http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.23, No.3, August 2018, pp.65-84
https://doi.org/10.7838/jsebs.2018.23.3.065

연구자 중심의 연구보안 체계 개선방안 연구

A Study on the Research Security System of the Researcher-Centric

이재균(Jeakyun Lee)*, 나원철(Onechul Na)**, 장항배(Hangbae Chang)***

초 록

정부는 4차 산업혁명 시대의 도래에 대한 적극적인 대응과 국민경제 발전을 위해 국가 R&D 투자를 지속적으로 확대하고 있다. 추격형 R&D에서 선도형 R&D로 패러다임을 전환하고, 연구자 중심의 창의성을 중시하는 R&D 역량 강화를 추진함에 따라 R&D 구조도 개방화가 점차 확산될 것으로 보인다. 이와 같이 다양한 R&D 환경의 변화로 인해 연구정보 유출 등 보안사고의 위험도 높아질 것이다. 이에 대비하여 연구성과물 보호를 위한 보안정책도 연구자 중심으로 전환해야 한다. 본 논문에서는 연구자가 연구수행 과정에서 필요한 보호조치를 자율적으로 수행 할 수 있도록 연구보안 체계를 연구자 중심으로 개선하는 방안에 대해 연구하였다.

ABSTRACT

The government is continuously expanding its national R&D investment to actively respond to the advent of the 4th industrial revolution era and to develop the national economy. The R&D structure is likely to be liberalized as the paradigm shifts from the pursuit type R&D to the leading type R&D, and R&D capacity enhancement that focuses on researchers' creativity is emphasized. Such changes in R&D environment will increase the risk of security accidents such as leakage of research information. In addition, security policy for protection of research result should be the Researcher-Centric Security and security policy should be changed. This study explored transforming the research security system into the Researcher-Centric Security system so that researchers can voluntarily implement necessary security measures in the course of conducting research.

키워드 : 연구보안, 연구자 중심 보안, 연구정보 보호
Research Security, Researcher-Centric Security, Protection of Research Information

---

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-2014-1-00636).
본 연구는 2018년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제(No.20174030201810)입니다.

* First Author, Department of Security Convergence, Graduate School, Chung-Ang University (illsan61@cau.ac.kr)
** Co-Author, Department of Security Convergence, Graduate School, Chung-Ang University (nastop@cau.ac.kr)
*** Corresponding Author, Department of Industrial Security, Chung-Ang University(hbchang@cau.ac.kr)
Received: 2018-06-11, Review completed: 2018-06-28, Accepted: 2018-07-13

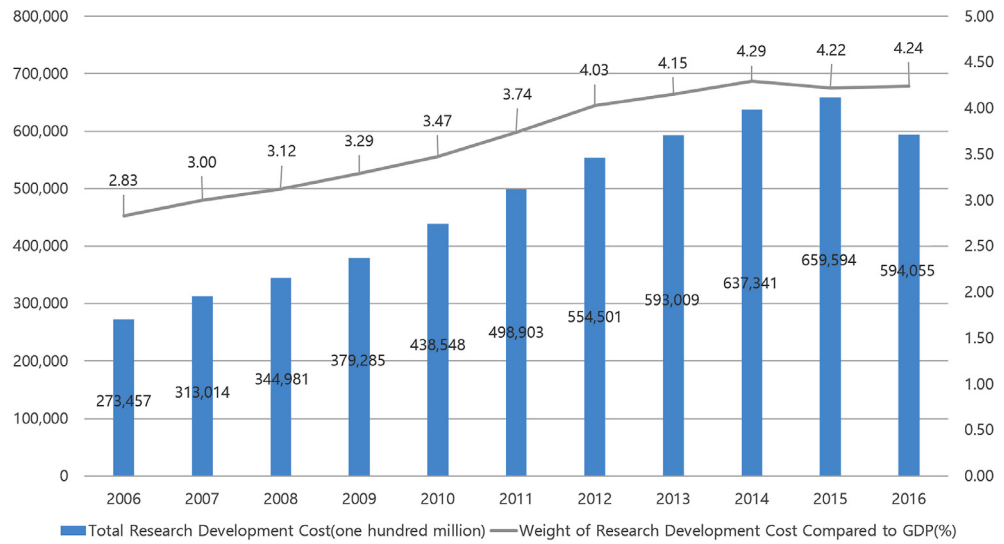
1. 서 론

글로벌 경제침체가 지속되면서 세계 각국은 저성장・고실업이 고착화되는 새로운 경제적 시대가 본격화됨에 따라, 주요 국가들은 연구개발(Research and Development, 이하 'R&D')이 미래 신성장 동력 확보 등 국민경제 발전에 도움이 된다고 판단하고 중장기 국가발전전략을 수립하는 등 국가 R&D 투자를 지속 확대하고 있다[15].

우리나라도 과학기술 기반조성과 혁신을 통해 국가경쟁력을 강화하기 위하여 5년마다 과학기술 발전에 관한 중장기 정책을 수립하고 R&D 투자를 매년 확대해 오고 있으나, 선진국의 견제와 후발국의 추격 등 영향으로 철강・자동차・반도체・디스플레이・휴대폰 등 주력 산업의 경쟁력이 약화되는 등 경제적 위기감이 높아지고 있다[2].

이러한 상황에서 4차 산업혁명은 인공지능(Artificial Intelligence, AI), 사물인터넷(Internet of Things, IoT) 등의 기술발전으로 기술・산업간 융・복합이 가속화되면서 경제・산업 등 사회전반에 걸쳐 많은 변화가 일어날 것으로 전망되고 있다. 정부는 이와 같은 시대적 변화에 대응하기 위하여 R&D 투자를 다양한 산업으로 확대하고, 추격형 R&D에서 선도형 R&D로 패러다임을 전환하였다. R&D도 연구자를 중심으로 자율성과 창의성에 중점을 두었으며, R&D 구조도 조직 내부에 제한되었던 폐쇄형 연구에서 외부 연구자와의 공동연구나 연구교류와 같은 개방형 혁신구조가 확산될 전망이다[15, 21].

한국과학기술기획평가원에서 발표한 자료에 따르면 국가 R&D 투자는 2006년 이후 꾸준히 증가하고 있으며 2016년 총 연구개발비는 2006년 27조 3,457억 원 대비 42조 598억 원이 증가한 69조 4,055억 원으로 대폭 증가한 것을 알 수 있는데, 이러한 국가 R&D 투자의 증가기조는 앞으로도 계속될 것으로 전망된다[10].



〈Figure 1〉 Weight of Research Development Cost compared to South Korea's Research Development Cost and GDP(Gross Domestic Product)

이와 같이 국가 R&D에 대한 지속적인 투자 증대로 인해 2016년을 기준으로 국가 R&D 사업 SCI(Science Citation Index, 국제 과학 논문 색인) 논문등재 성과는 37,385편, 국내 출원 특허는 30,807건, 해외 출원 특허 4,923건 등으로 국가 지식재산 창출을 통해 국가핵심기술을 비롯한 첨단산업기술 개발에 활용되는 등 국가경제 발전에 많은 기여를 하고 있다[14].

그러나 선・후발국을 막론하고 첨단산업기술 확보를 위한 국가 간 정보전이 치열해 지면서, 우리나라도 국가핵심기술과 첨단산업기술, 국가 R&D 성과물 등이 해외로 유출되는 사례도 늘어나고 있는 상황이다[22]. 특히 국가 R&D 성과물은 지식재산 창출은 물론 상용화 과정에서 국가핵심기술 또는 산업기술로 발전할 수 있어 해외로의 무단유출은 국가 경쟁력에 심각한 타격을 줄 수 있다. 2017년 국정감사자료에 따르면 2012년부터 2017년까지 총 157건의 산업기술이 해외로 유출되었으며, 이 가운데 국가핵심기술 유출 사건은 21건으로 매년 지속적으로 증가하고 있는 것으로 나타났다. 이중 대기업이 16%, 중소기업이 64%, 대학・공공연구기관이 20%를 차지하고 있는 것으로 나타났다[23].

정부는 이러한 위기상황에 대비하기 위하여 「과학기술기본법」과 「국가연구개발사업의관리 등에관한규정」(이하 공동관리규정)을 두어 국가 R&D 사업에 대한 보안대책을 강구토록 하고 있으며, 「산업기술의유출방지및보호에관한법률」(이하 산업기술보호법)을 제정하여 국가핵심기술과 산업기술의 무단 유출을 방지하고 있다.

하지만 이와 같은 정부의 산업기술 방지를 위한 대책은 최근 급변하는 R&D 환경 변화에 가변적으로 대응하지 못하고 있다. 또한 새로운 보안위협과 국가 R&D 사업에 대한 보안 취약성이 상존하고 있음에도 불구하고, 대부분의 국가 R&D 사업에서 중요한 역할을 담당하고 있는 연구기관, 대학 등의 연구보안 예산은 R&D 대비 매우 적게 편성되어 있으며 연구자의 보안의식 또한 매우 낮은 편이다. 따라서 본 연구에서는 이에 대비하여 국가 R&D 사업 연구성과물의 효과적인 보호를 위해 시대적 변화에 맞춘 연구자 중심의 보안관리 체계를 마련하여 개선해 나가고자 한다.

2. 연구개발과 연구보안

2.1 연구보안의 개념과 이행주체

연구보안은 국가 R&D 수행과정에서 창출되는 연구 성과물 보호를 위한 실무용어로 사용되었으나, 「산업기술보호법」과 「과학기술본법」이 제정되고 한국산업기술보호협회와 한국산업보안연구학회 등이 설립되면서 법・학문적으로 널리 정의되기 시작하였으며 산업보안과 연계하여 점차 학문적인 영역으로 발전하고 있다.

장항배[1]는 관련 법률과 선행연구를 통해 연구보안의 개념을 다수 제시하고 있음에도 불구하고 연구보안의 개념은 그 해석에 따라 지켜야 할 보안대상이나 주체 등이 달라 질 수 있는 등 불확실한 점이 남아 있다고 보았다. 이러한 불확실성은 대부분 연구보안을 정의하면서 관련 법제인 「과학기술기본법」과 「산업기술보호법」 등을 기반으로 하고 있으나, 연구보안 정의에 보안관리 이행주체를 정확하게 구분하여 명시하지 않아 실무적으로 적용할 때 혼선을 일으키기 때문인 것으로 보인다.

구체적으로 연구보안에 대한 정의와 관련하여 관련 법률을 살펴보면 「과학기술기본법」 제16조의 2에서는 “중앙행정기관의 장 및 국가 R&D 사업을 수행하는 연구기관의 장은 국가 R&D 사업의 성과가 외부로 유출되지 아니하도록 보안대책을 수립・시행하는 것”으로 규정하여 보안관리 이행주체를 연구기관으로 규정하고 있으나, 같은 법에 따른 「공동관리규정」 제24조의7제2항에서는 “연구기관의 장 및 연구책임자는 제24조의4제1항의 보안등급에 따른 보안관리 조치를 하여야하며, 그 내용은 별표 2의4와 같다”고 규정하여 보안관리 이행주체를 연구기관장과 연구책임자로 구분하여 명시하고 있다. 또한, 「산업기술보호법」 제12조에서는 “대상기관의 장은 산업기술과 관련된 국가 R&D 사업을 수행하는 과정에서 개발성과물이 외부로 유출되지 아니하도록 필요한 대책을 수립・시행하는 것”으로 규정하여 보안관리 이행주체를 대상기관으로 규정하고 있으나, 같은 법에 따른 「산업기술보호지침」 제1조3항에서는 “R&D 보안관리는 R&D 수행에 따른 보호관리의 세부 절차를 정함으로써 개발 중이거나 개발된 성과물의 유출을 방지하고 나아가 R&D의 효율적인 수행을 하는데 목적이 있다”고 규정하고, 제30조에서는 적용범위를 “R&D 보안관리는 R&D를 수행하는 대상기관 및 해당연구에 참여하는 연구원에 대하여 적용”한다고 명시하여 보안관리 이행주체를 대상기관과 연구원으로 구분하고 있다[8, 16, 18, 19].

관련 선행연구를 살펴보면, 한국산업보안연구학회는 산업기술 보호를 위한 산업보안을 설명하면서 산업기술 창출의 기반이 되는 연구보안에 대해 “정부의 지원을 받아 국가 R&D 사업을 수행하는 기관에서 연구내용 및 연구결과물이 외부로 유출되지 않도록 관리하는 제반업무”로 정의하여 보안관리 이행주체를 연구기관으로 보았다[6]. 그러나 국가과학기술인력개발원은 연구보안은 “연구를 수행하는 자가 연구의 준비 단계부터 연구의 수행과정 및 연구 종료 이후 발생한 주요 연구정보 및 연구성과물이 무단으로 유출되지 않도록 방지하기 위한 제반 활동”으로 정의하여 대학・정부출연연구소 등 공공연구기관과 기업 등 민간연구기관에 속한 연구자(연구책임자, 참여연구원)를 보안관리 이행주체로 보았다[9]. 장항배[1]는 연구보안은 “R&D 생애주기 기반의 보안관리 체계, 즉 연구수행 과정에서 발생할 수 있는 보안사고로부터 보호가 요구되는 대상을 효과적으로 지켜내는 관리활동”이라고 정의하면서 국가과학기술인력개발원의 정의를 뒷받침 해 주고 있다. 강선준[5]은 연구보안이란 “정부의 지원을 받아 국가 R&D 사업을 수행할 때 발생하는 유・무형적 연구성과물, 기술이나 경영상 필요한 정보 및 지식재산을 각종 침해행위로부터 안전하게 보호・관리하기 위한 소극적 또는 적극적인 대책과 활동”으로 정의하고 있다.

이상에서 살펴본 바와 같이 연구보안에 대한 정의를 종합・분석해 보면, 연구보안이란 연구보안의 주체인 연구기관과 연구자가 객체인 R&D 과정에서 창출되는 성과물이 무단으로 유출・공개되지 않도록 보호하는 제반 보안관리 활동으로 해석할 수 있다. 따라서 본 연구에서는 연구보안을 “연구기관 또는 연구자가 R&D 과정에서 창출되는 가치 있는 모든 성과물을 보안사고로 부터 보호하기 위한 제반 보안활동”으로 정의하고자 한다.

이처럼 연구보안의 개념에는 국가 R&D 사업을

수행하는 연구기관장을 이행주체로 하는 “연구기관의 보안”과 R&D 사업을 직접 수행하는 연구책임자를 이행주체로 하는 “연구책임자의 보안”이 둘 다 포함되어 있으며, 연구보안의 대상에 따라 이행주체별로 보안조치 사항이 각각 다르거나 서로 연계하여 공동으로 조치해야 한다는 것을 알 수 있다.

연구보안의 이행주체를 구분하는 실익은 연구보안 사고 시 발생하는 책임성과 범죄성 때문이다. 이창무[12]는 보안은 사람의 의도적인 행동으로 피해가 발생하는 상황을 전제로 하는 것이므로 불법여부 즉, 범죄성과 관련이 있다고 보았다. 이는 연구보안은 국가 R&D 성과물을 무단유출 하는 의도적인 행위와 관련이 있으므로 범죄와 연결된다고 볼 수 있다. 따라서 연구보안의 이행주체를 연구기관장(기관의 보안책임자)과 연구책임자(R&D 사업의 보안책임자)로 구분하는 것이 보안관리에 대한 의무와 보안사고에 대한 책임을 명확하게 구분하는 것이므로 실무적으로는 매우 중요하다고 볼 수 있다.

「국가연구개발사업보안관리표준매뉴얼」에서는 연구기관의 보안총괄책임자를 “연구기관의 시설보안, 정보보안, 연구보안을 총괄적으로 관리하는 책임자”로 정의하고 있으며, 연구보안관리자를 “중요한 R&D 정보를 보호하기 위하여 연구보안 규정 제・개정 및 계획수립, 감독, 지도 등 일련의 보호활동을 하는 연구보안 책임자 및 담당자”로 정의하고 있다[17]. 그리고 「산업기술보호지침및매뉴얼」에서는 연구책임자를 “연구의 절차와 방법에 따라 실제 연구를 진행하고 주관하는 책임자”로 정의하고 있다[7]. 본 연구에서는 관련 법제 및 선행연구를 분석하여, 연구기관장은 기관 전체의 보안에 대해 총괄적 책임이 있으며, 연구책임자는 R&D의 전 과정에 걸쳐 연구성과물 보호에 대한 총괄적 책임이 있다고 보았다.

2.2 연구자 중심의 R&D와 연구보안

연구자 중심의 R&D란 연구자를 중심으로 R&D에 대한 책임성은 강화하되 창의적이고 자율적이며 개방적 R&D 혁신 시스템을 지원하는 것이다[13]. 이를 상세히 설명하면 첫째, 연구자의 창의성을 중시하는 R&D 수행이다. 즉, 모든 연구 분야가 연결되는 초연결성과 융・복합적 연구 환경에서 창의적인 방식으로 연구를 수행할 수 있도록 행정적 처리를 간소화 하는 것이다. 둘째, 연구자의 자율적 R&D 활동이 보장돼야 한다. 즉, 기관 중심 관리에서 연구자 중심 지원제도로 개선하여 연구자가 책임성과 자율성을 가지고 연구할 수 있도록 지원하는 것이다. 셋째, 개방형 R&D 역량의 강화다. 즉, R&D 혁신을 위해 내・외부 연구기관 간 정보공유와 협력 등의 개방형 R&D를 활성화해야 한다.

이처럼 연구자 중심 R&D 환경으로의 변화에 따라, 연구보안도 연구자 중심의 연구보안 체계로 개선할 필요가 있다. 기존의 연구기관 중심의 관리적 연구보안 체계를 연구자 중심의 R&D에 그대로 적용하기에는 연구 환경적 차이로 인한 한계점이 존재한다. 연구보안도 연구자 중심의 보안관리 체계로 개선하여 새로운 R&D 환경에서 발생할 수 있는 다양한 보안사고의 취약성을 보완할 필요성이 있다.

따라서 본 연구에서는 연구자 중심의 연구보안의 개념을 “R&D 과정에서 창출되는 연구성과물 보호를 위해 연구자가 자율적으로 보안

〈Table 1〉 Security Area and Detailed Measure of Joint Management Regulation

Area	Detailed Measure
1. Security Management System	9
2. Management of Participating Researcher	9
3. Content of Research Development and Management of Results	7
4. Management of Research Facilities	6
5. Management of Information and Communication Network	16
Total of 5 Area	Total of 47

〈Table 2〉 Self-Assessment Table and Detailed Self-Assessment Table

Division	Self-assessment Table	Detailed Self-assessment Table	
Area	Checklists	Field	Checklists
1. Management	5	2	11
2. Assets	16	3	15
3. IT	9	3	23
4. The Outside	6	2	11
5. Incident Correspondence	4	3	12
5 Areas	40 Checklists	15 Fields	100 Checklists

조치 사항을 이행할 수 있도록 연구자를 중심으로 보안정책 수립 및 보안관리체계를 구축하는 것"으로 정의하였다.

부연하자면 연구기관이 보안목표와 보안조치 사항을 일방적으로 결정하고 이를 기반으로 수행 결과를 평가하는 관리중심의 보안체계가 아니라, 연구책임자가 R&D 과정에서 보안대책(보안조치 항목, 보호기간, 보호절차)을 유연하게 조치할 수 있도록 사전에 협의하여 연구기관장과 연구책임자의 업무를 분담함으로써 보안조치에 따른 의무와 책임을 인식하도록 하는 것이다. 그리고 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」 등에 산재되어 있는 연구보안 관련 보안조치 항목들을 통합하여 연구책임자 중심으로 간편하게 정리하고, 보안절차를 개선(전산화 등)하여 실행 매뉴얼 등을 제공해 주는 것이다.

3. 연구보안 법제와 보안관리 체계

3.1 연구보안 관련 법제 및 관리체계 비교

국가 R&D 사업에 대한 연구보안 관련 법제는 「과학기술기본법」과 같은 법에 따른 「공동관리규정」이 있는데, 동 규정은 국가 R&D 사업의 보안관리 조치사항에 대한 이행대상을 연구기관 및 연구책임자로 구분하여 연구보안을 5개 영역과 47개 세부조치사항으로 제시하고 있다.

산업기술 보호관련 법제는 「산업기술보호법」과 같은 법에 따른 「산업기술보호지침」이 있는데, 동 지침은 국가핵심기술 또는 산업기술을 보유하고 있거나 R&D를 수행하는 대상기관의 보안관리 지침으로 자가진단의 주체로서 대상기관의 장과 보안관리 부서장(이하 "보안책임자")을 명기하고, 자가진단 표(5개 분야 40개 점검

〈Table 3〉 Qualification Standard of Information Security Management System (Total of 18, based on 104 Item)

IS(Information Security) Management Processes	
Management Processes Steps	Detailed Management Processes
1. Establishment of IS Policies and Setting ISMS scope	2
2. Management Responsibility and IS Organization	2
3. Risk Management	3
4. Implementation of IS Countermeasures	2
5. Post Management	3
5 Steps	12
IS(Information Security) Countermeasures	
Control Area	Control Activities
1. IS Policies	6
2. IS Organization	4
3. Security of External Parties	3
4. Information Asset Classification	3
5. Education and Training on IS	4
6. Personnel Security	5
7. Physical Security	9
8. System Development Security	10
9. Cryptography Control	2
10. Access Control	14
11. Operations Security	22
12. Intrusion Incident Handling	7
13. Disaster Recovery Planning	3
13 Item	92

항목)와 세부적 자가진단 항목(5개 분야 15개 영역 100개 점검항목)을 제시하고 있다.

「정보통신망이용촉진및정보보호등에관한 법률」(이하 정보통신망법)과 같은 법에 따른 「정보보호관리체계」가 있다. 「정보보호관리체계」는 기업의 주요자산을 보호하기 위해 수립·관리·운영하는 보안관리 체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도로, 인증기준은 정보보호 관리과정과 정보보호 대책으로 구분하여, 정보보호 관리과정은 5단계 관리과정에 12개 세부기준을 제시하고 있으며, 정보보호 대책은 13개 항목에 92개 세부기준을 제시하고 있다.

3.2 연구보안과 산업보안, 정보통신보안의 범위

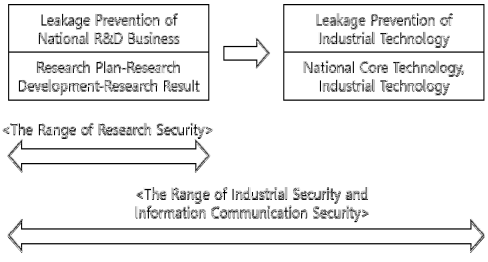
국가 R&D에 적용되는 보안활동은 관련 법령에 따라 연구보안과 산업보안으로 영역을 구분하여 적용하고 있다. 이러한 구분 기준은 R&D의 사전적 개념에 따르고 있는 것을 알 수 있는데, 두산백과사전[3]에서는 R&D를 “자연과학기술에 대한 새로운 지식이나 원리를 탐색하고 해명해서 그 성과를 실용화하는 일”로 정의하여 연구단계(연구보안)와 성과물의 실용화 단계(산업보안)로 나누고 있다.

즉, 연구보안의 범위와 대상은 R&D 과정에서

창출되는 모든 성과물을 대상으로 하고 있음을 알 수 있다. 「국가연구개발사업보안관리표준매뉴얼」은 연구성과물을 “R&D를 통하여 창출되는 특허・논문 등 과학기술적 성과와 유・무형의 경제・사회・문화적 성과”로 정의하고 있다. 이에 대해 산업보안의 범위와 대상은 「산업기술보호법」에 “산업기술과 관련된 국가 R&D 사업을 수행하는 과정에서 개발성과물이 외부로 유출되지 아니하도록”이라고 명시하고 있어, 산업보안의 대상은 모든 R&D가 아니라 산업기술과 관련된 연구성과와 개발성과물을 대상으로 하고 있음을 알 수 있다[18, 19].

따라서 연구보안의 범위는 R&D 과정 전체와 연구성과물로써 연구기획부터 지식재산권 확보까지의 단계이며, 산업보안의 범위는 산업기술과 관련된 R&D 과정 전체와 연구성과물에 개발성과물을 더하여, 연구보안 범위를 포함한 국가핵심기술 및 산업기술로 상용화된 이후의 단계까지 포함하고 있다고 할 수 있다.

또한, 정보통신보안은 정보통신기술이 연구보안 및 산업보안 등 거의 모든 분야에 걸쳐 활용・융합되고 있으므로 연구기관 및 대상기관 전체의 보안영역 중 하나이지만 그 활용도와 영향력이 크기 때문에 독자적인 영역으로 구축해 나가고 있는 것으로 이해해야 한다.



〈Figure 2〉 The Range of Research Security, Industrial Security, Information Communication Security

3.3 기존 보안체계의 시사점

「과학기술기본법」의 「공동관리규정」, 「산업기술보호법」의 「산업기술보호지침」, 「정보통신망법」의 「정보보호관리체계」에서 제시하고 있는 내용을 분석해 보면 다음과 같은 시사점을 발견할 수 있다.

첫째, 「공동관리규정」은 연구기관 전체에 적용되는 포괄적인 보안체계를 규정하고 있으므로 연구자 중심의 R&D 사업 수행에 대해 동일한 기준의 보안체계를 적용하는 것은 무리가 있다. 따라서 연구자 중심의 연구보안은 연구수행 과정에 필요한 내용으로 보안 체계를 구성하여 연구자(연구책임자 및 참여연구원)가 자율적으로 보안조치 사항을 이행할 수 있도록 개선하여 설계 할 필요가 있다. 또, 연구자 중심 R&D는 내・외부 연구기관 간 협업이나 공동연구와 같은 개방형 연구구조로 인해 연구 성과물의 외부 유출위험도 증가가 예상되고 있으나, 이에 대응하는 보안지표가 충분히 반영되어 있지 않았다[20]. 따라서 개방형 R&D 구조에 적합한 보안지표의 개선이 필요하다.

둘째, 「산업기술보호지침」은 「공동관리규정」의 연구보안을 준용하면서도 보안수준 자가진단에는 연구보안 내용이 거의 포함되어 있지 않았으며, 보안진단의 주체도 대상기관장과 보안책임자로 설정하고 있어 연구책임자의 보안조치이행 항목을 별도로 제시하지 않고 있었다. 따라서 「산업기술보호지침」 자가진단 항목도 연구보안 부분은 「공동관리규정」의 보안영역과 보안조치 항목에 통합해서 개선할 필요가 있다.

셋째, 「정보보호관리체계」는 정보보호 분야에 전문화되어 있는 보안체계로 모든 기관・기업・대학 등에 대한 정보보호체계를 관리 및 통제사항으로 제시하고 있으므로, 연구기관 또는

연구책임자의 전체적인 보안조치 항목을 포함하고 있지 않았다. 그러나 최근 정보통신의 발달과 ICT 융합 등으로 기관전체는 물론 연구책임자의 전 연구과정에서 정보보호 관리체계의 비중과 활용도가 높아지고 있는 점을 감안하여, 연구기관장(정보보호책임자)과 연구책임자가 이행해야 할 정보보호 관리 및 통제항목을 구분하여 연구자 중심의 연구보안 체계에 폭넓게 반영할 필요가 있다.

4. 연구자 중심의 연구보안 체계 개선방안

4.1 연구자 중심의 R&D 사업 보안영역 설정

본 연구에서는 앞에서 설명한 R&D 법제에 따른 보안체계의 시사점에서 기술한 바와 같이 각 기존의 연구보안 체계가 가지고 있는 한계점을 개선하여 연구자 중심의 연구보안 영역분류 및 보안조치 항목을 도출하고자 한다.

기존의 연구보안 체계는 앞서 살펴본 바와 같이 「공동관리규정」은 5개 영역 47개 세부조치사항을 제시하였으며, 「산업기술보호지침」은 자가진단 5개 영역에 40개 진단항목과 세부자가진단 100개의 진단항목을 제시하고 있고, 「정보보호관리체계」는 5개 영역 12개 관리항목과 92개 통제항목을 제시하고 있다. 이처럼 보안영역 구분 및 보안조지항목 들은 모두 각각 다른 법률에 근거한 것으로 모두 기관 및 기업의 보안수준 평가 또는 측정을 목적으로 개발된 보안지표로 구성되어 있다. 따라서 보안항목들이 대부분 중복되거나 누락되어 있는 등의 문제점이 발견되었다. 따라서 연구자 중심의 보안조치 항목을 하나로 통합하여 중복되는 부분은 삭제하고 새로 추가되는 항목은 편입하는 등 재조정이 필요하다.

본 연구에서는 연구보안 체계를 연구보안의 기본 규정인 「공동관리규정」의 체계를 준용하여 보안관리 정책, 참여연구원 관리, 연구개발 내용 및 성과의 관리, 연구시설관리, 정보통신망관리 등 총 5개 영역을 사용하였다.

4.2 연구자 중심의 연구보안 체계 개선방법 개발

본 연구에서는 연구자 중심의 연구보안 체계 개선을 위해 「공동관리규정」의 5개 연구보안 영역에 「산업기술보호지침」과 「정보보호관리체계」의 항목을 통합하고, 보안조치 항목 이행대상자를 기관 보안책임자로서의 연구기관장과 R&D 사업 보안책임자로서의 연구책임자로 구분하였다.

연구보안 영역별 보안조치 항목 개발은 4단계에 걸쳐 진행하였다. 1단계에서는 연구보안 관련법규에 의해 시행되고 있는 「공동관리규정」, 「산업기술보호지침」, 「정보보호관리체계」 등에서 제시하고 있는 보안관리 체계를 선정한 후, 보안조치 항목 이행대상이 구분되어 있지 않은 「산업기술보호지침」 및 「정보보호관리체계」에 대해서는 각 보안조치 항목별로 연구기관장과 연구책임자로 구분하는 전문가 설문조사를 실시하였다. 설문조사는 산・학・연・관의 연구보안 전문가를 대상으로 진행하였다.

2단계에서는 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」의 항목을 비교・분석한 후, 대표적인 연구보안 기본규정인 「공동관리규정」 보안체계에 맞추어 통합・분류하였다. 이 과정에서 각 보안체계마다 보안영역과 보안조치 항목의 명칭이 상이한 문제는 「공동관리규정」의 “보안영역”과 “보안조치 항

목"으로 용어를 정리하였으며, 중복・유사 항목은 삽입・명칭변경 등의 과정을 거쳐 하나의 항목에 통합하여 표기하였으며, 「공동관리규정」에 없던 새로운 항목은 추가하는 방식으로 모든 항목을 포괄적으로 나열하였다.

3단계에서는 2단계서 통합하여 포괄적으로 나열한 각 후보항목에 대해 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」에서 제시한 3개 체계의 각 항목별로 "연구기관장"과 "연구책임자"로 보안조치 이행대상자를 구분하여 "O"를 표시하여 출처를 밝혔으며, 동시 이행항목은 둘 다 "O" 표시를 하였다. 그리고 소계 칸을 두어 각 체계에서 제시한 개수를 숫자로 표시하였다.

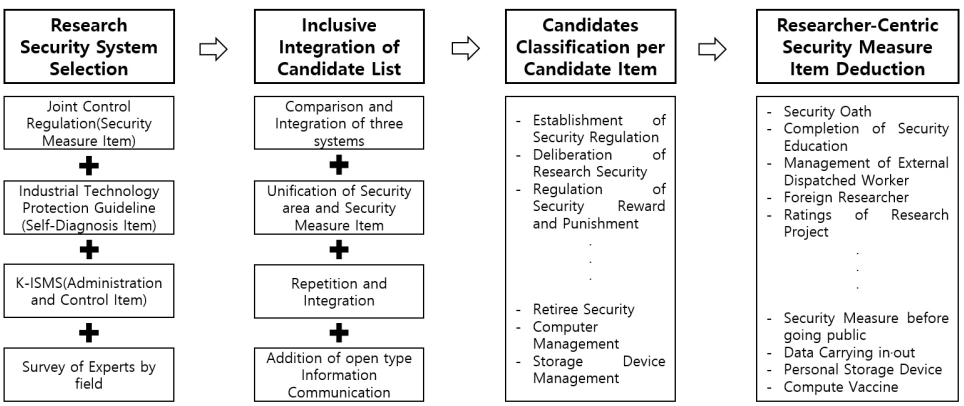
4단계에서는 3단계에서 구분한 연구책임자의 보안조치 이행항목과 공동 보안조치 항목에 표시된 항목만을 선별하여 재정리하였다.

이상과 같은 연구자 중심의 연구보안 보안조치 항목 후보를 도출하는 과정을 도식화 하면 다음 <Figure 3>과 같다.

4.3 연구보안 체계 통합 및 이행대상 구분

본 연구에서 추구하는 연구자 중심의 보안조치 항목을 도출하기 위해서는 먼저 「공동관리규정」, 「산업기술보호지침」, 「정보보호관리체계」 등 3개의 체계로 분리되어 사용되고 있는 보안체계를 하나의 체계로 일원화하는 통합과정이 필요하다. 이를 위해 3개 항목을 비교・분석한 후, 대표적인 연구보안 기본규정인 「공동관리규정」 보안체계에 맞추어 통합・분류하였다. 이 과정에서 각 보안체계마다 보안영역과 보안조치 항목의 명칭이 상이한 문제는 「공동관리규정」의 "보안영역"과 "보안조치 항목"으로 용어를 정리하였으며, 중복・유사 항목은 삽입・명칭변경 등의 과정을 거쳐 하나의 항목에 통합하여 표기하였으며, 「공동관리규정」에 없던 새로운 항목은 추가하는 방식으로 모든 항목을 포괄적으로 나열하였다. 통합하여 포괄적으로 나열한 각 후보항목에 대해 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」에서 제시한 3개 체계의 각 항목별로 "연구기관장"과 "연구책임자"로 보안조치 이행대상자를 구분하여 "O"를 표시하여 출처를 밝혔으며, 동시 이행항목은 둘 다 "O"표시를 하였다.

이를 정리하면 <Table 4>와 같다.



〈Figure 3〉 Deduction Process of the Researcher-Centric Security Measure Item

〈Table 4〉 Classification of Security System Integration and Security Measure Objects of Implementation

Area	Security Measure	Object of Implementation							
		Joint Regulation		Protection Guideline		ISMS		Subtotal	
		Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director
1. Security Management System (11)	Enactment and revision of one's own regulation · guideline reflecting a research security policy, approval of administrator and executives distribution	O		O		O		3	
	Regular examination on regulation · guideline in case of occurrence of external and interior environment change			O	O			1	1
	Constitute · manage a security manager planning session or research security council to consult · deliberate a research security agenda	O		O		O		3	
	Assignment of employee exclusive for security task · division of labor for comprehensive plan · management of research project security management	O		O	O	O		3	1
	Education · advertisement on r&d business security management division and security related regulation regarding a research manpower	O		O				2	
	Clear statement of reward and punishment on security superiors and regulation violator one's own security management regulation	O		O		O		3	
	Prepare a recurrence prevention measure such as prevention · action · respond etc. of security incident	O		O		O		3	
	Implementation of regular · frequent security inspection and security education on research institution and researcher	O		O		O		3	
	Establishment of response plan in case of emergency such as fire, flood, disaster, catastrophe, etc.	O		O		O		3	
	Retention status and status confirmation of security material, register a security transactor, discussion for disposal of expired security material			O	O			1	1
	Conduct a prior approval process in case of joint research · consignment research with foreign corporation and overseas research institution	O	O	O	O			2	2
2. Managing a Participating Researcher (10)	Specify a security responsibility duty such as participating researcher making security pledge · storage and obey security regulation etc.	O	O	O	O			2	2
	Conducting a security education to enhance the security awareness of research project researcher		O		O			2	
	Regulation and action such as security investigation for a retiree(expected to be)carrying out the data, withdraw of research results, block an access of computer network etc.	O		O	O	O	O	3	2
	Tendency understanding of retired researcher(in the range of not being contradictory to the law)			O				1	
	Regulation and fulfillment of security measure for of external institution and visitors such as external institution	O	O	O	O			2	2

〈Table 4〉 Classification of Security System Integration and Security Measure Objects of Implementation(Continues)

Area	Security Measure	Object of Implementation							
		Joint Regulation		Protection Guideline		ISMS		Subtotal	
		Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director
2. Managing a Participating Researcher (10)	Special management measure in case of suspect(ex-convict) of research result leakage participate in project	O		O	O			1	2
	Prior security education and homecoming report in case of researcher's overseas business trip (including lose data, contacts, etc.)	O	O	O	O			2	2
	Security measure on foreign researcher (english oath, on-limits area and limits on carrying in · out, tendency management)	O		O				2	
	Status management of foreigners who contact with security project participating researcher regarding a projects	O	O	O	O			2	2
	Fulfillment of affiliated approval procedure in case of foreign researcher participate in security project		O		O				2
3. Management of Research Development Content and Result(16)	Authorize security ranking or mark on every document produced during the execution process of research development project		O		O				2
	Check whether confidential documents and research data, storage device, etc. Is left alone in office desk, drawer, etc.				O		O		2
	Prepare a measure for information leakage through office machine for common use, muniment room, pc for common use, file server, etc.				O	O	O	1	2
	Fulfillment of approval procedure in case of peruse of confidential document and important research development data, records and carrying out to outside				O				1
	Security measure such as writing research note and security management regulation, peruse of research note and return	O	O	O	O			2	2
	Assurance method and propel of iprs (intellectual property rights) such as patent · utility model, etc. Per research conduction steps	O	O	O	O			2	2
	Prepare · conduct security measure for prevention of illegal outflow of major research data and research result	O	O	O	O			2	2
	Prior security inspection of research director in case of going public(including website) and offering of research development result	O	O	O	O			2	2
	Security inspection by research director beforehand for research development data which to be presented or go public during overseas business trip	O	O	O	O			2	2
	Obey related statue(national core technology, etc.) in case of overseas technology transfer of research development result	O		O				2	
	Conduct an education on procedure of risk management by phase, creation of legal right and contract procedure in case of external contract			O	O			1	1

〈Table 4〉 Classification of Security System Integration and Security Measure Objects of Implementation(Continues)

Area	Security Measure	Object of Implementation							
		Joint Regulation		Protection Guideline		ISMS		Subtotal	
		Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director
3. Management of Research Development Content and Result(16)	Consider a person inside the country as contracting objet in priority in case of using research development result	O						1	
	Prepare a prior security measure and application on belonging of result, materials offer and return of equipment, etc. In case of joint(cooperation, consignment) research agreement of security project with external institution	O	O	O	O			2	2
	Sign "prohibition agreement on third party rights of execution of technique(usage)" in case of agreement of research result execution of technique(usage)	O						1	
	Prior security inspection on open technique and range of product in case of participating in overseas exhibition			O	O			1	1
	Security measure regulation and inspect security fulfillment, conduct a security education in case of overseas expansion			O				1	
4. Management on Research Facility(8)	Prepare a plan and conduct on carrying information communication device such as laptop, exterior storage device, etc. In · out	O	O	O	O	O	O	3	3
	Install high-tech equipment such as cctv, intrusion alarm device, etc. And operate inspection on major facility	O		O	O			2	1
	Designate as retention area on important facilities such as r&d project · information storage computer room, etc. And special protection management	O		O		O		3	
	Control on carrying in unnecessary material, approval procedure and maintain records in case of visit · work in retention area			O	O	O	O	2	2
	Periodical inspection on security weak point and complement on retention area			O	O	O		2	1
	Internal access control of research facility of external resident institution(including venture company)	O		O	O			2	1
	Personal discriminatory granting and control on research facility visitor	O		O				2	
	In case of external visitor's access, prior authorization from chief security officer	O	O	O	O			2	2
5. Management of Information Network System(33)	Operate an installation on every kind of equipment such as computer network firewall aim for research project security, intrusion detection system, etc.	O		O		O		3	
	Conduct on implementation of security measure such as execution of security oath in case of consigning organization's data processing task to outsider or grant of access on information assets					O		1	
	Periodical inspection on fulfillment subjects when contract with outsider, termination of an agreement, when the person in charge is changed, offered data should be returned and remove an authorization of access, request a fixing letter of maintenance of secret on acquired content					O	O	1	1

〈Table 4〉 Classification of Security System Integration and Security Measure Objects of Implementation(Continues)

Area	Security Measure	Object of Implementation							
		Joint Regulation		Protection Guideline		ISMS		Subtotal	
		Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director
5. Management of Information Network System(33)	Implement a preparation for access control such as misuse monitoring and device security prepared for infringement incident such as information leakage, etc. In case of connecting a mobile device through internal · external network for the purpose of task					O	O	1	1
	Designate as major position who handles an important data such as personnel information, research data, etc.					O		1	
	Prepare a security control measure and separate a job role for intentional occurrence of incident such as authorization misuse					O	O	1	1
	Information security management system education and include a enhancement of expertise by duty which targets every employee(including outsider)					O		1	
	Arrangement of limit on information system access and periodical inspection of appropriateness through user authentication in case of access to local network from outside	O		O		O		3	
	Prior approval of security management director in case of installation of equipment · software on pc	O	O	O	O	O		3	2
	Establishment of management procedure, such as modification cycle of pc password, etc., specify a management responsibility, extra protection for administrator password			O		O		2	
	Security measure such as user authentication, cryptographic communication, periodical modification of cryptographic key and etc. In case of wireless network construction	O		O		O		3	
	Build r-hdd, portable storage device usage procedure and usage of authorized device from affiliated institution beforehand	O	O	O	O	O	O	3	3
	Build data backup system and storage of important data copy in long distanced security facility for safety accident	O		O		O		3	
	Control · approval on storage device being carrying in · out to inside · outside and limit on local network connection	O	O	O	O	O	O	3	3
	Conduct an inspection whether malicious program is installed or not on computerized equipment right after overseas business trip researcher has possessed	O	O	O	O			2	2
	Fill in mou regarding an establishment of scurity policy prepared for transmitting an important information to external institution, management responsibility of information transmission					O			1

〈Table 4〉 Classification of Security System Integration and Security Measure Objects of Implementation(Continues)

Area	Security Measure	Object of Implementation							
		Joint Regulation		Protection Guideline		ISMS		Subtotal	
		Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director	Research Institution	Research Director
5. Management of Information Network System(33)	Installation and update of security s/w, security patch, screen saver, etc. Targeting a pc for business use	O	O	O	O	O	O	3	3
	Store a composition modification of information system, records of usage log, prepared for security incident	O		O		O		3	
	Discriminatory granting of server access authorization according to one's position · task or importance of saved data	O		O		O		3	
	External security on user certification consideration and network data(system configuration, ip status) in case of construction of information system	O		O		O		3	
	Devise a security measure in case of external repair request on data restoration for pc, laptop, r-hdd etc.			O	O	O	O	2	2
	Take an action so that major data stored in hard drive, etc. Be not to illegally restored in case of destruction of computerized equipment and transfer to outside	O	O	O	O	O	O	3	3
	Physical or logical(firewall, etc.) separation of local network per laboratory	O		O		O		3	
	Prior approval in case of copy · save · transfer a pc data for business use to personal device such as cell phone, mobile storage device, etc.	O	O	O	O	O	O	3	3
	Security countermeasure preparation and conduct on approval procedure, etc. In case of data transfer to outside using internet	O	O	O	O	O	O	3	3
	Periodical security weak point inspection on website			O		O		2	
	Prohibit an internet connection on important work processing pc and frequently inspect on defects			O	O	O	O	2	2
	Inquire security beforehand in case of building a wireless network, internet phone					O	O	1	1
	Conduct a security education of response procedure to infringement incident, etc., such as countermeasure of hacking e-mail, etc.					O		1	
	Conduct a self-periodical simulation training response to cyber crisis			O		O		2	
	Save relevant(including electronic document) such as investigation records of incident in case of infringement incident			O		O		2	
	Build emergency contact system with maintenance enterprise as a preparation for system error, etc.			O	O	O		2	1
	Access management of route with possibility of leakage route such as messenger, internet storage, external e-mail, etc.	O		O		O		3	

이상의 결과를 바탕으로 연구기관장과 연구책임자의 공동 보안조치 항목을 정리하면 연구보안 5개 영역에 78개 보안조치 항목이 도출되었으며, 이중 연구책임자가 이행해야 할 보안조치 항목은 공동 보안조치 항목 41개와 단독 보안조치 항목 4개 등 총 45개 항목이 도출되었다. 이를 정리하면 다음 <Table 5>와 같다.

도출 결과를 분석해 보면 보안영역별 보안조치항목 총 78개 중 연구기관장 33개 42.3%, 공동 보안조치 항목 41개 52.6%, 연구책임자 4개 5.1%인 것을 알 수 있다. 이처럼 기존의 연구보안 체계는 대부분 연구기관의 보안조치 사항이 차지하고 있으며, 연구책임자의 단독 보안조치 항목은 5.1%에 불과하다. 따라서 연구자 중심의 보안조치 항목 도출은 공동 보안조치 항목과 연구책임자 보안조치 항목을 합한 것이다. 다만, 공동 보안조치 항목에 대해 연구기관장과 연구책임자의 업무범위를 세밀하게 구분하여 제시하지 못한 점은 본 연구의 한계이다.

국가과학기술인력개발원에서는 연구보안의 주체는 “공공 및 민간의 구분 없이 정부출연연구소 등의 공공연구기관과 기업 등 민간연구기관에 속한 모든 연구자를 포함하며, 당해 연구자가 속한 연구기관”으로 설명하고 있다[9]. 따라서 연구자는 연구기관의 보안체계를 벗어나지는 못 한다. 본 연구에서도 연구기관은 안전한 연구과제 수행에 기반이 되는 보안정책, 인원・시설, 정보통신 등 기관의 총체적 보안 관리를 담당하고, 연구책임자는 연구기관의 보안체계 범위 내에서 보안정보를 공유하며 연구과정에서 창출되는 연구성과물 보호를 중점적으로 수행할 수 있도록 개선하는 것이라고 할 수 있다.

5. 결 론

정부는 4차 산업혁명 시대의 도래에 대한 적극적인 대응과 국가경쟁력 제고를 위해 R&D 투자를 전 산업으로 확대하고 있다. R&D 정책도 추격형 R&D에서 선도형 R&D로 패러다임을 전환하고, 창의성과 자율성, 개방성을 중시하는 연구자 중심의 R&D 역량을 강화하였다. 그러나 이와 같은 R&D 환경의 변화로 인한 보안취약성에 적극적으로 대비하지 않으면 연구정보 유출 등 보안사고로 인해 국가경제에 악

〈Table 5〉 Deduction of Research Director's Security Measure Item

Area	Security Measure Item	Classification of Object of Implementation		
		Head of Research Institution	Joint Measure Item	Research Director
1. Security Management System	11	7	4	
2. Management of Participating Researcher	10	3	6	1
3. Content of Research Development and Management of Results	16	4	9	3
4. Management of Research Facilities	8	2	6	
5. Management of Information and Communication Network	33	17	16	
5 Area	78	33	41	4

영향을 미칠 수 있다.

본 연구는 국가 R&D 사업과 관련한 연구과제 수행과정에서 발생할 수 있는 연구결과물 유출 등 연구보안 사고를 방지하기 위한 것으로써, 기존의 연구기관 중심으로 구성되어 있는 연구보안 체계에서 연구과제를 수행하는 연구책임자가 수행해야 할 보안조치 항목을 선별・보완하여 보안의 편의성과 효율성을 제고하는 연구자 중심의 보안관리 체계로 개선하는 방안을 정립하였다.

세부적으로 먼저 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」의 항목을 비교・분석한 후, 대표적인 연구보안 기본규정인 「공동관리규정」 보안체계에 맞추어 통합・분류하였다. 다음으로 도출한 각 후보항목에 대해 「공동관리규정」과 「산업기술보호지침」, 「정보보호관리체계」에서 제시한 3개 체계의 각 항목별로 “연구기관장”과 “연구책임자”로 보안조치 이행대상자를 구분하여 주체별로 이행여부를 합산하였다. 합산 결과 연구기관장과 연구책임자의 공동 보안조치 항목을 정리하면 연구보안 5개 영역에 78개 보안조치 항목이 도출되었으며, 이중 연구책임자가 이행해야 할 보안조치 항목은 공동 보안조치 항목 41개와 단독 보안조치 항목 4개 등 총 45개 항목이 도출되었다. 본 연구에서는 통합보안체계 78개 항목 중 연구책임자가 이행할 수 있는 항목 45개를 선별하여 ‘연구자 중심의 보안관리체계’로 개발하였다. 따라서 연구기관은 안전한 연구과제 수행에 기반이 되는 보안정책, 인원・시설, 정보통신 등 기관의 총체적 보안 관리를 담당하고, 연구책임자는 연구기관의 보안체계 범위 내에서 보안정보를 공유하며 연구과정에서 창출되는 연구성과물 보호를 중점적으로 수행할 수 있도록 개선하는 연구자 중심의 연구보안 체계로 개선하는 것이 중요하다고 할 수 있다.

그러나 본 연구에서 제시한 연구자 중심의 연구보안 체계 역시, 다음과 같은 한계점을 지니고 있다. 첫째, 연구자 중심의 보안관리체계의 조기정착을 위해서는 먼저, 「공동관리규정」 제24조의4에 의한 보안과제의 분류기준과 관련하여 보안과제 분류기준과 과제등급 다양화와 등급별 보안이행 사항 간편화 등이 필요한데, 이에 대한 개선안을 다루지 못했다. 둘째, 연구책임자의 자율적인 보안관리에 대응하기 위해서는 연구자의 창의성을 저해하지 않는 범위 내에서 일정한 책임과 의무를 부과해야 하는데, 이에 대한 필요성은 인식하고 있었으나 개선방안은 연구하지 못했다.

셋째, 연구자 중심의 자율적인 보안관리가 정착되기 위해서는 R&D 생애주기에 맞추어 보안조치 항목과 실행 매뉴얼 제시가 필요한데, 이에 대해서도 향후 연구할 필요가 있다고 본다. 따라서 본 연구에서 제시한 연구자 중심의 연구보안 체계 개선방안에 따른 보안 매뉴얼 등 후속조치가 조속히 이루어져야 할 것으로 보이며, 본 연구에서 해결하지 못한 한계점에 대해서도 향후 지속적인 연구・보완을 통해 연구자(연구책임자 및 참여연구원) 중심의 실용적이고 효율적인 연구보안 체계로 발전시켜 나갔으면 한다.

References

[1] Chang, H., The Importance of Research Security for Maximizing R&D Performance, The Electronic Times, 2017.

[2] Han, Y. and Kim, J., Government Research and Development Budget Analysis in the FY 2018, KISTEP, 2018.

[3] Http://www.doopedia.co.kr/, 2018.

[4] Jo, J. and Na, Y., A Strategic Investment Portfolio of Government R&D Projects for the Fourth Industrial Revolution, Korea Institute of Science & Technology Evaluation and Planning, Vol. 216, pp. 1-29, 2017.

[5] Kang, S. J. and Kim, M. J., "The Policy Proposal for the Security of Research Achievements Performing the International Cooperative Research in an Age of Open Innovation-Focused on Improvement of the Laws related International Cooperative Research," Law Review, Vol. 57, No. 3, pp. 91-127, 2016.

[6] Korea Association for Industrial Security, Industrial Security Studies, 2012.

[7] Korea Association Industrial Technology Security, Industrial Technology Protection Guidelines and Manuals, 2017.

[8] Korea Communications Commission, Act on Promotion of Information And Communications Network Utilization and Information Protection, Etc., 2018.

[9] Korea Institute of Human Resources Development in Science and Technology, Understanding research security, 2015.

[10] Korea Institute of Science Technology Evaluation and Planning, KISTEP statistics brief, Vol. 21, pp. 1-13. 2017.

[11] Korea Internet & Security Agency, K-ISMS, 2018.

[12] Lee, C., "A Critical Review of Industrial Security Concepts," Korean Security Science Association, Vol. 50, pp. 290-294, 2017.

[13] Lee, J. and Lee, N., Researcher-centered R&D system Innovation direction and task, Korea Institute of Science & Technology Evaluation and Planning, Vol. 208, pp. 1-18, 2017.

[14] Ministry of Science and ICT, 2017 White Paper of Science and Technology Statistics, 2018.

[15] Ministry of Science and ICT, 2018 Ministry of Science and ICT Department R&D project comprehensive enforcement plan, 2017.

[16] Ministry of Science and ICT, Framework Act on Science And Technology, 2018.

[17] Ministry of Science and ICT, ICT and Future Planning, Manual of security management on national research development project, 2014.

[18] Ministry of Science and ICT, Regulations on The Management, Etc. of National Research And Development Projects, 2018.

[19] Ministry of Trade, Industry and Energy, Act on Prevention Of Divulgence And Protection of Industrial Technology, 2017.

[20] Na, O., Chang, H., "An exploratory study for designing research security framework," Convergence Security Journal, Vol. 16, No. 2, pp. 50-62, 2016.

[21] Oh, J. H. and Koo, H., "The Influence of Cooperation Elements on the Joint R&D

Performance: Focused on IT R&D Project," The Journal of Society for e-Business Studies, Vol. 23, No. 1, pp. 23-36. 2018.

[22] Shim, W., "An Ex Ante Evaluation Method for Assessing a Government Enforced Security Measure," The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 241-256, 2015.

[23] The Financial News, Serious core industry technology outflow 'Corporate, national competitiveness is eaten', 2017.

저 자 소 개

이재균 (E-mail: illsan61@cau.ac.kr)
1985년 강원대학교 행정학과 전공 (학사)
1995년 강원대학교 행정대학원 행정학과 전공 (석사)
2018년 중앙대학교 융합보안학과 전공 (박사)
관심분야 산업보안, 산업보안 유관기관, 정책정보

나원철 (E-mail: nastop@cau.ac.kr)
2013년 한성대학교 컴퓨터공학과 전공 (학사)
2017년 중앙대학교 융합보안학과 전공 (석사)
2017년~현재 중앙대학교 융합보안학과 (박사과정)
관심분야 산업보안, 기업정보 보안, 연구보안, 보안데이터 분석

장항배 (E-mail: hbchang@cau.ac.kr)
2006년 연세대학교 정보시스템관리 전공 (박사)
2007년~2011년 대진대학교 경영학과 조교수
2012년~2013년 상명대학교 경영학과 조교수
2014년~현재 중앙대학교 산업보안학과 부교수
관심분야 중소기업 정보보호, 정보 오남용 및 유출방지, 성과분석 체계