을 토대로 연구현장 수용성에 유의하여, 해외사례(미국 RSI-ISAO 프로그램 등)의 설립동향을 토대로 추가 고려 필요함을 확인
- 단기적으로는 유사사례를 참고하여 추진단 등의 형태로 유관기관 내 부서(10인 내외)로 우선 기능부터 도입 및 운영하고, 향후 조직 확장 또는 분리·신설 등 고려하는 방향 제시
  - 최근 신설 사례가 없음을 감안할 때 기존 조직 내 부서 형태가 현실적임을 확인하였으며, 이는 해당 조직의 기성 자원을 활용할 수 있다는 측면에서도 장점
  - 국내 산업보안 유사조직의 경우 기능과 대응범위에 따라 10인 초반에서 30인 이내로 유지 중이므로, 초기 10인 내외 조직 규모는 대체로 적절함을 확인
- 전담 집행조직의 근거 법률은 필수적인 선결사항은 아니나. 조직의 존립기반 및 예산 안정성 측면에서 바람직함을 확인

❑ (시사점) 향후 ①조직 형태, ②설립 목적 및 명칭(안), ③역할 및 기능, ④조직 구조 및 인력 등 구체화된 기획(안) 도출과 연구현장의 이해와 설득에 대한 면밀한 고려 필요

- 별도의 조직 신설 관련 전문가자문단의 검토와 연구보안 현장자문위원회의의 확인을 거치고, 필요시 근거제도 제·개정 등을 위한 공청회를 활용하여 기획의 구체성과 연구현장 등 이해관계자의 공감대 마련을 병행하는 것이 바람직
  - 연구보안 전담조직 부재 시 예상되는 국가·연구기관·연구자 수준의 문제 및 전담조직의 기대효과 등을 마련하고, 이를 연구현장 설득 및 인식 제고에 활용 가능

2 연구현장의 연구보안 인식 기반 현장지침 설계 시사점 도출

❑ (국내외 사례 및 이해관계자 의견 수집) 국내외 유사 가이드라인 사례를 종합하고 현장연구자 등 이해관계자 의견을 광범위하게 청취하여 기존 연구보안 현장지침의 한계 및 개선방향 도출

- 미국과 일본을 중심으로 한 유사 가이드라인 및 체크리스트 사례와 국내의 연구보안 · 산업보안 지침 및 관련규정 10종*을 복합적으로 검토하여 기존 연구보안 현장지침의 한계를 식별

  * (예) 국가R&D표준관리 표준매뉴얼(2014, 미래부) 등 연구보안 지침 3종, 산업보안 안내서(2021, 산업부) 등 산업보안 지침 4종, 한국인터넷진흥원 통신기반시설가이드 등 기타규정

- 현장연구자, 연구기관 및 전문기관 실무자, 제도 전문가 의견 등을 포괄적으로 수집하여 연구보안 지침의 방향성 수립

  ※ 산 · 학 · 연 현장연구자 및 연구개발과제 수행기관 및 연구관리 전문기관 실무자 등 전 영역의 이해관계자에 대해 FGI 수준의 인터뷰를 진행하여 연구보안의 개념적 이슈와 실천적 한계를 극복하기 위한 현장지침 방향 수립에 관한 의견을 청취하고, 아울러 연구보안 체계 내실화 방안의 소개를 병행함으로써 제도홍보 및 현장착근의 기반 마련

❑ (작성방향 제시) 연구보안 체계 내실화 방안에 의거하여 연구보안의 개념과 관점을 재정립하고, 보안등급 및 연구개발 수행기관유형(산·학·연)을 안배한 구성으로 현장적용성 제고 방향 설정

- 전통적인 연구진실성(research integrity) 관점과 보안사고 예방을 위한 절차적 규준으로서의 연구보안의 개념을 수립

- 3단계 보안등급 분류(보안·민감·일반과제) 및 5대 영역(참여연구원 관리, 성과물·기술이전, 정보통신망 관리, 시설보안 관리, 실태점검)과 산 · 학 · 연 기관유형을 복합적으로 고려하는 방안 제시

- 현장지침의 대상기관유형별 목차를 정의하고 연구관리 전주기에 방점을 두어 현장연구자와 연구개발기관 실무자가 과제수행 과정에서 발생하는 의문점을 해소하고 내실화 방안에 따른 연구보안 지침의 준수와 생활화를 촉진하도록 안배

❑ **(시사점) 연구현장과 이해관계자를 중심으로 한 연구보안 체계 내실화 착근에 실질적으로 기여할 수 있는 현장지침의 작성기반 마련**

○ 2024년 연중 현장지침 제정 목표를 무난하게 달성 가능한 기초자료 수집을 완료하였으며, 향후 제도개선 방향과 한 방향을 바라보도록 현장지침 본문 작성 추진 예정

3 보안등급 분류체계 설계를 위한 탐색적 연구

❑ **(등급분류 기반 마련) 선행연구와 과업의 특성을 종합적으로 고려하고 전문가 의견을 수렴하여 국가연구개발사업 세부과제의 보안등급의 2단계 평가체계를 제시**

○ (전주기 대응) 보안대책 등 기존 제도와의 일관성과 과제전주기 대응을 위해, 선정평가 이전의 기획연구진과 연구개발과제평가단의 자체 등급분류를 위한 체크리스트를, 선정평가 이후 보안등급분류위원회의 점수기반 평가체계를 모두 제시하는 가이드 작성 방향을 수립

○ (2단계 분류체계 방향성 제시) 과제 선정평가 이후 보안등급분류위원회의 보안등급 분류를 위한 스테이지게이트 방식의 2차에 걸친 분류체계 수립 방향성 설정

- 국가안보(무기체계개발) 연관성을 기준으로 1차적으로 검토하고, 과제규모(연구비, 참여연구원) 및 수행 기관유형(대기업, 출연연 등), 공동연구여부 등 과제정보와 기술성과 경제성 등 연구개발과제평가단의 선정평가 결과를 재활용 또는 보안과제등급분류위원회의 5점척도 평가결과를 조합하여 보안등급 분류 여부를 2차적으로 재검토하는 접근 방향 수립

❑ **(시사점) 향후 체크리스트와 2단계 분류체계 각각의 구체적이고 면밀한 등급분류 방안을 제도개선 방안의 수립과 발맞추어 마련 필요**

○ 현장지침과 유사하게 등급분류 가이드라인의 실제 작성과 제정에는 전술한 연구보안 제도개선의 결과가 유의미하게 환류되어야 하나, 해당 제도개선 활동이 동 연구와 별개로 진행되고 있어 유의미한 환류에 시간이 소요될 가능성이 존재

○ 효율적인 진행을 위해 법제도 및 현장 연구관리 관점에서 보안과제와 민감과제 간 포함관계 등 선행 의사결정이 가능한 사안을 중심으로 기관유형에 따른 등급분류 가이드라인을 과제 생애주기 관점에서 먼저 마련하는 것이 적절

참 고 문 헌

[논문]

강동석·유시형 (2009). “공공정보시스템 효과성 측정지표의 타당성 검증에 관한 연구 – 행정정보 DB 구축사업을 중심으로”, 정보처리학회논문지 16(3): 417-422.

나원철·장항배 (2020). “국가연구개발사업 연구개발과제의 보안등급 평가모델 개발”, 기술혁신학회지 23(4): 841-862.

민정훈 (2023). 미국 118대 연방의회의 정치적 특징 및 전망분석, IFANS 주요국제문제분석 2023-4. 국립외교안보연구원.

박재적 외. (2023) ‘인도·태평양 지역 경제안보“ 주요국의 국내정치 동학과 한국의 경제안보전략. 대외경제정책연구원.

이효영(2022).“경제안보의 개념과 최근 동향 평가”, 주요국제분석 2022-08, 국립외교원 외교안보연구소.

조용래·박현준·이선아·최종화·이정노 (2020). “산업기술안보 관점의 국가 전략목적기술(CPT) 도입과 정책방향”, STEPI Insight 제256호, 2020.6.15. 과학기술정책연구원.

Carrai, M. A., Randolph, J. and Szonyi, M. (Eds.) (2022). The China Questions 2: Critical Insights Into Us-China Relations, Harvard University Press.

Fajgelbaum, P. D. and Khandelwal, A. K. (2022). “The Economic Impacts of the US-China Trade War.” *Annual Review of Economics* 14(1): 205-228.

Grizold, A. (1994). “The Concept of National Security in the Contemporary World,” *International Journal on World Peace* 11(3): 37-53.

Hameiri, H., and Jones, I. (2013). “The Politics and Governance of Non-Traditional Security.” *International Studies Quarterly* 57(3): 462-473.

Schmid, J. and Edenfield, N. (2023). “Scientific and Technological Flows Between the United States and China.” Research Report RR-A2308-1, RAND.

白井俊行 (2022).「内閣府エビデンスシステム (e-CSTI) の概要と今後の方向性」. カレントアウェアネス 354: 18-20.

[보고서]

과학기술정보통신부·한국과학기술기획평가원 (2023).「국제연구협력 시 연구자산 유출 방지를 위한 주요국 정책사례집, 한국과학기술기획평가원」..

과학기술인력개발원 (2015). 연구보안 이해.

국가과학기술연구회 및 국가정보원(2021) 연구보안길라잡이.

국가과학기술자문회의 심의회의 (2023).「신뢰받는 연구생태계 구축을 위한 연구보안 체계 내실화 방안(안)」.

국가과학기술자문회의 전원회의 (2023).「세계를 선도하는 글로벌 R&D 추진 전략(안)」.

대중소기업농어업협력재단 (2019). 중소기업_기술보호 지침.

미래부 (2014). 국가R&D표준관리 표준매뉴얼.

중소벤처기업부 비영리법인 현황 정보 (중소벤처기업부).

산업기술보호협회 (2021). 산업보안 안내서.

지식재산위원회 (2022). 기술의 해외유출과 탈취 방지를 위한 연구자 가이드 라인.

특허청 영업비밀보호센터 (2017). 꼭 알아야 할 영업비밀 관리 표준서식 활용서.

한국공학교육학회 (2008) 연구센터소개-한국산업기술보호협회, Ingenium, 15(1): 42-44.

APS (2021), Impact of US Research Security Policies : US Security and the Benefits of Open Science and International Collaborations, American Physical Society.

BEIS. (2021) “Dedicated government team to protect researchers' work from hostile activity”, Press Release.

Department for Science, (2023) “Innovation & Technology, RCAT Update August 2023”.

Department for Science, Innovation & Technology. (2023) RCAT Update August 2023. DSIT Report.

JASON (2019), Fundamental Research Security, JSR-19-21, The MITRE Corporation; 内閣府 (2023)「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト」.

National Protective Security Authority (2023). Trusted Research Guidance for Academia; Centre for the Protection of National Infrastructure (2022) Trusted Research Guidance for Industry.

NIH OER (2023). NIH Foreign Interference: General Principles, Case Studies, Publicly Available Information on Specific Cases, and Oversight Reports, National Institutes of Health.

NSTC (2019). ‘Recommended Practices for strengthening and security and integrity of America’s science and technology research enterprise.

The Select Committee on the Strategic Competition between the US and CCP (2023). A strategy to win America’s Economic Competition with the Chinese Communist Party, United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party.

[온라인 자료]

중소벤처기업부 비영리법인 현황 정보(https://www.mss.go.kr/site/smba/ex/bbs/View.do?cbIdx=241&bcIdx=1048411&parentSeq=1048411)

미국 NIH 홈페이지(https://grants.nih.gov/policy/foreign-interference/data, accessed on Feb 14 2024.

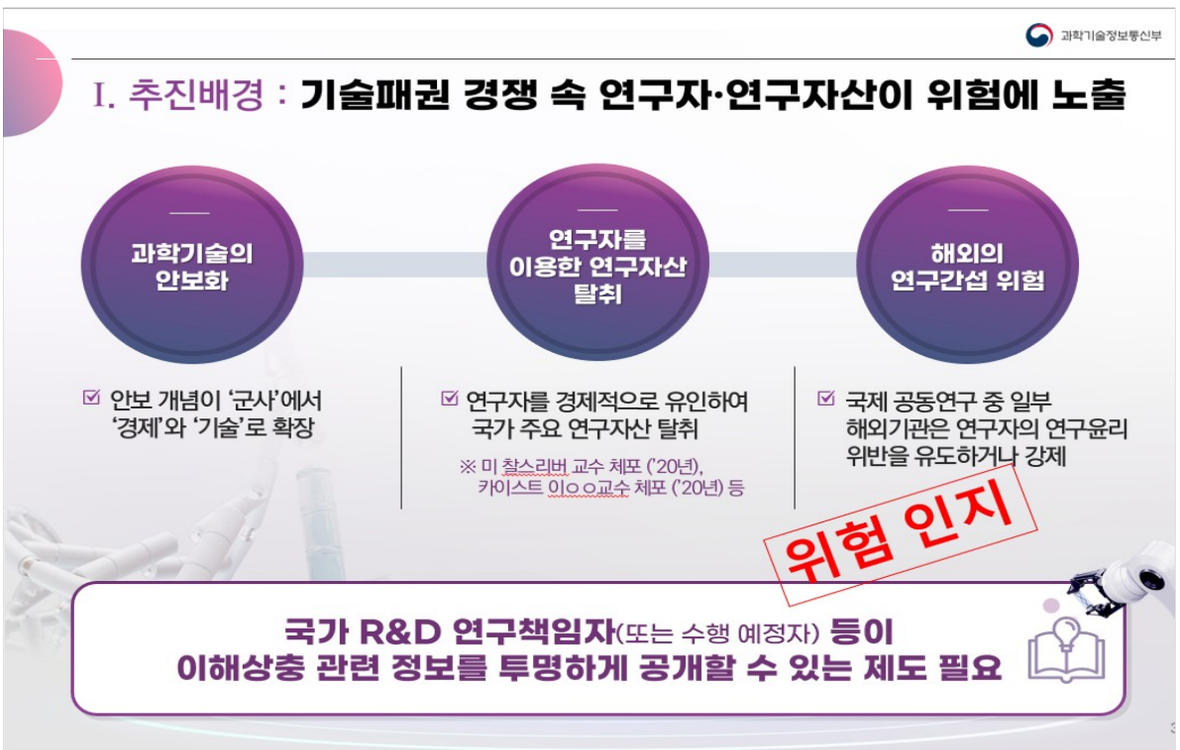
일본 문부과학성 홈페이지https://www8.cao.go.jp/cstp/english/doc/checklist_for_univ_en.pdf

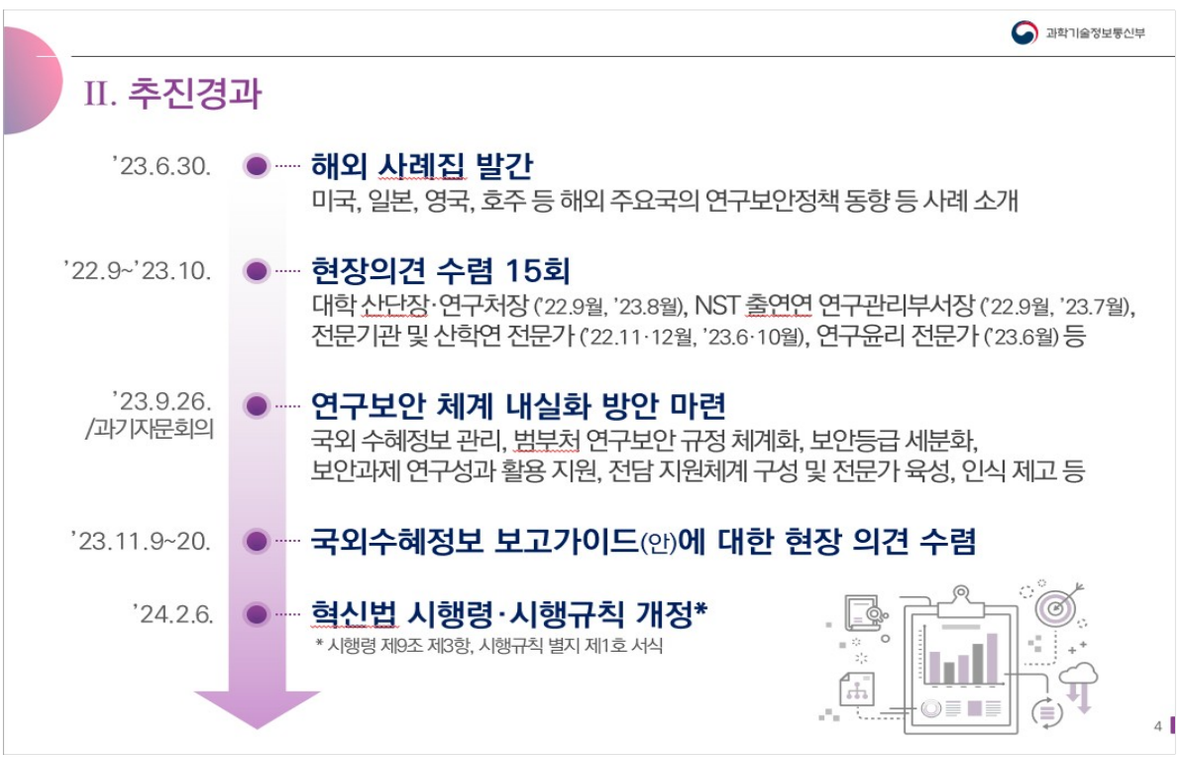
법제처 법령해석 사례(2020-09-17),

https://moleg.go.kr/lawinfo/nwLwAnInfo.mo?mid=a10106020000&cs_seq=424259&currentPage=1&keyField=&keyWord=&sort=date

한국산업기술보호협회 홈페이지(kaits.or.kr)

참고 1 국외수혜정보보고 교육자료


과학기술정보통신부
I. 추진배경 : 기술패권 경쟁 속 연구자·연구자산이 위험에 노출
과학기술의 안보화
☑ 안보 개념이 '군사'에서 '경제'와 '기술'로 확장
연구자를 이용한 연구자산 탈취
☑ 연구자를 경제적으로 유인하여 국가 주요 연구자산 탈취
※ 미 찰스리버 교수 체포 ('20년), 카이스트 이○○교수 체포 ('20년) 등
해외의 연구간섭 위험
☑ 국제 공동연구 중 일부 해외기관은 연구자의 연구윤리 위반을 유도하거나 강제
위험 인지
국가 R&D 연구책임자(또는 수행 예정자) 등이
이해상충 관련 정보를 투명하게 공개할 수 있는 제도 필요


과학기술정보통신부
II. 추진경과
'23.6.30.
해외 사례집 발간
미국, 일본, 영국, 호주 등 해외 주요국의 연구보안정책 동향 등 사례 소개
'22.9~'23.10.
현장의견 수렴 15회
대학 산단장·연구처장 ('22.9월, '23.8월), NST 출연연 연구관리부서장 ('22.9월, '23.7월),
전문기관 및 산학연 전문가 ('22.11·12월, '23.6·10월), 연구윤리 전문가 ('23.6월) 등
'23.9.26. /과기자문회의
연구보안 체계 내실화 방안 마련
국외 수혜정보 관리, 범부처 연구보안 규정 체계화, 보안등급 세분화,
보안과제 연구성과 활용 지원, 전담 지원체계 구성 및 전문가 육성, 인식 제고 등
'23.11.9~20.
국외수혜정보 보고가이드(안)에 대한 현장 의견 수렴
'24.2.6.
혁신법 시행령·시행규칙 개정*
* 시행령 제9조 제3항, 시행규칙 별지 제1호 서식
4

과학기술정보통신부

III. 보고내용: 주요 내용

예시

iris 범부처통합연구지원시스템 Integrated R&D Information System

IRIS 소개 | 사업정보 | 알림·고객 | R&D 정보서비스

일반과제 연구책임자 ('24.2.15.~'27.2.14.)의 국외수혜정보 보고

2

보고 시기	지원·지급 출처 (외국 정부/기관/단체 등)	지원·지급 사유 (연구 수행/노무·자문 제공 내역 등)	지원·지급 기간	지원·지급 금액 (인력/시설/보수 등)	연구개발과제와의 관련 여부
협약 시	A국 □□기업	~에 관한 연구	'22.4.1~'24.3.31.	총 5만불	해당과제 선행연구
	B국 ○○대학	연구인력 지원	'24.3.1~'25.2.28	박사급 2명 석사급 4명	해당과제 참여예정
수행 중	C국 △△연구소	~주제로 강연	'24.5.1	1000만원	해당과제 무관

2 **보고 시기** — 모든 과제 **국가 R&D 협약 시** / 모든 과제 **과제 수행 중 발생일로부터 30일 이내(권고)**

※ 1회 입력으로 국가연구자번호와 연계해 서버 저장, 추후 다른 과제 신청·수행 시 연구자가 수정 용이하도록 설계(IRIS)

7

과학기술정보통신부

III. 보고내용: 주요 내용

예시

iris 범부처통합연구지원시스템 Integrated R&D Information System

IRIS 소개 | 사업정보 | 알림·고객 | R&D 정보서비스

일반과제 연구책임자 ('24.2.15.~'27.2.14.)의 국외수혜정보 보고

보고 시기	지원·지급 출처 (외국 정부/기관/단체 등)	지원·지급 사유 (연구 수행/노무·자문 제공 내역 등)	지원·지급 기간	지원·지급 금액 (인력/시설/보수 등)	연구개발과제와의 관련 여부
협약 시	A국 □□기업	~에 관한 연구	'22.4.1~'24.3.31.	총 5만불	해당과제 선행연구
	B국 ○○대학	연구인력 지원	'24.3.1~'25.2.28	박사급 2명 석사급 4명	해당과제 참여예정
수행 중	C국 △△연구소	~주제로 강연	'24.5.1	1000만원	해당과제 무관

3 **보고 방법** — (과제 협약 시) 제출하는 연구개발계획서에 국외 수혜정보를 포함하여 작성
(과제 수행 중) IRIS 내 연구자정보 현행화

8

과학기술정보통신부

III. 보고내용: 주요 내용

예시

iris 범부처통합연구지원시스템 Integrated R&D Information System

IRIS 소개 | 사업정보 | 알림·고객 | R&D 정보서비스

일반과제 연구책임자 ('24.2.15.~'27.2.14.)의 국외수혜정보 보고 ④

보고 시기	지원·지급 출처 (외국 정부/기관/단체 등)	지원·지급 사유 (연구 수행/노무·자문 제공 내역 등)	지원·지급 기간	지원·지급 금액 (인력/시설/보수 등)	연구개발과제와의 관련 여부
협약 시	A국 □□기업	~에 관한 연구	'22.4.1~'24.3.31.	총 5만불	해당과제 선행연구
	B국 ○○대학	연구인력 지원	'24.3.1~'25.2.28	박사급 2명 석사급 4명	해당과제 참여예정
수행 중	C국 △△연구소	~주제로 강연	'24.5.1	1000만원	해당과제 무관

④ **보고 사항** 외국 정부·기관·단체 등으로부터 재정적·행정적(연구과제·인력·장비·시설 등) 지원 및 노무 또는 자문 등으로 대가를 받는 사항

※ 신청·선정·지정·협약·계약 등을 포함하며 단순 문의·제안·논의 및 종료사항 미포함

9

과학기술정보통신부

III. 보고내용: 주요 내용

예시

iris 범부처통합연구지원시스템 Integrated R&D Information System

IRIS 소개 | 사업정보 | 알림·고객 | R&D 정보서비스

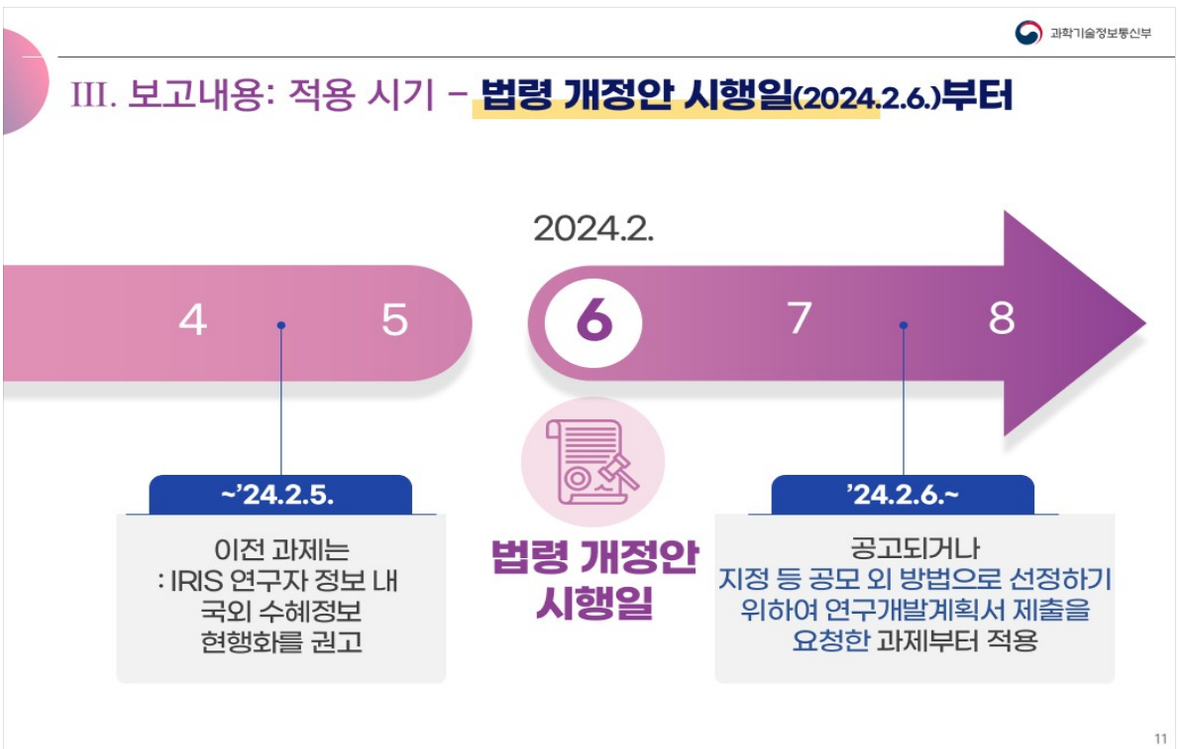
일반과제 연구책임자 ('24.2.15.~'27.2.14.)의 국외수혜정보 보고

⑤

보고 시기	지원·지급 출처 (외국 정부/기관/단체 등)	지원·지급 사유 (연구 수행/노무·자문 제공 내역 등)	지원·지급 기간	지원·지급 금액 (인력/시설/보수 등)	연구개발과제와의 관련 여부
협약 시	A국 □□기업	~에 관한 연구	'22.4.1~'24.3.31.	총 5만불	해당과제 선행연구
	B국 ○○대학	연구인력 지원	'24.3.1~'25.2.28	박사급 2명 석사급 4명	해당과제 참여예정
수행 중	C국 △△연구소	~주제로 강연	'24.5.1	1000만원	해당과제 무관

⑤ **보고 항목** 지원 · 지급 출처, 사유, 기간, 금액, 연구개발과제와의 관련 여부

10


과학기술정보통신부
III. 보고내용: 적용 시기 – 법령 개정안 시행일(2024.2.6.)부터
2024.2.
4
5
6
7
8
~'24.2.5.
이전 과제는
: IRIS 연구자 정보 내
국외 수혜정보
현행화를 권고
법령 개정안
시행일
'24.2.6.~
공고되거나
지정 등 공모 외 방법으로 선정하기
위하여 연구개발계획서 제출을
요청한 과제부터 적용
11


과학기술정보통신부
III. 보고내용: 주체 별 역할
과기정통부
☑ 제도 문의 게시판 운영
☑ IRIS 내 시스템 설계·운영
☑ 해당 연구책임자 대상 연구보안 안내메일 발송
부처·
전문기관
☑ 보고대상 관련 안내
☑ 공고문·협약서에 국외 수혜정보 작성 관련 문구 추가
공고문
연구책임자는 외국정부·기관·단체 등으로부터 행정적 ·재정적 지원을 받거나 노무 또는 자문 등을
제공하고 받는 대가에 관한 사항을 협약용 연구개발계획서에 포함하여 제출하여야 한다.
협약서
연구책임자는 국가 R&D 수행 중 외국정부·기관·단체 등으로부터 행정적·재정적 지원이나
노무 또는 자문 등을 제공하고 받는 대가에 관한 사항을 국가연구개발혁신법 제20조에 따른
통합정보시스템을 통해 중앙행정기관(전문기관)에 알려야 한다.
연구기관
☑ 보고대상 관련 안내
☑ 보안사고 등으로 소관 R&D 부처 요청 시 검증 자료 제공
연구책임자 등
☑ 국가 R&D 과제 협약·수행 시 해당 사항 보고 *
* 해당 (연구)책임자 개인이 보고
※ 1회만 입력하면 추후 다른 과제 신청·수행 시 자동 입력 후 수정 가능
12

과학기술정보통신부

IV. 질의응답

Q2.

해외 주요국의 외부수혜현황 보고 제도와의 차이점은?

해외 주요국		우리나라
국가 R&D 신청 ·수행 시	보고 시기	국가 R&D 협약 ·수행 시
국내외 기관 수혜현황보고 의무화	보고 사항	국외 기관 수혜현황보고 의무화, 보고항목 최소화

국가	지원현황*	수혜내용 (과제명)	역할 (책임/참여)	지원출처 (기관명)	주요수행처	지원기간	지원금액	(수혜)M/M	국가과제 관련성	책임자 정보
		O		O		O	O		O	
	O	O		O	O	O	O	O	O	
	O	O	O	O		O	O	O	O	O

* 신청중/수혜중/수혜예정 등

과학기술정보통신부

IV. 질의응답

Q3.

참여연구원의 국외 지원사항도 보고 대상인지?

☑ 주관연구개발기관의 연구책임자, 공동·위탁연구개발기관의 책임자에 대한 국외 지원사항만 해당

Q4.

(연구)책임자가 변경되는 경우 보고 시기는?

☑ 책임자 변경에 따른 협약 변경 시, 변경된 책임자의 국외 수혜정보 보고


과학기술정보통신부
IV. 질의응답
Q5.
해외 본사 및 별도 법인(국내지사 등)이 있는 기관의 금전적·비금전적 지원의 경우 보고 대상인지?
☑ 본사와 지사의 소재가 다를 경우 본사 위치를 기준으로 보고
☑ 해외정부(공공기관 포함) 또는 해외 본사 기업·비영리단체의 국내법인/지사/연락사무소(출장소) 등의 행정적, 경제적 지원 및 강의, 자문 등 대가는 보고 대상
Q6.
보고 대상이 되는 시기는?
☑ 선정·지정·협약·계약 체결 등 지원 확정 또는 신청한 경우 보고 대상이며, 단순 문의·제안·논의 사실만으로는 보고 사항이 아님
※ 보고사항(지원기간, 지원금액 등)은 수시 수정 가능
☑ 협약 당시 수혜 중인 지원사항은 보고 대상이나, 종료된 지원사항은 보고 대상이 아님
※ 협약 대상 국가R&D 과제수행과 기간이 중첩(또는 포함)되는 수혜 사항만 보고
16


과학기술정보통신부
IV. 질의응답
Q7.
학회발표, 자문 등의 대가 수수도 보고 사항인지?
☑ 대가가 있는 경우 보고 사항(교통·음식·숙박/체재비 명목의 실비 지원도 포함)이나,
동일 기관으로부터 받은 수혜 대가의 연간 누계가 5,000달러(USD) 초과하는 경우로 한함
Q8.
대가 없이 자문을 수행하는 경우도 보고 사항인지?
☑ 대가 * 가 없는 자문 등은 보고 사항 제외
* 금전, 유가증권 등 노무에 대한 보수 제공

과학기술정보통신부

IV. 질의응답

Q9.

해외 실험장비를 유상 구입 또는 무상 사용하는 경우도 '비금전적 지원' 보고사항인지?

☑ 외국의 시설·장비를 무상으로 또는 사회통념상 현저히 낮은 금액으로 증여·대여받는 경우 보고 사항임
☑ 해외 연구기관 또는 판매업체로부터 정당한 대가 지불 후 장비 구입 또는 사용하는 경우 보고 사항이 아님
☑ 외국의 시설·장비(표본·소모품 포함)에 대한 단순 공동활용은 보고 사항이 아님

Q10.

해외 정부·기관·단체 등에서의 겸직도 보고 사항인지?

☑ 대가가 있는 겸직은 보고 사항이며, 대가가 없는 명예직은 보고 사항이 아님

과학기술정보통신부

IV. 질의응답

Q11.

국외기관과 비밀유지계약을 체결한 경우 국가연구개발혁신법에 따른 국외수혜정보 보고가 가능한지?

☑ 비밀유지계약 등의 내용에 따라 보고가 곤란한 경우 지원기관·금액 기재 없이 보고 가능한 내용만 작성
※ "지원·지급 출처"에 해당국가명, "지원·지급 내용"에 "비밀유지계약 있음"으로만 기재

Q12.

단순 실수로 누락 또는 오보고한 경우 불이익은?

☑ 연구현장에 불이익이 발생하지 않도록 유연하게 제도를 운영할 예정

과학기술정보통신부

V. 사례적용

'24.3.10. 국가R&D과제(일반과제)를 협약한 연구책임자 A의 국외로부터 지원받은 사항이 아래와 같을 때 보고하여야 하는 국외수혜정보와 보고시기는?

		보고대상 여부	보고시기
1	B국 연구소로부터 '21.3.10.~'23.3.9.까지 연구과제를 지원 받음	–	–
2	B국 연구소에 자문료를 받고 '24.2.1. 자문 수행* * 자문수행일은 자문회의 개최/자문서 제출일 기준	–	–
3	C국 기업과의 공동연구과제를 '23.10.5. 신청하였으며 '24.3.11. 미선정 통보 받음	✓	국가R&D협약 시('24.3.10.) ※ 미선정 통보 후 수정(삭제) 가능
4	C국 연구소로부터 '22.4.1~'24.3.31.까지 연구과제를 지원 받음	✓	국가R&D협약 시('24.3.10.)
5	D국 대학과의 공동연구 공모과제*에 '24.4.5. 지원 * 선정여부 미정	✓	해외과제 신청 시('24.4.5.)
6	D국 기업의 연구시설을 '24.6.1.~'25.5.30.까지 무상지원 받기로 '24.5.1. 계약 체결	✓	해외와 계약 체결 시('24.5.1.)

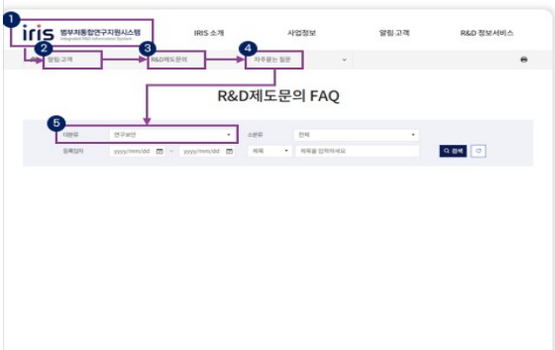
국가R&D과제 협약일('24.3.10.) 기준
계속 또는 예정된 국외지원정보 → 협약 시 보고사항 ○
종료된 국외지원정보 → 협약 시 보고사항 X

국가R&D과제 수행 중
발생 또는 예정된 국외지원정보는 보고사항임

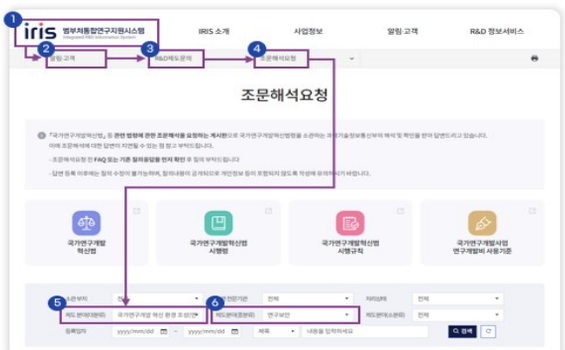
과학기술정보통신부

VI. 문의처

- **연구자는 소속 연구기관 문의가 우선**
  - 연구기관 → (대응이 어려운 경우) → 전문기관 → (추가 유권해석이 필요한 경우) → KISTEP
- **IRIS 제도문의 게시판**(www.iris.go.kr)



① IRIS → ② 알림·고객 → ③ R&D 제도문의
④ 자주묻는질문 → ⑤ [대분류] 연구보안



① IRIS → ② 알림·고객 → ③ R&D 제도문의
④ 조문해석요청 → ⑤ [대분류] 국가연구개발혁신환경조성
⑥ [중분류] 연구보안

29


감사합니다
국외 수혜정보 보고 제도 교육(안)
과학기술정보통신부

참고 2 연구보안 현장지침(가제) 본문(예)

제1장 보안관리체계

1.3 연구보안책임자 지정

☞ 현장의견과 내실화방안에 따른 1)과제등급별, 2)기관유형별 맞춤형 안내지침 작성

해당과제		
일반과제	민감과제	보안과제
O	O	O

기관유형		
대학(학)	연구소(연)	기업(산)
	O	

국가연구개발혁신법

제21조(국가연구개발사업 등의 보안) ③ 제2항에 따라 보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는 보안관리 조치를 하여야 한다.

국가연구개발혁신법 시행령

제46조(보안관리 조치) 법 제21조제3항에서 "보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는 보안관리 조치"란 다음 각 호의 조치를 말한다.

7. 보안책임자 지정

연구보안책임자 지정의 필요성 ☞ **관련법령 및 제도기반 해석에 따른 필요성/배경 제시**

- 연구기관의 연구개발 보안업무를 철저하게 수행하고, 지속적으로 관리하기 위하여 연구기관의 장은 연구보안관리 업무를 전담해서 처리할 수 있는 연구보안 관리자(연구보안 책임자 및 담당자)를 지정하여 임명하여야 함

연구보안책임자의 임무 ☞ **지침에 대한 주요내용 설명**

- 연구보안 관리를 위한 종합계획 수립 및 이를 효율적으로 운영하기 위한 지도 감사 및 교육 진행
- 연구보안 관리와 관련된 전반적인 보안조치 수행
- 연구보안 사고를 사전 예방하기 위한 정기 연구보안 실태 점검
- 연구보안 미진사항에 대한 보완책 마련 및 보안사고 방지를 위한 절차 수립
- 연구보안 업무를 효율적이고 체계적으로 수행하기 위한 연구보안심의회 운영 및 관리
- 각 연구개발과제에 대한 연구보안 규정 준수 강화를 위한 분임연구보안 책임자 및 분임연구보안 담당자의 지정·운영

참고3 연구현장 관계자 의견 수렴을 통한 시사점 도출 결과

○ 학제 및 산학연 분야별 연구자의 연구보안 현장 인식 의견 수렴

주요 이슈	학	연	산	비고
연구보안 정책인식 (필요성/ 방향)	· 연구보안의 필요성은 공감되며 정책의 틀을 잡아나가야 할 시점이라고 생각됨 · 장기적으로 연구계를 설득해 가며 기존 정책과 공존 필요 – 국제협력 강화·성과강조 등과 상충이 있는 것으로 느껴짐 – 최근 예산삭감으로 어려운 시점에 추가 압박으로 인지 가능 – 만약 연구보안이 제재로만 작용할 시 민감·보안과제 기피현상 발생 가능	· 기존 보안 관련 경험이 쌓였기에 연구보안 내실화방안 취지와 개념에 긍정적임 · 단, 현재 국정원, 과기부, NST등 다양한 채널로 연구보안이 이루어져 현장 혼선 존재 · 감사 대상으로 활용될 우려	· 민간 입장에 대한 고려가 부재한 것은 사실 · 기업규모가 클수록 자체 연구보안 관리 수준*이 고도화되어 있어 별도의 연구보안 정책은 규제로 간주하는 경향** * 기본적인 인프라(IT, 시설출입 등) 관리 ** 공동연구 등 협약-계약 단계에서 법리적 검토를 통한 예방조치 및 사후조치 체계 구축	· 부처 간 협업통한 안내로 현장 혼선 감소 필요 · 자율적인 연구보안 문화 형성 필요성
연구보안개념	· 연구보안은 산업보안과 달리 자산 유출 시 '신산업태생, 국부창출, 기술선점 판도'에 장기적 악영향을 주는 개념	· 연구수행 전반을 아우르는 물리적보안(카드키, 출입통제 등)부터 연구성과물(연구데이터)까지로 개념이 포괄적 · 연구보안의 범위가 넓어 상세한 부분은 기관 가이드만 준수하면 된다고 생각함	· 과제관리와 성과물 관리, 시설보안, 정보보안을 구분하지 않고 "보안"으로 뭉뚱그려 접근하는 경향 · 많은 경우 기업의 연구활동은 프로젝트 단위로 이루어짐을 감안할 필요	· 현장 연구자가 체감 가능한 연구보안 및 범위 개념 제시 · 산업보안과 구별되는 연구보안의 특징에 대한 공감대 형성은 필요함
연구자산개념	· 기존 전통적인 5대 보안영역 외에 학제에 따라 연구자산 다각화* * 셀·프로토콜·연구노트·데이터·특허·소재 · 인적 노하우가 가장 큰 자산 – 사람의 이동으로 인한 자산유출이 가장 치명적	· 과제를 통해 생산되는 연구데이터와 연구성과물, 연구수행 중 활용되는 연구장비, 연구재료를 연구자산으로 인식 · 연구산출물인 논문, 지적재산권 뿐 아니라 경제적 가치를 생성하게 하는 성과를 모두 연구자산으로 인식	· 연구활동의 투입-산출물을 총체적으로 자산 개념으로 접근하므로, 기본적으로 대학이나 출연연과 대동소이한 인식 · 특히, HR 및 특허, 영업비밀 위주로 관리하고 있음	· 연구자산·보안에 대한 현장 적용 대상개념 구체화 및 명확화

주요 이슈	학	연	산	비고
학제별 개방성의차이	· 기술수준이 낮은 분야는 보안정책보다 개방성을 더 높이는 방향성 필요 – 전반적으로 아직 해외에서 배워야 할 것이 훨씬 많은 상태 · 학제 별 개방성 수준 및 문화가 다른 점 고려 – 기초분야의 시설장비 무료사용 등 학문발전을 위해 공유하는 부분이 많으며 개방성 높음	· 기술수준이 높아졌다 하더라도 앞선 해외기관은 늘 존재 · 융합연구와 도전형 연구를 위해서는 해외 협업이 필요 · 특정분야(생명)에서는 글로벌 진출(인허가 등)을 위해 반드시 국제협력이 요구됨 · 국제협력 참여 위해서는 우리가 가진 기술을 보여줘야하고 경쟁도 필요하므로 결국 기술을 공개하게 됨 -산업보안의 경우 철저히 지켜지나 전체 보안은 어려움	· 민간부문 특성 상 적용하기 어려운 개념임 – 협업 자체의 개념이나 적용은 학·연과 크게 다르지 않음 아쉬운(경쟁사 대비 열세 등) 경우에 협업 추진 등	· 학문 및 분야 별 보안수준이 달라질 수 있으며 이해관계자 공감대를 기반으로 한 정책 추진 필요
연구보안 현황	· 실험실을 옮겨다니며 학생들이 배우는 부분이 많기에 보안조치가 많지 않음 · 유학생이 실험자료를 자국으로 보내는 경우도 있으며 교수들에게 천인계획 참여 요청 메일이 오는 경우 있음 · 지메일, 드랍박스 사용하는 교수들 다수이며 대학 별 정보통신망 환경이 다름	· 기관차원에서 국정원 연구보안평가 등 지속적인 평가가 이루어짐 · 개별적인 사고가 발생할 경우 내규 지침등으로 제재를 받으나 현장에서는 원인-결과 부분에 대한 이해도는 낮음 – 단순한 인자상의 문제로 동일 실수가 발생 · 해킹 공격도 그간 다수 받아 왔기에 정보통신 체계 견고 – 출연연 내부 민감과제 수행자는 원내망을 별도 분리하는 등 보안상태 철저 – 민감분야의 경우 외부메일 송부시에도 결제필요	· 대기업으로 갈수록 유출의 창구는 기업 내부보다는 퇴직자나 협력사인 경우가 많음	· 산학연 보안 현황준수가 제각각 이어서 개별 입장 고려 필요 · 연구보안을 준수하 있으나, 구체적인 사항에 대한 설명 필요 · 각 상황에 발생되는 문제가 다르면 대학의 경우는 컨트롤타워가 부재함

주요 이슈	학	연	산	비고
연구보안 현장체감 개선방법	・일반적인 문서정보만으로 연구보안 인식개선에는 한계가 있음 ・기존 보안과제 관리현황, 사고사례에 대한 분석으로 연구자를 설득해야 할 필요 있음 ・다양한 사례분석(국방·원자력·금액 고려)으로 중점분야 도출한 핀셋 정책 필요 ・'과기원' 위주 시범사업 적용으로 현장파악 바람	・다양하게 발생하는 연구현장내 연구보안 문제에 이해도가 낮음 ・상황에 따라 발생하는 연구보안의 심각성을 체감하지 못하거나, 주의사항에 대해 인지하지 못함 ・일상과 연구수행이 동일시되어 인지하지 못하는 경우가 발생 ・알기쉬운 상황별 연구보안교육이 필요	・대기업으로 갈수록 출연연과 유사한 편	・사례분석·시나리오 개발로 현장에서 체겸할 수 있도록 안내
민감기술 분야	・학제 별 학자들의 공감을 살 수 있는 민감 테마는 존재 - 생명과학은 오가노이드 분야가 국부창출에 영향 - 농업은 종자분야가 첨예하며 인건비가 싼 개도국으로 기술 유출 시 산업지형 변화를 일으킬 수 있음 - 배터리/소재는 효율성을 변화시킬 수 있는 프로토콜 연구가 민감 - 정보전자의 경우 PCT출원할 정도면 민감한 과제라고 봄, 빠른 표준 선점을 위한 과제 중요 - 기초분야는 기술이 어떻게 확장될지 예측 불가함	・원자력 분야 전체가 민감기술로 지정될 수 있는 것은 아님 - 원자력 건설 운용은 세계공통이며 우리나라도 미국 대비 60% 기술수준, 설비 능력이 수출 당락 결정 - 원자력 운용 비밀자료는 운영 노하우로 산업비밀에 해당되며 국제협력시에도 상호 비밀을 유지 ・원자력 분야는 SMR 등 원천 기술, 우주결합 분야가 민감기술임 - 우주선 탐사 시 에너자원천으로 무엇을 쓸 것인가 아직 표준 정립이 되지 않아 나라별 독특한 기술확보 경쟁 심화 - 우주선 제작 관련 대학 협조 시 외국인 연구원들도 참여하고 있는 것으로 알고 있음 - 우주청 설립 시 민감과제 지정 다수 필요	・분야를 특정하는 경우는 드물고 보안등급에 따라 접근성 관리 등 일련의 보안조치를 적용하는 방식을 채택* * Apple 등 해외 기업도 유사	・학계의 공감을 살 수 있는 민감과제 지정이 중요

주요 이슈	학	연	산	비고
민감과제지정	· 연구관리의 '예측가능성' 필요하므로 기획단계부터 민감과제 지정 검토 · 미국 등도 민감과제는 극소이며 소규모 지정 필요 · 민감과제 선정은 중앙행정기관장(전문기관)의 고유 역할로 정량적 판단이 어려움	· 보안과제와 민감과제의 명확한 기준이 필요함(모호한 기준은 혼돈을 가져옴) · 기술수준이 낮은 과제는 민감과제 대상 제외 · 전문기관이 다루는 과제 중 평균 보다 금액이 높은 과제, Top-down 과제를 분석한 후 그 외 전문기관 재량에 따라 지정 · 민감과제 수가 증가 시 행정부담이 커질 수 밖에 없음	-	· 기술 수준이 높은 분야 위주 민감과제 지정하는 것 고려 · 연구기획부터 평가까지 연구자 예측가능성 고려하여 민감과제를 시작부터 지정 필요 · 민감과제 정의를 명확하게 해야함
해외수혜신고제도	· 김영란 법제도와 유사성이 높아 기술유출 방지 목적을 위해 운영되는 것인지 의문 →시설장비 무료사용, 대가성 없는 금전 지급, 모호하게 지급되는 실비 등 사례 다수 · 실제 연구가 되는 부분에 대해서만 신고하는 것이 바람직 - 대규모 국제공동 연구 참여 시 가진 것을 보여줘야 참여 가능하며 이때 기술 유출 가능	· 기본적인 김영란법을 준수하는 해외출장 신고제도, 해외 학회발표, 보안과제 시 외국인 접촉 신고 등은 운영 중 · 세부신고 사항은 출연연 보안등급에 따라 차이가 있고, 구체적인 가이드라인은 부재	· (대기업) 국가과제 수행 빈도가 낮아 해당 사항이 없다고 생각 · (중소기업) 대부분 해외수혜를 기대하기 어려운 기술 수준인 경우가 많아 신고할 일이 없다고 예단하는 경향	· 24년 실시되는 해외수혜 신고에 대한 안내가이드 필요 · 산학연 입장 별 FAQ 구성 고려
과제평가/성과공개	· 과제평가 불이익 등 방지 - 민감/보안과제라 논문화 하지 못하거나, 성과가 비공개되어 평가 불이익을 받게 될까 불안 - 젊은 교수의 경우, 평가 불이익을 받게되면 승진 등에 문제	· 수행중인 과제의 성과공개(논문,특허이전)가 불가능하면 연구실적평가 등에 불이익이 생길것이라 여김 · 현 평가체계에서 민감/보안과제로 분류되는 것에 부정적임	· 민감보안과제 참여 시 성과공개 관련 기업경영 타격이 있으므로 '미래가치 실현'을 참고한 보상방안 등 검토 필요 · 대기업으로 갈수록 논문은 게재에 소극적이라 큰 관심이 없고, 특허의 경우 전담부서가 알아서 관리하므로 대학이나 출연연 대비 사안의 심각성에 대한 인지도는 미흡	· 충분한 사전설명과 민간/보안과제의 평가, 성과공개시 보상방안에 대한 현장 논의 필요

주요 이슈	학	연	산	비고
인센티브	· 국가를 위해 희생한 부분이 있다고 생각하기 때문에 합당한 조치 필요 · 제재나 감시가 많아진다면 인센티브가 크게 매력적 요인은 아님	· 보안수당의 경우 기존 운영제도가 연구자에게 더 이익이 컸음(ETRI) · 인력공급이 아닌 이상 금전적인 인센티브는 한계를 갖고 있으며, 연구비내 연구수당부분은 장기적인 매리트가 없음 · 행정부담이 증가되는 상황에서 인센티브(연구수당)은 동기부여가 어려움(연구자의 본업이 연구인데 연구시간을 할애해서 행정지원을 하는 것은 무의미)	· 인터뷰 대상자들은 대체로 관심이 없음(고려 자체를 안 하는 수준) - 민간의 경우 국가과제 수당에 메리트를 느끼기 어려우므로, 당연한 귀결에 가까움	· 동기부여가 될 수 있는 인센티브에 대한 아이디어발굴 필요
보안사고 처분	· 대학에서 기술이 유출되었다는 것을 입증하는 것 자체가 어렵고 번거로운 일임	· 기관규정에 따라 처리함(국정원법, 혁신법 등)	· 국내 기업은 예방적 조치에 중점을 두는 경향인 반면, 특히 미국계 기업은 사후 조치에 방점을 두는 편 - 평소에는 개인 자율(integrity)에 의존하나, 문제 발생 시 파멸적 페널티 부여	-
외국인 연구자 /유학생	· 유학생은 국부창출의 인적자산이므로 흡수 필요하나 민감기술 분야는 유의 필요 - 인구감소와 지방대 소멸, 교육부의 유학생 30만 유치운동으로 앞으로도 증가 예상 - 지방대는 학생이 적어 유학생도 민감한 연구를 수행할 가능성 높음 - 학생적응을 위한 지원만 존재하고 별도 보안관리는 없음 - Lab 실에서 학생을 차별하여 연구를 분리시키기 어려움 - 정책적 행동강령, 분리요구 등 필요할 것임	· UST 학생은 5~6년 출연연 상주하며 연구 노하우 체득하며 일부 우려사항 존재 - 연구원마다 차이는 존재하나 많은 외국인연구자들이 포닥, 학생신분으로 근무하며 많은 역할 수행 · 기관차원의 외국인연구원만 별도로 관리시 담당 연구책임자입장에서는 과잉대응이라는 인식도 있음(잠재적 범죄자)	· 실무자 급 외국인 연구자의 보안서약의 수행과 이행 관리 등은 대기업으로 갈수록 강도가 높음 · 대기업은 Leader급에 해외에서 스타 연구자를 영입하는 경우가 잦은데 이러한 인력들에 대한 보안관리는 오히려 느슨한 편	· 연구원내 외국인 연구원의 사전 보안서약 등 보안개념 강화 및 담당 연구책임자도 공감할 수 있는 보안교육 필요 · 민감 과제 이상 유학생 접근 제한 행동강령

주요 이슈	학	연	산	비고
퇴사자 /은퇴자	· 은퇴자 동향 파악은 거의 불가	· 퇴사자의 경우, 기존 연구원 자산이 개인소유라는 착각을 갖기도 함 · 이직, 창업을 통한 인력유출도 일어나고 있으며, 연구자산(성과, 데이터 등)도 같이 유출됨 · 원자력 분야의 경우 중동 원자로 수출과 맞물려 다수 은퇴자들이 진출 중에 있음 · 퇴직 시, 은퇴 회사 지식을 활용하지 않아야 하지만 체득 노하우는 어쩔 수 없음	· 퇴사자가 협력업체와 연계하여 유출하는 사례는 언론지상을 통해서도 자주 보도됨 – 사실상 가장 주요한 유출 경로가 퇴사자와 협력업체 · 글로벌 대기업으로 갈수록 협력사 연구보안 관리를 본사만큼 하기 어려운 경우가 대부분	· 국가핵심기술 또는 주요 연구자들에 대한 연구자 풀 구축 등 제도적인 인력관리가 필요함
사업화	· 창업 시 금전이 오고가므로 기술유출 유혹이 다수 존재 · 기술이전 성과가 중요한데 중국 투자를 받으면 손쉽게 기술이전이 이뤄짐	· 기술이전등으로 기술유출은 의심됨 · 정부지원으로 설립된 기업이 M&A 되어 해외로 넘어가는 방향이 옳은 것인지 알 수 없으나 민간활동이므로 간섭 어려움 · 별도로 국가연구개발 성과에 대한 추적이 진행되지 않고 있음(5년이 지난 후)	–	· 기존 국가연구개발 성과창업 대한 규정 등에 연구보안 인식과 유출방지에 대한 검토 필요
교육	· 연구보안은 결국 연구윤리, 진실성 문화와 귀결되므로 인식개선 위한 교육 필요	· 연구윤리와 같은 온라인교육처럼 연구보안 온라인교육이 실시되도 긍정적임 · 현재 KIRD에 교육이 있으나 좀더 구체적인 상황과 자세한 내용이 있었음 함 · 민감 분야 연구를 하더라도 해당 분야에 지속적으로 몸담고 있으면 해이해지는 순간이 반드시 찾아오므로 반복적 교육이 중요할 것임	· 연구당사자에 대한 교육보다는 사내 보안체계의 고도화에 의존하는 경향	· 단편적인 지식전달 교육이 아닌 현장에서 활용할 수 있는 교육컨텐츠가 필요함

주 의

1. 이 보고서는 과학기술정보통신부의 수탁을 받아 한국과학기술기획평가원에서 수행한 혁신정책지원사업 「국가R&D 보안정책 설계를 위한 기초연구」 연구개발과제 최종보고서입니다.

2. 이 연구개발내용을 대외적으로 발표할 때에는 반드시 과학기술정보통신부(한국과학기술기획평가원)에서 시행한 혁신정책지원사업의 결과임을 밝혀야 합니다.

3. 국가과학기술 기밀 유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 아니 됩니다.