

일본의 경제 안보 중요기술 관련 기술 유출 방지 대책 논의

[애자일] KIAT 산업기술정책단 정책기획실('23.7.2)



- ◆ 폐쇄적 혁신에서 벗어나 국경을 초월한 글로벌 개방형 혁신이 필요한 현 상황에서 경제 안보와 관련된 중요기술 유출 방지를 위한 일본의 사례를 공유하고자 함
※ 경제 안보상의 중요기술에 관한 기술 유출방지책 제안(日 내각관방 내 경제안보입법자문단, '24.6)

0. 검토 개요

- **(개요)** 일본은 경제 안보상 중요기술의 기술 유출 방지를 위하여 내각관방 내 「경제안보입법자문단」에서 관·민 기술협력 체제로 기술 유출 현황 분석, 방지·지원책, 리스크 매니지먼트 등 검토
 - 국제 동향과 국제화를 염두에 두고, 특히 국가가 지원하는 연구개발 프로그램에서 필요한 기술 유출 방지 대책 및 리스크 관리에 대해 3번에 걸쳐 검토
 - * ('24.03) 국가 간 경제 안보상 중요기술의 공동연구 추진
 - * ('24.04) 경제 안보상 중요기술 관련 연구개발 성과의 사회적 공유 및 기술 유출 대책 검토
 - * ('24.05) 그간 회의 최종 검토 및 정리
- **(주요 검토 사항)** 대학·연구기관의 연구 무결성(Research Integrity)* 및 연구 보안** 대책 및 국가연구 개발사업 결과 공개 시 기술유출 방지 등 검토
 - * G7에서는 연구의 정당성, 사회적 관련성, 책임 및 품질을 확보하여 지키기 위한 직업적 가치관, 원칙 및 모범사례 준수로 정의
 - ** G7에서는 경제적·전략적 리스크 및 국가적·국제적 안보 위협을 초래하는 행위자 및 행동으로부터 연구 커뮤니티를 보호하는 활동으로 정의
 - **(연구 보안·무결성 대책)** G7 국가, 주요국 논의를 참고, 경제 안보상 중요기술 관련 국제협력 확대를 위하여 국가연구개발사업에 관해 연구 성과 공개를 전제로 한 대학·연구기관의 연구 보안·무결성 대책 논의
 - * 경쟁적 연구비를 투입하는 연구개발사업에서 정부지침에 근거한 연구 무결성 대책이 철저히 이루어져야 하는 사업
 - * 국제공동연구 대상국으로부터 요구받는 사항, 외국의 선진적 대처에 동등한 연구 보안 대책이 필요할 경우 등
 - **(기술유출 방지)** 국가연구개발사업 성과의 사회적 환류 시 국제적 대응 및 산업경쟁력 강화를 위하여 기술유출 방지에 필요한 대응책 검토
 - * 일본의 현재·미래 기술 우위성 강화가 필요한 기술 영역 위주이며, 우방국 등의 대응 방안 및 공급망 강화, 기업 등의 영업비밀 관리에서 기술 유출 방지 대책 참고

- **(한국의 유사 활동 현황-산업기술보호위원회)** 한국에서는 「산업기술보호위원회」에서 산업기술보호와 관련된 종합계획 수립 및 국가핵심기술의 수출 등을 심의·의결을 하고 있음
 - **(기능)** ▲종합계획 수립 및 시행, ▲국가핵심기술 지정·변경 및 해제, ▲국가핵심기술(국가첨단전략 기술)의 수출·해외M&A 등 심의·의결
 - * (근거) 산업기술보호법 제7조
 - **(구성)** 산업통상자원부 장관(위원장), 관계부처 차관급*, 민간전문가** 등 25인
 - * 기재부·교육부·과기정통부·외교부·법무부·국방부·농림부·복지부·환경부·국토부·해수부·중기부 차관 및 특허청장, 국가정보원장 지명자(14명)
 - ** 위촉직 위원(10명) : 임기2년('22.3.15~'24.3.14)
 - **(심의절차)** 분야별 전문위원회 사전심의 → 산업기술보호위원회 심의
 - **(운영실적)** '23.11월 기준, 총 6회 개최 41건의 안건 처리(의결41, 보고5)

[산업기술보호위원회 안건 처리 현황]

구분	수출승인	수출 불승인	M&A 승인	제도개선 등	계
'22년	8	1	1	3	13
'23.11월	41	-	-	5	46

* '22년 총 3회 개최, 안건 처리 총 13건(의결12, 보고1)

<참고> 제47회 산업기술보호위원회('23.12) 개요 및 결과

* 산업부 보도자료 참조

- (의결안건) 국가핵심·국가첨단전략기술 수출·해외M&A 승인(총12건)
 - 해외자회사 생산 및 소송대응을 위한 국가첨단전략기술자료 반출 → 수출승인
 - 수소자동차 관련 기 승인 수출대상 변경 및 해외 공동개발을 위한 국가핵심기술 자료반출 → 수출승인
 - 해외 투자유치에 의한 최대주주 변경 → 조건부 해외 M&A승인
 - 특허소송 대응 및 의약품 해외 인허가를 위한 국가핵심·첨단전략기술 자료 반출 → 수출승인
- (보고안건) 산업기술보호법 개정 추진동향 및 향후 과제
 - ① 산업기술보호법 주요 개정 내용
 - (처벌강화) ▲벌칙 강화, ▲침해행위 확대, ▲징벌적 손해배상 한도 상향
 - (관리강화) ▲보유기관 등록제 신설, ▲실태조사 강화, ▲과태료 대상 확대
 - (심사강화) 해외인수합병 승인 관련 ▲심사항목 추가, ▲대상기관과 함께 외국인에게도 공동신청 의무 부여
 - (기업지원) 기술보호를 위한 보안시설 설치·운영 지원근거 마련 등
 - ② 후속 조치
 - (시행령 후속 개정) 법 개정사항을 반영하여 법 공포일로부터 6개월 이내에 시행령 후속 개정
 - (기반 구축) 기술유출범죄 처벌 실효성 제고를 위한 기반 구축
 - (실태조사 강화) 현장중심 정책기반 조성을 위한 현장실태조사 강화

1. 경제 안보 중요기술 공동연구

- **(배경·현황)** 기술은 국가의 자율성·필수성의 중요한 부분을 구성하고, 국가 과학기술력 향상을 위해 개방적이고 자유로운 연구 환경 확보와 국제협력 추진 필요성이 있으며, 이에 따른 연구 보안·무결성 대책 또한 필요
 - 연구활동의 국제화·개방화에 수반하는 연구비 부정 사용 및 기술유출 리스크가 지적되고 있으며, 관련 대책은 경제 안보상 시급한 과제로 대두
 - 주요국에서는 경제 안보상 중요기술에 대한 정책을 발표하고, 양·다국가 간 협의 시에도 관련된 논의가 활발해지고 있으며, 동맹국 간 협력의 필요성이 높아지고 있음
 - G7에서는 「연구 보안과 무결성 관련 G7 공통 원칙」에서 연구 무결성과 연구 보안의 정의를 내리며 강조함
 - 「G7 Best Practice for Secure & Open Research('24.2)」에서는 연구 보안 및 무결성의 모범사례를 정리하여 공유
 - * ①연구 보안 위험에 노출된 연구 영역의 특징과 정보 공유, ②「Due Diligence 6」를 실시하고 투명성 및 관련 정보의 공개를 보장함으로써 위험한 활동 영역의 개별 연구 프로젝트에 대한 리스크 경감책 실시, ③연구 관계자 간 연구 보안·무결성 관련 대화·정보공유의 장, 인식 개선 활동 확립 등
 - * Due Diligence : 실사(5p-② 참고)
 - 특히, 국가 간 경제안보상 중요기술 공동연구 추진 시 외국 또는 단체에 의한 연구 부당 간섭 방지를 위한 연구 보안 관점에서 노력이 중요하고 책임 있는 국제협력을 추진할 필요가 있음
 - 주요 국가들도 연구 보안 노력을 추진하고 있으며, '24년에는 EU 및 캐나다가 관련 정책을 발표하였고, 미·일정상회담('24.4) 공동성명에서 경제안보 강화 문구*를 추가하였음
 - * 중요·신흥기술의 진흥 및 보호 등에 의해 미·일의 기술적 우위성을 높인다. 이와 함께 경제안보를 강화한다.
 - 일본에서는 지금까지 내각부(과학기술·이노베이션 사무국)를 중심으로 연구 무결성 확보에 대한 대응 방침을 수립하였지만, 기밀정보 누설 및 사이버 공격 사태* 등으로 연구 보안 관점에서의 대처가 요구되고 있음
 - * 산업기술종합연구소 외국연구자 기밀 정보 누설('23.6), 우주항공연구개발기구 사이버 공격('23.11)
- **(주요국 동향)** 국가별로 연구 보안의 정의·범위 등은 다르게 인식하고 있으나 큰 틀에서 연구 보안의 필요성에 대해서는 각국에서 중요하게 인식하고 있음
 - **(미국)** NSPM-33* 및 NSPM-33 실시기이드에서 연구 보안이 명확히 정의됨과 동시에 정보공시 요건, 프로세스 강화, 리스크 식별·분석 등 자국정부 지원 연구개발사업을 외국으로부터 보호하기 위한 지시가 이루어졌고, 「CHIPS·과학법('22)」을 포함하여 관계 부처나 미국과학재단(NSF) 등의 연구 보안 정책이 진행되고 있음
 - * 미국정부지원의 연구개발에 관한 국가안전보장 대통령령 각서 33호('21)

- (캐나다) 「연구파트너십에 관한 국가 보안 지침(’21)」 발표 및 실행 중이며, ’24년에는 「Sensitive Technology Research Areas」와 「Named Research Organizations」를 공표하여 민감 기술과 관련 연구기관 관련 연구 보안을 확보하기 위한 정책이 진행되고 있음
- (EU) 유럽경제안보전략 실시의 일환으로 경제안보 전략 패키지를 발표(’24.1), 이후 연구 보안에 관한 이사회 권고*를 채택하여 회원국에 대해 권고를 진행하고 있고, 유럽위원회에 대해서도 「European Centre of Expertise on Research Security」의 설치를 포함한 보다 구조적인 지원 옵션을 검토하고 평가한다는 11가지 권고가 이루어지고 있음
 - * 연구 보안 활동 지침 및 목록 수립, 지원 서비스 기관 창설, 정부 내 분야 횡단적인 협력의 강화, 연구 관련 기관 관련 내용 등
- (영국) 국제연구협력 무결성을 위한 「Trusted Research 캠페인(’19)*」을 진행 중이고, 대학에서는 연구 협력 지원팀을 설치하여 국제공동연구 시 국가 안보상 리스크를 상담·지원하며, 정부에서는 영국 내 대학을 외국의 기술안보 위협으로부터 보호하기 위한 협의를 시작한다고 표명함
 - * 영국의 연구자, 대학, 산업계가 국제협력에 자신을 가지고 잠재적 리스크에 관해 충분한 정보에 근거하여 의사결정할 수 있도록 지원하고, 잠재적 리스크로부터 보호하기 위한 대처이며, 관련 가이드를 지속적으로 발굴
- (호주) 정부·대학·ARC* 공동 TF에서 「대학 섹터에 대한 외국 간섭 대항 가이드라인」을 발표하였고, 이 가이드라인에 근거하여 각 대학 자체 대처를 실시하게 하며, ARC에서 필요한 경우 리스크 검토를 진행토록 함
 - * 호주 연구 평의회: 호주 연구개발 자금 배분 기관
- (일본) 통합혁신전략추진회의(’21.4)에서 연구 활동의 국제화, 개방화에 따른 새로운 리스크에 대한 연구 무결성 확보 대응 방침을 결정하고, 관련 가이드라인·체크리스트 제정, 후속 조사 등을 실시하였고, 국립연구개발법 개정(’24.3) 시 연구 보안, 무결성 확보 등을 포함한 관계부처 신청을 공표
- (연구 보안 대책) 개방적이고 자유로운 연구 환경을 확보하고, 동맹국 등과 대등한 입장에서 국제공동 연구를 실시하기 위한 연구 보안 대책 필요
 - 미국을 비롯한 각국 문서에도 밝혀지고 있듯이, 연구 개방성 및 협력의 중요성은 인식되고 있으나, 일부 국가는 개방적 연구 환경을 이용하여 연구비용과 리스크를 회피하며 부당하게 자국 경쟁력을 증대시키려고 함
 - 이를 방지하기 위하여 연구 성과 공개 원칙 등을 유지하고, 개방적이고 자유로운 연구환경을 확보한 후 국제협력을 추진해 나가기 위해 연구 보안 관련 정책을 검토하여야 함
 - 그리하여, 동맹국 등 제도와 실태를 바탕으로 일본의 경제안보상 중요기술 육성 및 상대국과 대등한 국제협력을 확대하기 위하여 이하 G7의 정리에 따라 조치 방안을 강구

① 위험에 노출되는 연구 영역의 식별 및 정보 공유

- 지금까지 실시해온 연구 무결성 대처를 기반으로 위험에 노출되는 연구 영역 및 특정 영역의 국제공동연구 추진을 하고, 외국의 선진적 대처와 유사한 연구 보안 대처가 필요
- 검토 시 연구현장 관계자들과 긴밀한 소통이 중요

② Due Diligence*를 실시하고, 투명성·개방성을 확보하여 리스크가 있는 영역을 특정하고 표준 조직 관행으로 위험 완화 조치를 시행

- * 실사라고 이해되며, 사전적 의미는 어떠한 사업에 있어 의사결정 이전에 적절한 주의를 다하고 계획을 수립하여 수행하여야 하는 주체의 책임 즉, 소정의 절차에 따른 조사 행위
- 경쟁적 연구비 투입 프로그램의 경우 연구 성과 공개를 전제하며, 정부 지침에 근거한 연구 무결성 대책이 Due Diligence와 연결되도록 연구자·연구기관이 사용할 수 있는 가이드라인·체크리스트를 확인하고 유관기관에서 철저한 검토를 실시
- 특정 영역에서는 국제공동연구 대상국 또는 동맹국 등과 유사한 연구 보안 노력 필요
- * 외부데이터 리소스 이용 또는 연구기관 간 컨소시엄을 결성하여 실사를 수행하는 메커니즘 등으로 오픈소스·Due Diligence 등에 의한 Risk Management 실행도 검토

③ 연구관계자 간 연구 보안·무결성 관련 소통·정보공유를 위한 인식을 증진시키는 자원 확립

- 연구비 제공 부처·기관 활동뿐만 아니라 수사·공안당국, 법률 집행기관 등의 정부 내 관계기관 간 제휴를 촉진할 필요가 있음
- 또한, 관련 기관을 중심으로 상담·지원센터를 설치하고, 정부과 연구계 간 쌍방향 정보 교환의 장을 만들고 그 기능을 강화할 필요가 있음

● 향후 과제

- 관계 부처 간 긴밀한 연계를 통하여 대책을 강화할 필요가 있고, 경제 안보를 둘러싼 국제적인 움직임에 대응하기 위해 연구 보안·무결성에 관한 리스크를 특정하는 분석력의 강화가 필요함
- 연구 보안·무결성 대책 추진 시 특정 국가·연구자 차별이 생기지 않도록 유의할 필요가 있음
- 유관기관 규모와 실정에 맞는 연구 보안·무결성 대책 추진을 위하여 체제 정비 및 선진적인 대책 방안을 강구하고, 본 대책 및 종합과학기술·이노베이션 회의 검토자료를 근거로 정부·관계기관 간 공통 방침을 수립하고 실천해 나가야 함

2. 연구개발 성과의 기술유출 방지

- **(배경·현황)** 지속적인 기업 영업비밀 누설 사건이 발생하고 있으며, 향후 그 부작용으로 중요기술의 대외 의존도가 높아질 우려가 있음
 - 산업기술종합연구소 직원의 부정경쟁방지법 위반 체포('23.6) 등 기업의 영업비밀 누설을 둘러싼 사건이 지속되고 있는 상황
 - * 미국에서는 CHIPS·과학법을 제정('22.8)하고 반도체 설비투자 등 지원 기금을 포함하여 5년간 총 527억불을 지원하고, 지원 대상자로부터 안보 우려국에 대한 기술 라이선스나 제조 능력 확대를 금지하는 가드레일 조항 발표
 - 기술유출의 경로는 크게 '상품', '금전', '사람'으로 볼 수 있고, '상품'과 '금전'에 의한 기술유출 시 외환법에 따라 수출·투자통제 대상이 되고, '사람'의 경우 불법적으로 영업비밀을 취득·유출 시 부정경쟁방지법 적용을 받음
 - 따라서, 경제보장촉진법('24.3)에 따른 공급망 지원 시 특정 중요 소재·부품 관련 핵심기술이 유출될 경우 향후 대외 의존도가 높아질 우려가 있음
 - * (참고) 일본기업 770개사 대상 설문조사 결과, 영업비밀 유출 탐지를 하지 않는 기업은 영업비밀 유출을 경험하지 못했다고 응답한 반면, 탐지 활동을 하는 기업은 영업비밀 유출 경험을 해본 기업 응답 비율이 더 높음
 - **(정부연구개발사업 단계별 기술유출 방지책)** 일본 우위의 소재·부품 관련 정부연구개발사업 지원 시 시작부터 종료 시까지 기술유출을 방지하기 위한 조치 필요
 - **(주요 대상 분야)** i) 파괴적 혁신을 진행 중인 기술을 포함하여 미래 기술 우위 창출을 목표로 하는 기술 분야, ii) 일본이 기술적 우위를 가지고 있는 기술 분야 중 이미 특정 조치가 이루어지지 않은 각 부처 지원 R&D사업*
 - * 특히, 국제공동연구에서 협력대상국과 동등한 입장에서 수행이 필요한 경우
- ① 해당 연구개발 프로그램에서 요구되는 기술유출 방지 조치 요구 사항
- * 경제보장촉진법에 따른 공급망 지원에서는 이미 기술유출방지대책 요건이 정해져 있어 위 주요 대상 분야 연구개발 프로그램에 대한 대책을 마련하는 것이 효과적이고, 설계·생산·활용의 각 단계별로 대책이 필요
 - **(실사)** 연구개발 진행 단계별 기술유출 리스크 수준에 따른 실사 실시
 - * ex) 알 필요가 있다는 원칙을 바탕으로 각 프로젝트마다 개인의 동의를 얻어, 프로젝트에 접근할 수 있는 직원을 선정할 때 비공개 계약 체결, 정보 제공 등 각 프로젝트의 성격 안에서 진행 단계별 리스크 수준에 따라 필요한 실사 실시(개인별 정보관리 서약서 작성, 오픈소스 실사 실시)
 - **(리스크 관리)** 업무의 IT화에 따라 중요 정보가 적절하게 관리되고 있는지, 대량의 정보 유출 등 부자연스러운 행위는 없는지 모니터링을 실시하며, 해당 행위 확인 시 이메일 및 데이터 저장 관련 감사 시스템 구축

- **(규정 준수)** 전 직원이 준수해야 할 정보관리규정을 정하고, 이를 준수하기 위한 서명 및 사후 조치 실시
- **(인식 제고)** 내각부(과학기술혁신추진실)에서 발행한 연구 성실성 체크리스트를 참고하여, 회사 및 거래처에 대한 리스크 해소 노력 관련 사내 인식 제고 활동 실시
- **(부서 신설)** 경제안보 전담 부서 신설로, 관련 부서 정보 통합과 종합상담 서비스, 조직 간 리스크 관리 등 제공
- **(연구자 기피 방지)** 기술유출을 방지하기 위한 조치를 할 때, 사업에 참여하는 연구자의 지나치게 기피하지 않도록 각 사업의 특성과 위험성에 맞게 균형적이고 맞춤형으로 필요하고 충분한 조치를 취해야 함
 - * 연구자 기억에 남아있는 정보를 관리하는 과정에서 연구자의 과도한 기피를 초래할 수 있음

〈참고〉 기업의 독자적 노력을 통해 영업비밀 관리를 강화한 사례

* 사업의 국제화와 연구개발을 전제로 한 기업의 독자적인 노력을 통해 영업비밀관리를 강화한 아래 사례를 참고하여 주요 기술에 대한 접근 관리, 접근 가능 직원 관리, 거래처 관리 등 기술유출 방지 조치를 실행할 필요가 있음

① 기술에 대한 접근 관리

- 물리적 환경의 보안유지로 기업의 업무영역 내 단계별 보안구역을 구분하고, 각 구역 내에서 취급 가능한 문서 등의 정보 구분 명시
- 실제 생산·제조를 염두에 두고 각 연구개발단계에 따라 기술에 접근할 수 있는 직원의 범위를 적절하게 설계할 수 있도록 하고 직원에게 필요한 대우를 제공

② 기술에 접근할 수 있는 직원 관리

- 중요기술을 보유한 직원을 식별하고, 외부와의 접촉여부를 확인하여 리스크 관리
- 퇴직 후 경쟁회피 서약을 일정기간 유효하게 하기 위하여 스톱옵션 행사 또는 추가퇴직수당 지급을 조건으로 경쟁사 이직 불가 조항을 규정

③ 공동연구 파트너 등 사업 파트너 관리

- 거래처를 통한 기술유출 방지를 위해 거래처 리스크 평가 체크리스트를 작성하고, 거래처로부터 제출받은 정보를 바탕으로 리스크 평가를 실시하며 개방하는 부분과 폐쇄하는 부분을 잘 구분하여 전략적 협력을 실시

② 일본판 Bayh-dole 제도* 관련 규정에 대한 쟁점 해소 필요

* 대학 등 비영리기구가 연방정부의 지원을 통해 창출한 발명의 특허권을 연방정부에 귀속시키는 대신 자체적으로 소유하고 활용할 수 있도록 하는 제도(1980년 제정, 미국)

- 현재, 정부가 산학연에 위탁한 R&D사업의 결과로 취득한 결과물의 특허권 등 지식재산권은 일본 산업기술진흥법 제17조에 따라 위탁받은자에게 귀속시킬 수 있어, 대부분 사업의 경우 지적재산권을 R&D 위탁받은자에게 귀속시키는 계약을 맺고 있음
(단, 일부 위탁 R&D의 경우 성과보전 등의 이유로 국가가 소유하는 경우도 있음)

- 다만, 해당 지식재산권의 양도는 정부의 사전 승인이 필요한 상황인데 자회사 또는 모회사로의 양도는 제외가 되며 만약 자회사 또는 모회사가 외국회사인 경우 기술유출 우려가 있음

* case 1) 외국 기업의 일본 법인이 지식재산권을 모회사에 양도하는 경우

* case 2) 국내 기업의 자회사가 M&A 등을 통해 외국 기업의 자회사가 되어 매각 또는 양도하는 경우

* case 3) 국내 회사의 본사가 해외로 이전하여 외국회사가 된 경우

- 현재 경제산업성은 '위탁 연구개발 시 지식재산 관리 운영 지침'을 마련하여 자회사 또는 모회사가 외국 기업일 경우 국가 등 R&D 위탁자에 사전에 알리도록 계약서에 명시하게 하였으나, 이 지침은 경제산업성(산하 독립행정기관 포함) 위탁 R&D에만 해당

- 따라서, 경제안보 중요기술에 대해 정부가 위탁한 연구개발사업 결과물의 지식재산권을 외국기업 등에 양도할 시 사전에 위탁자에게 알리고 상황에 맞게 조치할 수 있도록 규정이 마련되어야 함

● 향후 과제

- 경제안보를 위한 중요기술의 연구개발 성과가 사회적으로 구현되는 것을 고려하여, 필요에 따라 민·관 간 대화를 진행하며 관계부처 간 공통된 기준 및 대책을 조율할 필요가 있음

- 기술유출 방지를 위해 조치를 취해야 할 R&D사업을 파악할 때, 경제안보에 대한 국제적 움직임을 고려하여 일본에 위협을 주는 것이 무엇인지에 대한 연구·분석 수행 기능을 강화할 필요가 있음

- 영업비밀 관리 강화의 좋은 예를 참고하여, 기업규모 등을 고려하여 리스크에 따른 적절한 조치를 취하기 위하여 대책을 원활하게 추진할 방안을 검토할 필요가 있음

※ 한국산업기술진흥원 산업기술정책단 정책기획실 권준민 연구원 / jmkwon@kiat.or.kr

※ 본 자료에 수록된 내용은 작성자의 개인 의견으로 기관의 공식 견해가 아님을 밝힙니다.