https://doi.org/10.33778/kcsa.2024.24.3.173

국가연구개발 보안 환경 개선을 위한 등급별 연구보안 관리지침 설계 - FGI 분석을 활용하여

나 원 철*

요 약

최근 기술유출 등의 보안위험이 지속적으로 발생함에 따라 연구보안의 중요성이 대두되고 있다. 특히 국가연구개발의 실질적 보안관리 활동 수행을 위한 현장 중점적 지침이 부족한 상황이다. 따라서 본 연구는 중요도에 따라 국가연구개발과제에 등급을 부여하고 등급별로 연구보안 관리지침을 설계함으로써 과제 수행 인력들이 연구보안 활동을 효율적이고 간편하게 할 수 있도록 하였다. 먼저, 국가연구개발과제의 등급체계를 중요도에 따라 세 단계로 구분하고 연구보안 관리항목 관련 선행연구 분석을 통해 연구보안 관리지침 후보군을 간략화하여 도출하였다. 다음으로, 초점집단 인터뷰(Focus Group Interview)를 통해 등급체계와 관리지침 후보군에 대한 타당성을 검증하고 등급별 연구보안 관리지침을 마련하였다. 본 연구는 향후 연구보안 정책에 학술적으로 기여하고 현장 연구보안 관리체계 수립에 도움이 될 것으로 기대한다.

Design of research security management guidelines by grade to improve the national research and development security environment - Using the FGI method

Na Onechul*

ABSTRACT

Recently, as security risks such as technology leaks continue to occur, the importance of research security is increasing. In particular, there is a lack of on-site focused guidelines for conducting practical security management activities for national research and development. Therefore, this study assigned grades to national research and development projects according to importance and designed research security management guidelines for each grade so that personnel related to the projects could perform research security activities efficiently and conveniently. First, the grading system of national research and development projects was divided into three stages according to importance and a candidate group of research security management guidelines was derived by simplifying them through an analysis of prior research on research security management items. Next, the validity of the grading system and management guideline candidates was verified through a focus group interview and research security management guidelines for each grade were prepared. This study is expected to contribute academically to future research security policies and to help establish an on-site research security management system.

Key words : Research Security, National R&D Projects, Research Security Management Guidelines, Focus Group Interview

접수일(2024년 08월 19일), 수정일(1차: 2024년 09월 12일), 게재확정일(2024년 09월 20일)

* ㈜안랩/컨설팅본부 (주저자)

1. 서 론

1.1 국가연구개발 현황

국가연구개발은 국가 과학기술 혁신과 발전을 촉진하고 있으며, 경제적 및 사회적 발전을 이루기 위한 핵심적 활동이다[1]. 미국, 중국 등의 해외 주요국에서도 첨단기술 확보와 과학기술 경쟁력 강화를 위해 노력하고 있다[6].

하지만 이러한 국가연구개발의 중요성에도 불구하고 최근 5년간 93건의 산업기술 유출 사건이 발생하였고[10], 이는 우리나라 국가경쟁력을 약화시키고 막대한 경제적 손실을 발생시키고 있다[13]. 산업기술 유출 사건의 대표 사례는 다음 표와 같다.

<표 1> 산업기술 유출 사고 사례

연도	분야	사고
2023	반도체	반도체 세정장비 핵심기술 유출 사건 → ○○사 연구원 7명이 반도체 세정장비 국가핵심기술을 불법으로 유출한 뒤 동종업체 ○○○사를 설립하여 중국에 동일한 장비를 수출
2021	전기전자	2차전지 소재분야 국가핵심기술 해외 유출사건 → ○○사 퇴직 연구원 2명이 해외 경쟁사로 이직하면서 클라우드 서비스를 통해 국가핵심기술을 유출
2020	자율주행	자율주행차 핵심 센서 기술 유출 사건 → ○○대학 교수가 연구개발 과제 수행 중, 중국의 기술인력에게 무단으로 자료를 공유

이에 따라 기술의 유출을 사전에 방지하고 보다 안전한 연구개발 환경을 만들기 위한 국가연구개발 보안(이하 연구보안)에 대한 필요성이 높아지고 있다[11].

1.2 연구보안 특징

연구보안이란 연구개발 기획, 수행, 성과 창출에 이르기까지, 연구개발 수행 전 과정을 보호하는 제반 활동이다[3]. 최근의 연구개발 현장에서는 기획부터 성과창출에 이르는 전방위적 보안관리의 중요성이 강조되고 있다[12].

연구보안은 기존의 산업보안과 비교적 비슷한 개념을 가지고 있다. 연구보안과 산업보안 모두 기술을 보호하는 것이지만, 연구보안은 기술의 완성 전 추진 중인 연구와 관련된 모든 내용을 보호하기 위해 준수해야 할 절차와 기준을 마련하고 적용하는 예방의 개념이며, 산업보안은 완성된 기술이 유출되었을 시 적용하는 처벌의 개념에 가깝다[2, 16]. 예를 들어 <표 1>의 산업기술 유출 사고 사례 모두 연구보안 및 산업보안의 범주에 해당하나, 2023년 반도체 사고 사례와 같이 이미 완성된 반도체 세정장비 핵심기술의 유출을 막기 위한 보호 활동은 산업보안에 가깝고, 2020년 자율주행 사고 사례와 같이 연구개발 중이었던 자율주행차 핵심 센서 기술의 유출을 막기 위한 보호 활동은 연구보안에 가깝다고 할 수 있다.

연구보안의 법적 근거가 되는 관련 법령은 예산을 배분하고 조정하는 『과학기술기본법』, 국가연구개발사업 수행의 전반적 내용을 담은 『국가연구개발혁신법』, 국가연구개발사업의 평가를 담당하는 『연구성과평가법』, 국가전략기술 육성을 위한 『국가전략기술육성법』이 있다[20].

해외 주요국에서도 연구보안에 대한 필요성을 인지하고 적극적으로 대응지침을 마련하고 있다. 특히 미국, 일본, 영국, 호주 등의 주요국에서는 연구보안에 대한 전담조직을 신설하거나 연구자 대상으로 가이드 제작하여 배포하고 있다[23].

1.3 연구보안 한계점

이렇듯 우리나라와 해외 주요국에서는 연구보안에 대한 심각성을 인지하고 국가적 대응에 힘쓰고 있지만, 우리나라 연구보안 정책에는 아직 몇 가지 문제점이 존재한다.

첫째 “법·제도” 문제다. 연구개발 현장의 원활한 운영을 지원하는 혁신법이 제정되었지만 연구보안 관련 보안규정이 소관부처마다 상이하고 보안 규정 위반 시 제재에 대한 법적 근거가 부족한 상황이다[16]. 그리고 법제도 상 연구보안 적용의 범위가 주로 과제 단위로 한정되어 있어 기관 차원의 거시적 차원의 보안 대책이 마련이 시급하다. 이는 연구개발 현장의 보안

관리를 행함에 있어 연구자들에게 혼란을 야기시키는 원인이 되고 있다.

둘째 “보안과제” 문제다. 현재 국가연구개발과제의 보안등급은 일반과제, 보안과제 두 가지로 구분되어 있으며, 그 중 보안과제는 그 수가 매우 저조한 상황이다[16], 일반과제는 보안대책을 적용하지 않아도 되는 과제이니 현재 대부분의 연구개발 현장에서는 보안대책을 전혀 적용하지 않은 채 연구가 진행되고 있다. 하지만 한편으로는 연구개발 현장에서 보안과제로 분류될 시 보안조치 사항들에 부담을 느끼고 있어, 보안등급 부여 체계를 정비하여 완충지대를 마련할 필요가 있어 보인다.

셋째 “지원체계” 문제다. 과제를 수행하는 기관 내 연구보안을 전담으로 수행하는 조직이나 인력이 매우 부족한 상황이며, 조직 및 인력이 참고할 만한 가이드라인도 부재한 상황이다. 특히 과제를 수행하는 연구자들의 연구보안에 대한 인식이 부족한 것도 심각한 문제라고 할 수 있다.

앞서 나열한 연구보안 문제점들 중 가장 시급한 두 가지 사항은 국가연구개발과제의 등급체계를 수립하는 것과 연구보안 관리지침을 마련하는 것이다. 그리고 이 두 가지를 통합하여 국가연구개발과제 등급에 따라 연구보안 관리지침 적용 정도가 차등화되어야 할 것이다. 따라서 본 연구에서는 기존 연구보안 선행연구를 분석하여 국가연구개발과제 등급체계 및 연구보안 관리지침을 도출하고, 전문가 인터뷰를 통해 두 가지 영역을 연결하는 연구를 수행하고자 한다.

1.4 연구방법

본 연구는 국가연구개발과제 연구자 및 보안 담당자의 연구보안 관리 편리성과 효과성에 도움이 될 수 있도록 국가연구개발과제의 등급별 연구보안 관리지침을 설계 및 검증 보완하였다.

세부적으로 국가연구개발과제의 보안 중요도를 판정할 수 있는 등급체계를 선행연구를 참고하여 설계하였다. 다음으로 국가연구개발과제의 보안 관리를 위한 연구보안 관리지침을 선행연구를 통합 분석하여 설계하였다. 마지막으로 국가연구개발과제 등급체계와 연구보안 관리지침을 연결하고 연구보안 전문가를 대상으로 초점집단 인터뷰(Focus Group Interview) 결과를 반영하여 최종 국가연구개발과제 등급별 연구보안 관리지침을 마련하였다.

2. 이론적 배경

2.1 국가연구개발과제 등급체계 선행연구

연구개발을 통해 산출되는 정보들의 가치가 점차 중요해지면서 연구보안의 필요성이 강조되고 있다. 특히 연구개발 산출물, 성과물, 결과물에 대한 중요도를 판단하여 등급을 부여하는 선제적 개념의 보안대책 수립이 중요해지고 있다. 하지만 현재 국가연구개발과제의 보안등급은 보안과제, 일반과제의 두 등급으로 구분되어 있고 대부분의 국가연구개발과제가 일반과제로 수행되고 있다[18]. 따라서 일반과제로 수행되는 과제 중에서 중요도가 높아 보안관리가 필요한 과제를 판단하여 등급을 부여하는 것이 시급한 상황이다.

먼저 선행연구 수집 대상을 확정하기 위해 연구보안의 보호 대상을 파악할 필요가 있다. 연구보안을 통해 지켜야 할 중요한 가치 있는 대상은 그 범위가 넓다고 볼 수 있다. 연구개발 수행 중에 산출되는 데이터, 정보, 문서, 정보시스템 등이 있으며, 연구개발 종료 후에 산출되는 결과물, 기술, 특허, 혹은 영업비밀 등도 보호의 대상이 된다[9]. 이렇듯 다양한 보호 대상들을 참고하여 등급화를 시도한 선행연구를 분석하였다.

나원철의 연구[18]에서는 ISO/IEC 27001, LSE(London School of Economics and Political Science) 정보자산 분류표, Harvard University 정보 분류체계, 민간기업 S사 문서보안 등급, 행정안전부 정보시스템 등급을 종합적으로 분석하여 유출 시 위험도를 주요 요인으로 고려하여 매우 중요한 1등급 과제, 일반적으로 중요한 2등급 과제, 유출되어도 문제 없는 3등급 과제로 구분하였다. 1등급 과제는 국가 차원에서 보호되어야 하며, 만약 과제 관련 정보가 유출된다면 연구자 뿐만 아니라 산업 인프라, 국가에까지 악영향을 미칠 수 있는 과제로 보았고, 2등급 과제는 과제 참여 연구자와 과제 수행 기관에 악영향이 있을 수 있는 과제, 3등급 과제는 과제 수행 내용이 유출되어도 악영향이 없는 과제라고 보았다.

한소영의 연구[8]에서는 특허청의 기업정보 등급

산정 기준, ASIS의 정보 등급분류 평가기준, Massachusetts Institute Technology의 정보 등급 구분, 한국인터넷진흥원의 정보 중요도 평가기준을 종합분석하였고, 정보의 접근권한과 활용도를 주요 요인으로 도출하여 국가연구개발과제 내 연구개발 정보에 대해 기밀정보, 1등급 중요정보, 2등급 민감정보, 3등급 공개 정보로 등급화를 수행하였다.

연구개발과제의 등급화 관련 연구는 매우 부족한 상황이지만, 본 연구에서는 다수의 선행연구를 탄탄하게 분석한 상기 두 가지 연구결과를 참고하여 국가연구개발과제 3등급 체계로 아래와 같이 설계하고자 한다.

<표 2> 국가연구개발과제 등급체계

등급체계	과제 정보 유출 시 위험도	과제 정보 접근권한(활용 범위)
1등급 과제	유출될 시 국가와 관련 산업, 기업, 연구자에게 중대한 악영향을 줄 우려가 있는 과제	과제 수행 연구자(책임자 및 참여인력)에게만 접근권한이 있음
2등급 과제	유출될 시 관련 기업, 연구자에게 악영향을 줄 우려가 있는 과제	과제 수행 연구조직 전체에 접근권한이 있음
3등급 과제	유출되어도 악영향이 없는 과제	모두가 접근 가능함

2.2 연구보안 관리지침 선행연구

현재 국가연구개발과제의 보호 활동을 위해 활용되는 연구보안 관리를 위한 정책들은 그 범위가 상당하기에 연구자들에게 많은 부담을 가중시키고 있다[15]. 또한 연구보안 관리의 수행 주체가 연구개발을 수행하는 조직인지, 연구개발을 수행하는 조직 내 연구보안 관리자인지, 연구개발을 수행하는 연구자인지 그 구분이 명확하지 않다. 따라서 본 연구에서는 연구보안 관련 선행연구를 분석하여 기존 문제점을 보완할 수 있고 연구자들이 간편하게 활용이 가능한 연구보안 관리지침을 도출하고자 하였다.

미래창조과학부의 국가연구개발사업 보안관리 표준매뉴얼[15]에서는 국가연구개발사업 규정의 개요와 기획·관리·평가, 연구개발결과의 귀속 및 활용 촉진, 기술료의 징수 및 사용, 그리고 보안관리에 대한 내용이 담겨져 있다. 해당 매뉴얼은 우리나라의 지금까지 연구보안 관련 자료 중 가장 먼저 제시된 가이드이며, 방대한 양의 컴플라이언스 내용이 들어있어 현재에도 연구보안의 선도적 기반 자료로 활용되고 있다. 매뉴얼에서의 연구보안 관리지침은 보안관리체계, 참여 연구원 관리, 연구개발 결과 및 내용의 관리, 연구시설 관리, 정보통신망 관리의 총 5개의 영역으로 구분되어 있고, 세부적으로 40개의 항목으로 구성되어 있다. 그리고 각 항목마다 사업의 등급(모든과제, 보안과제)별, 사업의 이행대상(연구기관, 연구책임자, 참여연구원)별 이행여부를 제시하였다.

나원철의 연구[19]에서는 국내외 연구보안 관련 선행연구 7개를 분석하여 연구보안 수준평가 항목(연구보안 추진체계, 연구시설과 장비 보안, 전자정보 보안, 주요 연구정보 관리, 연구노트 관리, 지식재산권/특허 관리, 기술사업화 관리, 내부연구원 관리, 인가된 제3자 관리, 외부자 관리) 10개를 객관 타당하게 도출하였고, 연구개발 수행과정, 연구개발 보호 대상, 연구개발 보호 범위의 3가지 개념 위에 통합시켜 연구보안 수준평가 모형을 설계하였다. 또한 모형에 대한 타당성을 검증하기 위해 대학 연구실 환경에 직접 적용하여 실증 분석하였다.

연구보안관리 길잡이[21]에서는 연구보안에 대한 이해를 위한 기본적 개념과 구성에 대해 설명하였다. 또한 보안관리의 주체는 연구기관, 연구자, 보안관리 대상은 연구원, 연구시설, 연구자료, 연구성과물, 보안관리 방법은 보안규정, 보안장치, 보안시스템으로 구분하였고, 연구진행 단계별 연구자의 연구보안관지, 보안관리 항목별로 연구기관 연구보안관리로 구분하여 연구자가 쉽게 이해하고 이행이 가능한 연구보안 관리 항목을 나열하였다.

해외 연구보안 연구[4, 5, 22]에서는 연구개발 수행 시기별로 연구보안 관리를 수행해야 함을 강조하였고, 특히 보안의 세 가지 기본요소인 기밀성, 무결성, 가용성을 기반으로 안전한 연구개발을 위해 연구개발의 연속성 유지와 산출되는 자료 및 정보를 효과적으로 보호할 수 있는 방안을 마련하였다.

상기 연구보안 관련 선행연구을 비교분석하여 아래 표와 같이 연구보안 관리지침 후보군을 수립하였다. 연구보안 관리 영역과 관리 항목은 가장 최신에 발간된 연구보안 길잡이 연구를 기반으로 통합정리하였고, 과제 등급별로 차별화하여 보안대책을 수립할 필요가 있는 항목들 위주로 축소화하여, 연구보안의 기반이자 관리적 관점인 ①연구보안 관리체계, 연구보안의 물리적 관점인 ②연구시설 및 장비, 연구보안의 기술적 관점인 ③정보시스템 보안, 연구보안에서 가장 핵심적으로 보호해야 할 대상인 ④연구산출물 관리, 연구보안에서 유출의 위험 요소인 ⑤연구자 보안의 5가지로 구분하여 설계하였다.

<표 3> 연구보안 관리지침 후보군

연구보안 관리 영역	연구보안 관리 항목	상세 설명
1. 연구보안 관리체계	1.1 자체 연구보안 규정 수립	• 연구기관과 연구보안 관리부서는 연구보안 관련 법령을 기반으로 연구기관 내 규정을 제정해야 함 • 연구보안 관리부서는 규정을 연구기관의 특성에 맞게 수시로 개정해 나가야 함
	1.2 연구보안 담당자 지정	• 연구기관은 연구보안 관리부서를 설치하고, 연구보안 담당자를 지정하여야 함 • 연구기관은 연구보안 담당자 인사이동 시 즉시 새로운 인력으로 변경하고 인수인계 작업을 수행하여야 함
	1.3 연구보안 교육	• 연구보안 관리부서는 연간 연구보안 교육계획을 수립하고 연구기관 내 연구자들을 대상으로 연구보안 교육을 시행하여야 함 (연 1회) • 연구보안 관리부서는 연구개발과제 수행 연구자를 대상으로 사전 보안교육을 실시하여야 함 (연구개발 수행 전)
	1.4 연구보안 실태점검	• 연구보안 담당자는 각 연구 부서별로 실태조사를 실시하여야 함 (상시, 월 1회) • 실태조사란 PC 보안, 사용자 접근 관리, 연구산출물 관리를 중점적으로 점검함
	1.5 해외공동(위탁)연구 관리	• 연구자는 해외 연구기관과 공동(위탁) 연구 시 협약 전 연구기관 및 연구보안 관리부서로부터 사전 승인절차를 진행하여야 함 (연구개발 수행 전) • 연구보안 담당자는 협약 시 지식재산권 보호대책, 보안서약서, 비밀유지의무 등의 연구보안 조치사항을 수행하여야 함 (연구개발 수행 전)
2. 연구시설 및 장비	2.1 연구시설 지정	• 연구보안 담당자는 연구기관 내 연구시설 등에 대해 보호구역으로 지정하여 관리해야 함
	2.2 연구시설 출입자 통제	• 연구시설에는 반드시 허가된 연구자만이 출입하여야 함 • 연구시설 출입자는 연구책임자 및 연구보안 담당자로부터 사전 승인을 받아야 함
3. 정보시스템 보안	3.1 정보자산 관리	• 정보자산(서버, PC, usb 등)을 도입할 경우 연구책임자 혹은 연구보안담당자로부터 보안성 검토 및 승인을 받아야 함
	3.2 네트워크 보안	• 연구기관의 네트워크 구성도는 대외비로 지정하여 안전하게 보관하여야 함 • 연구기관 내 업무망은 인터넷망(외부망)과 분리하고 IPS, Firewall 등의 보안시스템을 구축 및 운영해야 함 • 무선 네트워크는 구축하지 않아야 하며, 불가피하게 구축할 시에는 보안성 검토를 받고 주기적으로 점검하여야 함
	3.3 사용자 접속 관리	• 연구정보시스템 접속 시 2Factor 인증을 사용하여야 함 • 사용자 접속기록(식별정보, 접근기록, 이용시간, 업무 행위)은 인증 여부와 무관하게 기록 및 유지되어야 함 (최소 3년 이상) • 연구개발과제에 따라 연구정보시스템에 대한 접근을 차별적으로 설정하여야 함
	3.4 개인PC 보안	• 연구자는 개인용 PC에 비밀번호(숫자, 문자, 특수문자 조합 8자리 이상)와 화면보호기 기능을 설정하여야 함 • 연구자는 개인용 PC에 소프트웨어를 설치할 시 연구보안 담당자의 승인을 받아야 함 • 연구자는 개인용 PC에 공유폴더를 생성하지 않아야 함 • 연구자의 개인용 PC는 주기적으로 백신 프로그램을 실행시키도록 설정해야 함 • 연구자는 외부로 연구자료를 전송할 시 파일에 암호화 기능을 설정해야 함
	3.5 정보통신매체 보안	• 연구자는 사전에 인가된 정보통신매체(노트북, usb 등)만을 사용해야 함 • 연구자는 정보통신매체를 외부로 반출하거나 반입할 시 연구책임자, 연구보안 담당자의 승인을 받아야 함 • 연구자는 암호가 걸린 보안 usb를 사용하여야 함
4. 연구산출물 관리	4.1 연구자료 등급화	• 연구자는 연구개발과제 수행 중 발생하는 연구자료(파일, 연구노트, 문서 등)에 대해 연구보안 담당자와 협의하여 중요도를 판정하여 등급을 부여해야 하고, 등급에 따라 차별화된 보호대책을 적용해야 함 (연구개발 수행 중)
	4.2 연구자료 관리	• 연구자는 연구자료를 별도의 정보시스템에 저장하고, 연구보안 담당자는 연구자별 접근권한을 차별적으로 부여하고 관리하여야 함 (연구개발 수행 중)

		• 연구자는 연구자료 출력 후 잠금기능이 있는 장소에 보관하고, 연구자료 반출입 시 출납내용을 기록하여야 하며, 연구보안 담당자는 출력된 연구자료와 반출입 시 출납내역에 대한 보안성 검토를 수행하여야 함 (연구개발 수행 중) • 연구자료를 외부로 반출하여 제공할 시에는 연구책임자 혹은 연구보안 담당자로부터 승인을 받아야 함 (연구개발 수행 중)
	4.3 연구노트 작성 관리	• 연구자는 연구노트를 작성하고 관리번호를 부여하여야 함 (연구개발 수행 중)
	4.4 연구성과물 관리	• 연구성과물을 대외 공개 시에는 연구보안 담당자로부터 공개해도 되는지 사전 검증을 거쳐야 함 (연구개발 수행 후) • 연구자는 연구성과물의 지식재산권 확보, 기술이전 수행 시 연구보안 관리부서 및 연구보안 담당자와 협의하여 결정하여야 함 (연구개발 수행 후)
5. 연구자 보안	5.1 채용 시 보안 관리	• 연구기관은 채용 예정 연구자를 대상으로 보안서약서를 징구하여야 함 • 채용 후에는 연구보안 담당자가 연구보안 교육을 실시하여야 함
	5.2 퇴직 시 보안 관리	• 퇴직 예정 연구자는 모든 연구자산(연구노트, 저장장치 등)을 반환하고 별도의 퇴직 서약서를 징구하여야 함
	5.3 해외 출장 시 관리	• 해외 출장 전 발표하거나 공개해야 할 연구자료에 대해 연구보안 담당자에게 보안성 검토(비밀번호 설정 등)를 받아야 함 • 연구자는 외국인과 접촉 전 외국인 접촉 신청서, 접촉 후 결과보고서 등을 연구보안 담당자에게 제출하여야 함
	5.4 외국인 연구원 관리	• 연구개발 과제에 외국인 연구원이 참여하는 것은 원칙적으로 금지되지만, 참여가 필요한 경우 사전 승인절차(연구보안 관리부서)를 이행해야 함 • 채용 대상 외국인 연구원에게는 영문 비밀유지의무 부과와 함께 보안서약서, 범죄기록증명원을 징구하여야 함 • 외국인 연구원은 별도로 보안 관리사항(실태점검, 참여현황 등)을 구분하여 관리하여야 함
	5.5 공동(위탁) 연구원 관리	• 공동(위탁)연구를 수행하는 경우, 연구보안 담당자는 공동(위탁) 연구자를 대상으로 비밀유지계약서를 작성해야 함
	5.6 임시 방문자 관리	• 외부 임시 방문자는 연구책임자로부터 사전 방문 신청 및 승인을 받아야 함 • 보안준수 의무사항(신원확인, 출입증 발급, 보안스티커 등)을 사전에 준비하여 확인시켜야 함
	5.7 상시 근무자 관리	• 상주하는 외부 연구원의 경우 외부 연구기관과 연대책임을 부과함 • 장기출입증을 별도로 발급하고 연구기관 출입이력을 관리함

3. 분석 방법 및 결과

연구보안 관리지침 후보군에 대한 내용 검토와 국가연구개발과제 등급체계에 연구보안 관리지침 후보군을 연결 및 배치하고자 전문가 인터뷰를 진행하였다. 국가연구개발과제 등급체계와 연구보안 관리지침의 타당성, 연구보안 관리지침의 등급화에 대한 의견을 수렴하고 분석의 신뢰성을 확보하기 위해 전문가들에 의한 초점집단 인터뷰(Focus Group Interview)를 수행하였다. 초점집단 인터뷰는 특정 주제를 대상으로 관련 전문가들을 초빙해 의견을 자유롭게 나누면서 핵심 정보를 수집하는 연구방법이다[7].

인터뷰 대상 전문가는 국가연구개발과제의 정책과 연구개발 보안에 대한 이해가 동시에 가능한 인원으로 정하였다. 최종 선별 인터뷰 대상자는 연구개발 정책과 보안에 대해 모두 이해가 높은 전문가 2명, 민간 연구개발 현장에서의 보안 실무 경험이 풍부한 실무 보안 전문가 3명의 총 5명의 전문가를 선정하여 인터뷰를 진행하였다.

<표 4> 인터뷰 대상자 정보

참여자	소속	경력	비고
A	대학교수(보안)	15년 이상	박사
B	대학교수(정책)	10년 이상	박사
C	보안 컨설턴트	20년 이상	석사
D	보안 컨설턴트	15년 이상	학사
E	기업 보안 담당자	10년 이상	석사

인터뷰 진행은 총 3단계로 구분하여, 먼저 인터뷰의 목적과 연구의 상세 소개(국가연구개발과제 등급화, 연보안 관리지침), 다음으로 주요 질문(등급별 연구보안 관리지침 매칭), 마지막으로 추가 의견 수렴으로 진행하였다. 다음은 연구보안 관리지침 개선을 위한 인터뷰 핵심 질문이다.

- 기존 국가연구개발과제 보안등급체계에 대해 어떻게 생각하시나요?

- 기존 국가연구개발과제 연구보안 관리지침에 대해 어떻게 생각하시나요?

- 본 연구에서 도출한 국가연구개발과제 보안등급체계와 연구보안 관리지침 후보군에 대해 의견을 부탁드립니다.

인터뷰를 통해 도출된 의견들은 가감 없이 중립성을 유지하도록 분석하였으며 해당 인터뷰를 통해 본 연구의 신뢰성 및 타당성을 확보하였다.

전문가 인터뷰 의견을 수렴하여 아래 표와 같이 국가연구개발과제 등급별 연구보안 관리지침을 마련하였다. 과제 등급별 연구보안 관리 내용은 크게 수행 주체와 수행 방법으로 구분하여 작성하였다. 수행 주체는 용어의 혼용을 정리하고자 ①국가연구개발과제 수행 연구책임자 및 연구자(이하 연구 수행자), ②연구기관, ③연구보안 조직 및 연구보안 담당자(이하 연구보안 관리부서)의 3가지로 구분하였다. 연구보안 관리부서의 역할은 크게는 연구기관을 대상으로 연구보안 관리를 수행하는 조직이며, 세부적으로는 국가연구개발과제 단위를 대상으로 연구보안 관리 활동을 수행하는 조직을 말한다. 수행 방법은 ①보호 대상(what), ②보호 방법(how)의 관점으로 정리하였다. 추가적으로 연구보안 수행 시기는 연구개발 수행을 기준으로 수행 전, 수행 중, 수행 후의 3단계로 구분하였고, 연구개발의 어느 한 시점이 아닌 지속적으로 상시 수행해야 하는 단계를 별도로 표기하였다.

<표 5> 국가연구개발과제 등급별 연구보안 관리지침 제안

연구보안 관리 영역	연구보안 관리 항목	연구보안 수행 시기	과제 등급별 연구보안 관리 내용	
			1등급	2등급
1. 연구보안 관리 체계	1.1 규정 수립	상시 (연 1회)	(수행 주체) 연구보안 관리부서 (수행 방법) 규정은 연구보안 관리부서에서 제정 및 개정하고 연구기관 내 경영진 승인을 받아야 함	
	1.2 연구보안 담당자 지정	상시 (발생시)	(수행 주체) 연구기관 (수행 방법) 연구기관은 연구보안 관리부서를 설치하고, 연구보안 담당자를 지정하여야 함	
	1.3 연구보안 교육	상시 (연 1회)	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 연구기관 내 모든 인원을 대상으로 기초 연구보안 교육을 수행하여야 함 ※ 기초 연구보안 교육 : 연구보안에 대한 전반적 개념과 연구보안의 중요성에 대한 인식 고취를 목적으로 함	
		수행 전	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 연구수행자를 대상으로 연구개발 수행 전, 수행 중, 수행 후 심화 연구보안 교육을 수행하여야 함 ※ 심화 연구보안 교육 : 국가연구개발과제 수행에 실질적으로 필요한 보안 요구사항에 대한 상세한 설명을 목적으로 함	-
	1.4 연구보안 실태점검	수행 중	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 국가연구개발과제 수행 환경을 대상으로 월 1회 보안 실태점검을 수행하여야 함	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 국가연구개발과제 수행 시 자체적으로 월 1회 보안 실태점검을 수행하여야 함
	1.5 해외 공동(위탁) 연구 관리	수행 전	(수행 주체) 연구기관 (수행 방법) 연구기관은 해외 연구기관과 공동(위탁)연구를 수행하는 국가연구개발과제에 대한 사전 승인절차를 진행하여야 함	-
			(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 해외 연구기관과 공동(위탁)연구를 수행하는 연구 수행자를 대상으로 지식재산권 보호대책 마련, 보안서	

			약서/비밀유지의무 징구 등의 선행 보안 조치를 취하여야 함	
	1.6 정보자산 관리	상시 (발생 시)	(수행 주체) 연구기관, 연구보안 관리부서 (수행 방법) 연구 수행자가 정보자산(서버, PC, usb 등)을 도입할 경우, 연구기관의 승인을 득하여야 하고 연구보안 관리부서로부터 보안성 검토를 받아야 함	
2. 물리 보안	2.1 연구시설 지정	상시 (발생 시)	(수행 주체) 연구기관 (수행 방법) 연구기관은 국가연구개발과제 수행 장소 등 주요 연구시설에 대해 보호구역으로 지정하고 관리하여야 함	
		상시 (발생 시)	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 연구시설에 대해 특별보호구역으로 지정하고 관리하여야 함 ※ 특별보호구역은 출입문 이중 잠금장치 시건, CCTV 설치, 출입관리대장 작성 등 강력한 물리적 보호 장치를 적용해야 함	-
	2.2 연구시설 출입자 통제	수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구시설에는 반드시 허가된 인력만 출입할 수 있도록 연구 수행자는 연구보안 관리부서로부터 반드시 사전 승인을 받아야 함	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 연구시설 출입자에 대해 목록을 작성하고 관리하여야 함
3. 정보시스템 보안	3.1 네트워크 보안	상시 (발생 시)	(수행 주체) 연구기관 (수행 방법) 연구기관은 연구기관의 모든 네트워크 구성도(IP 포함)에 대해 대외비로 지정하여 안전하게 관리하여야 함	
		수행 전	(수행 주체) 연구기관, 연구보안 관리부서 (수행 방법) 연구기관은 연구시설을 대상으로 업무망과 인터넷망을 분리하여 운영하여야 하며, 연구보안 관리부서는 연구시설로 통하는 네트워크에 IPS, 방화벽 등의 보안시스템을 구축하여 관리하여야 함 ※ 1등급 과제 수행 환경에서는 인터넷 사용 불가하도록 망 분리하여야 함	(수행 주체) 연구기관, 연구보안 관리부서 (수행 방법) 연구기관은 연구시설을 대상으로 P2P, 웹하드, 메신저 등의 인터넷 접속을 제한하여 운영하여야 함
		수행 전, 수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구시설에 무단으로 무선통신망을 구축해서는 안되며, 불가피하게 구축할 시에는 연구보안 관리부서로부터 보안성 검토(비밀번호 설정, SSID 숨김 등)를 받고 주기적으로 점검받아야 함	-
	3.2 사용자 접속 보안	수행 전, 수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구보안 관리부서는 연구정보에 접속 가능한 시스템을 대상으로 예외 없이 2Factor 인증을 사용하도록 설정해야 하며, 연구 수행자는 이에 따라 접속하여야 함	-
		수행 전, 수행 중, 수행 후	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구보안 관리부서는 연구 수행자가 연구정보시스템에 접속한 기록(식별정	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구보안 관리부서는 연구 수행자가 연구정보시스템에 접속한 기록(식별정

			구 수행자는 외부로 연구자료를 전송할 시 연구보안 관리부서와의 협의를 통해 전송 여부를 결정하고, 파일에 자체 암호화 기능을 설정하여 전송해야 함	를 전송할 시 파일에 자체 암호화 기능을 설정하여 전송해야 함
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구보안 관리부서로부터 인가받은 정보통신매체(노트북, usb 등)만을 사용하여야 함	
	3.4 정보통신매체 보안	수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 정보통신매체를 외부로 반출하거나, 내부로 반입할 시 연구보안 관리부서의 승인을 받아야 함	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 정보통신매체를 외부로 반출하거나, 내부로 반입할 시 연구책임자의 승인을 받아야 함
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구보안 관리부서로부터 지급받은 보안usb를 사용하여야 하며, 연구보안 관리부서는 보안usb 보유현황을 주기적으로 점검하여야 함	-
4. 연구 산출물 관리	4.1 연구자료 등급화	수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구개발 수행 중 산출되는 연구자료(파일, 연구노트, 문서 등)에 대해 연구보안 관리부서와 협의하여 중요도에 따라	-

			보, 접근기록, 이용시간, 업무행위 등)을 최소 3년 보관하고 주기적으로 점검하여야 함	보, 접근기록, 이용시간, 업무행위 등)을 최소 1년 보관하여야 함
		수행 전, 수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구보안 관리부서와 협의하여 연구 수행자의 역할 및 직위에 따라 정보시스템 내 연구정보에 차별적으로 접근이 가능하도록 설정하여야 함	(수행 주체) 연구 수행자 (수행 방법) 연구책임자는 연구자별로 역할 및 직위에 따라 정보시스템 내 연구정보에 차별적으로 접근이 가능하도록 설정하여야 함
	3.3 PC 보안	수행 전	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 모든 연구 수행자의 개인 PC에 비밀번호(숫자, 문자, 특수문자 조합 8자리 이상)와 화면보호기 기능을 설정하도록 통제하여야 함	(수행 주체) 연구 수행자 (수행 방법) 연구책임자는 모든 연구 수행자의 개인 PC에 비밀번호(숫자, 문자, 특수문자 조합 8자리 이상)와 화면보호기 기능을 설정하도록 통제하여야 함
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 소프트웨어를 설치할 시 연구보안 관리부서의 승인을 받아야 함	
		수행 중	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 개인 PC에 공유폴더를 생성하지 않아야 함	-
		수행 전, 수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구보안 관리부서는 모든 연구 수행자의 PC에 백신 프로그램을 설치하고 주기적(매일)으로 실행되도록 설정하여야 함	
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 외부로 연구자료

			등급을 부여하고, 연구보안 관리부서는 등급에 따른 차별화된 보호대책을 적용해야 함	
	4.2 연구자료 관리	수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구개발 수행 중 산출되는 모든 연구자료를 별도의 정보시스템에 저장하고, 연구보안 관리부서는 저장된 연구자료를 보호해야 함	
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 출력된 연구자료를 잠금 기능이 있는 장소에 보관하고, 연구자료 반·출입 시 출납내용을 기록하여여 하며, 연구보안 관리부서는 출력된 연구자료와 반출·입 출납 내용을 주기적으로 검토하여야 함	
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자가 외부로 연구자료를 반출하여 제공 시에는 연구보안 관리부서의 승인이 있어야 함	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자가 외부로 연구자료를 반출하여 제공 시에는 연구책임자의 승인이 있어야 함
	4.3 연구노트 작성 관리	수행 중	(수행 주체) 연구 수행자 (수행 방법) 연구 수행자는 연구노트(파일, 종이문서 등)를 작성하고 관리번호를 부여하여야 함	
	4.4 연구성과물 관리	수행 후	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자가 연구성과물을 외부로 공개할 시에는 연구보안 담당자로부터 공개 가부에 대한 사전 검증을 거쳐야 함	-
		수행 후	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구성과물에 대한 지식재산권 확보, 기술이전 등을 진행할 시 연구보안 관리부서와 협의하여 결정하여야 함	-
5. 연구자 보안	5.1 채용 시 보안 관리	상시 (발생 시)	(수행 주체) 연구기관, 연구보안 관리부서 (수행 방법) 연구기관은 채용한 연구 수행자를 대상으로 보안서약서를 징구하여야 함	
		상시 (발생 시)	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구보안 관리부서는 채용한 연구 수행자를 대상으로 연구보안 교육을 수행해야 함	
	5.2 퇴직 시 보안 관리	상시 (발생 시)	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 퇴직 예정 연구 수행자는 연구보안 관리부서에 모든 연구자산(연구노트, 정보통신매체 등)을 반환하고, 별도의 퇴직 서약서를 작성하여 제출하여야 함	
	5.3 해외 출장 시 관리	수행 중, 수행 후	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 해외 출장 전 발표하거나 공개해야 하는 연구자료에 대해 연구보안 관리부서로부터 보안성 검토(공개 가능 여부, 공개 범위, 비밀번호 설정 등)를 받아야 함	(수행 주체) 연구 수행자 (수행 방법) 연구책임자는 해외 출장 전 발표하거나 공개해야 하는 연구자료에 대해 보안성 검토(공개 가능 여부, 공개 범위, 비밀번호 설정 등)를 수행하여야 함
		수행 중	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 외국인 접촉 전 접촉 신청서를 작성하고, 접촉 후 결과보고서를 작성하여 연구보안 관리부서에 제출하여야 함	-
6. 외국인 연구자 관리	6.1 외국인 연구원 관리	상시 (발생 시)	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자는 연구개발 과제에 외국인 연구원이 참여하는 경우, 연구보안 관리부서로부터 사전 승인절차를 이행해야 함	

		상 시 (발생 시)	(수행 주체) 연구기관, 연구보안 관리부서 (수행 방법) 연구기관은 채용한 외국인 연구원을 대상으로 영문 보안서약서, 비밀유지의무, 범죄기록증명원을 징구하여야 함	
		수 행 중	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 외국인 연구원을 대상으로 별도의 보안 관리사항(실태점검, 참여현황 등)을 관리하여야 함	(수행 주체) 연구 수행자 (수행 방법) 연구책임자는 외국인 연구원을 대상으로 별도의 보안 관리사항(실태점검, 참여현황 등)을 관리하여야 함
7. 외부자 보안	7.1 공동(위탁) 연구원 관리	상 시 (발생 시)	(수행 주체) 연구보안 관리부서, 연구 수행자 (수행 방법) 연구 수행자가 공동(위탁)연구를 수행하는 경우, 연구보안 관리부서는 공동(위탁) 연구자를 대상으로 비밀유지계약서를 작성해야 함	
	7.2 임시 방문자 관리	상 시 (발생 시)	(수행 주체) 연구보안 관리부서 (수행 방법) 외부 임시 방문자는 사전 방문 신청을 통해 연구보안 관리부서의 승인을 받아야 하며, 보안준수 의무사항(신원 확인, 출입증 발급, 보안 스티커 부착 등)을 확인 및 적용해야 함	
	7.3 상시 근무자 관리	수 행 전	(수행 주체) 연구보안 관리부서 (수행 방법) 연구보안 관리부서는 장기간 상기 근무자의 경우 장기 출입증을 별도로 발급하고, 연구기관 출입이력을 주기적으로 점검해야 함	

본 연구에서 마련한 연구보안 관리지침이 기존 관련 지침과 차별화되는 부분은 연구보안 관리부서의 보안 활동에 중점을 두었다는 점이다. 기존 관련 지침을 설명하는 선행연구에서는 연구 수행자 중심의 보안 활동을 강조하고 있지만, 실제 보안 현장에서는 보안 담당자가 대부분의 보안 활동을 수행하고 있고 연구 수행자는 보안 활동을 수동적으로 행하는 보조자 입장에 있기 때문에 본 연구에서는 연구보안 담당자에게 많은 보안 활동을 부여하는 관리지침을 설계하였다.

연구보안 관리 항목 구성에 대해서는 이견이 없었지만, 연구보안 관리 항목을 묶어주는 연구보안 관리 영역의 범위가 다소 포괄적으로 구성되어 있다는 의견이 있어 더욱 세밀하게 분류하였다. 연구자 보안 영역은 연구자 그룹인 연구자 보안 영역, 외국인 연구자를 대상으로 한 외국인 연구자 보안 영역, 외부 연구자를 대상으로 한 외부자 보안 영역의 세 가지 영역으로 세분화하였다. 마찬가지로 정보시스템 보안 영역도 세분화하여 네트워크 보안, 사용자 접속 보안, PC 보안, 정보통신매체 보안의 네 가지 영역으로 구분하였다. 추가적으로 연구시설 및 장비 보안 영역은 보안 업계 현장에서 주로 사용되는 용어를 반영하여 물리 보안 영역으로 명칭 변경하였다. 그리고 연구보안 관리항목 중 정보자산 관리 항목에 대해서는 정보시스템을 포함한 관리적 차원의 영역으로 판단되어 연구보안 관리체계 영역으로 이동하였다. 또한 연구보안 수행 시기에 대해서도 기존 연구개발 수행 전, 중, 후로 구분하던 것을 단순히 하나의 지점으로 구분하기에는 애매한 항목들이 다수 존재하기에 연구보안 수행시기를 더욱 세분화하여 추가 반영하였다.

최종적으로 1등급 과제와 2등급 과제의 연구보안 관리지침 내용의 주요 차이점을 연구개발 수행 시기별로 세 가지 정리하고자 한다. 첫째, 연구개발 수행 전 1등급 과제와 2등급 과제의 주요 차이점은 관리/기술/물리 관점에서의 연구보안 관리 수준의 강화된 적용 여부로 볼 수 있다. 연구보안 교육, 해외 공동(위탁)연구 관리, 연구시설 지정, 네트워크 보안, 사용자 접속 보안 등의 항목에서 관리/기술/물리를 망라하여 통합적 관점에서 1등급 연구개발 과제에 대해 보다 높은 수준을 요구하고 있다. 둘째, 연구개발 수행 중 1등급 과제와 2등급 과제의 주요 차이점은 연구보안 관리부서의 적극적 개입으로 볼 수 있다. 다시 말하면 연구보안을 수행 및 통제하는 주체가 연구보안 관리부서이면 보다 엄격한 보안관리가 가능하고, 연구 수행자가 자율적으로 연구보안을 수행 및 통제하면 보다 유연한 보안관리가 가능함을 의미한다. 연구보안 실태점검, 연구기설 출입자 통제, PC 보안, 해외 출장 시 관리 등의 항목에서 연구보안 관리부서의 적극적 개입을 요구하고 있다. 셋째, 연구개발 수행 후 1등급 과제와 2등급 과제의 주요 차이점은 연구성과물의 관리 및 통제이다. 연구개발 수행 후 산출되는 최종 연구성과물에 대한 가치를 무단으로 도용하는 것을 방지하기 위해 대외 공개 및 활용 시 엄격한 통제를 적용하는 것을 요구하고 있다.

추가적으로 초점집단 인터뷰를 통한 논문 검증과정이 다소 부족할 수 있기에 감사 추적법[14]을 활용하여 연구의 논증을 탄탄히 하고자 하였다. 감사추적 기법은 소위 내부에서 보는 것보다 외부에서 볼 때 더 잘 보일 수 있음을 고려한 연구 방법으로써 연구 오류를 최대한 줄이기 위해 연구의 결과를 다른 시각에서 검증하는 방법을 말한다. 이는 주로 사전 검증보다는 도출된 결과에 대한 사후 검증이 목적이라고 할 수 있으며 연구 결과의 신빙성 여부를 판단하는 데 도움을 준다[17].

연구 결과에 대한 감사 추적은 보안 업계 현장에서 25년 이상 경험을 쌓아온 전문가가 수행해 주었으며 연구 결과가 도출된 경위와 그 근거의 전후관계에 대해 면밀하게 검토하였다. 검토 결과, 연구 결과가 도출되는 과정에 문제점은 없으며 기존 선행연구들과의 차별성이 존재하는 것으로 보았다. 또한 연구보안 담당부서 혹은 연구보안 담당자가 현장에서 실질적으로 참고 가능한 지침이라고 평가하였다. 하지만 본 연구에서 참고한 선행연구의 부족함을 가장 큰 문제점으로 지적하였으며, 향후 해외 연구보안 관련 연구를 탐색하여 참고하는 것을 권고하였다.

4. 결론

세계적으로 국가연구개발의 중요성이 높아지고 있는 가운데 기술유출의 심각성이 대두되고 있다. 이는 안전한 국가연구개발 수행이 필요해지고 있으며, 연구보안에 대한 관심과 심도있는 연구가 필요함을 의미한다. 연구보안은 연구개발 과정에서 산출되는 모든 것을 보호하는 제반활동을 말한다. 하지만 우리나라 연구보안 정책과 방향성에 세 가지 문제점이 존재하고 있다. 연구개발 현장의 보안 관련자와 연구 수행자에게 혼란을 야기시키는 법제도 문제가 있다. 그리고 과제의 등급을 체계적인 평가기준 없이 일반과제로 부여하는 문제점이 있다. 마지막으로 연구보안을 수행하려 해도 참고할만한 가이드라인이 부재한 현실과 연구보안에 대한 관심 부족이 심각한 문제점으로 나타나고 있다.

본 연구는 이러한 연구보안의 시급한 문제점 중, 연구 수행자, 연구보안 관리자 등이 과제의 등급에 맞는 연구보안 관리 활동을 할 수 있도록 국가연구개발과제 등급별 연구보안 관리지침을 설계하였다. 먼저 국가연구개발과제의 등급체계를 설계하기 위해 선행연구를 분석하였고, 1등급 과제, 2등급 과제, 3등급 과제를 분류하였다. 각 등급별 과제는 과제의 정보 유출 시 위험도와 과제의 정보 접근권한에 대한 수준을 기준으로 삼아 설계하였다. 다음으로 국내외 연구보안 관리지침에 대한 선행연구를 분석하여, 연구보안 관리체계, 연구시설 및 장비, 정보시스템 보안, 연구산출물 관리, 연구자 보안의 5가지 구분된 연구보안 관리지침 후보군을 수립하였다. 연구보안 관리지침 후보군에 대한 타당성을 검증하고 보다 면밀하게 고도화하기 위해 연구보안 전문가를 대상으로 초점집단 인터뷰를 수행하였다. 인터뷰 결과를 반영하여 수행 시기, 관리영역, 관리 항목, 관리 내용으로 구분하고, 연구 수행자보다 연구보안 관리부서의 역할에 중점을 둔 새로운 관점의 관리지침을 설계하였다.

해당 연구는 최근 국가적 관심이 증대되고 있는 연구보안에 대해 학문적 기초자료로써 도움이 될 것으로 판단되며, 특히 현장 연구보안 관리체계를 수입하는 데 많은 도움이 될 것으로 기대한다. 하지만 연구결과의 도출에 있어 FGI에 참여한 인원이 민간의 연구개발 정책 및 현장 보안 전문가라는 점을 고려했을 때, 정부 차원의 연구개발 보안 관련자의 의견을 개진했으면 더 풍부한 검증이 되었을 것으로 판단된다. 또한 기존 국내 연구보안 선행연구와 연구보안 전문가가 부족한 연유로 연구의 논증을 탄탄하게 뒷받침하지 못한 점에 대해서는 추후 해외 연구보안 선행연구를 면밀하게 탐색하여 반영함으로써 보충해 나가야 할 과제로 생각된다.

참고문헌

[1] Ahn, J. M., "New Directions for National R&D: Enhancement of Societal Impact and Openness," Journal of Social Science, Vol. 42, No. 3, pp. 119-139, 2016.

[2] Bae, J. M., Kim, S., and Chang, H. B., "A Study on Design Direction of Industry-Centric Security Level Evaluation Model through Analysis of Security Management System," The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 177-191, 2015.

[3] Bae, S. and Chang, H. B., "A Study on the Design of Security Level Evaluation Model for University Research Institutes," Korean Journal of Industrial Security, Vol. 12, No. 1, pp. 51-78, 2022.

[4] Blevins, Emily G., and Gallo, Marcy E., "Research security policies an overview," Congressional Research Service, Vol. IF12589, 2024.

[5] Canadian Centre for Cyber Security, "Security considerations for research and development organizations," Awareness series, 2024.

[6] Choi, J. and Jung, Y., "A Case Study on the National Major Technologies Leakage to Overseas Countries," Korean Journal of Industrial Security, Vol. 12, No. 2, pp. 137-160, 2022.

[7] Go, H. J., and Lee, C. M., "A Study on the Analysis and Countermeasures of Industrial Security Using FGI," Korean Security Management Association, Vol. 72, pp. 71-93, 2022.

[8] Han, S. Y., "Design of a Grade Classification System for Research and Development (R&D) Information," Chung-Ang University Graduate School, Thesis, 2023.

[9] Jeon, M., and Chang, H. B., "The Design Research on ICT Security Concepts and Domains," Information Systems Review, Vol. 21, No. 3, pp. 49-61, 2019.

[10] Kim, G. R., "South Korea's Defense Industry Development Strategy - Focusing on Technology Protection Policy -," Convergence Security Journal, Vol. 24, No. 1, pp. 83-93, 2024.

[11] Kim, Y. K. and Chang, H. B., "The Observational Study on Researcher Security Design Direction by R&D Security Accident Case," Journal of Platform Technology, Vol. 10, No. 4, pp. 91-96, 2022.

[12] Lee, J., Na, O., and Chang, H. B., "A Study on the Research Security System of the Researcher-Centric," The Journal of Society for e-Business Studies, Vol. 23, No. 3, pp. 65-84, 2018.

[13] Lee, T. and Hong, S., "A Study on the Actual Condition and Prevention of Industrial Security Crimes : Focusing on the Composition of the Model for Calculating the Amount of Damage Caused by Industrial Technology Leakage," Review of KIISC, Vol. 76, pp. 27-51, 2023.

[14] Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Newbury Park, CA: Sage.

[15] Ministry of Science, ICT and Future Planning, "Manual of Security Management on National Research Development Project," 2014.

[16] Ministry of Science and ICT, “A plan to strengthen the research security system to build a trustworthy research ecosystem,”2023.

[17] Na, J., “A review on verification strategies for qualitative research : Focusing on member check, peer debrief, and audit trail,”EDUCATIONAL RESEARCH, Vol. 70, pp. 233-254, 2017.

[18] Na, O., and Chang, H. B., "Design of National R&D Project Security Rating Evaluation Model", Journal of Korea Technology Innovation Society, Vol. 23, No. 4, pp. 841-862, 2020.

[19] Na, O., and Chang, H. B., "Research on the Level Evaluation Model of the Organization Research Security," The Journal of Society for e-Business Studies, Vol. 25, No. 3, pp. 109-130, 2020.

[20] National Law Information Center, https://www.law.go.kr/, 2024.08.18.

[21] NST, National Intelligence Service, "Research

Security Guide for Researchers," 2022.
[22] PangYu, "R&D project risk management research", E3S Web of Conferences, 2021.
[23] Yu, J., and Kim, B. K., "Trends and implications of major countries' policies related to research asset protection," kistep brief, Vol. 60, pp. 1-14, 2023.

〔저자소개〕

나 원 철 (Onechul Na)
㈜안랩 컨설팅본부/책임 컨설턴트
연구 세부분야 : 산업보안(Industrial Security), 연구보안(Research Security), 기업정보 보안(Corporate Information Security)

email : onechulna@gmail.com