연구보안 사고사례분석을 통한 연구자 보안대책 설계방향 관찰연구

[1] 김영권, [2*] 장항배

The Observational Study on Researcher Security Design Direction by R&D Security Accident Case

[1]Youngkwon Kim, [2*]Hangbae Chang

요 약

오늘날 기술이 국가 경쟁력과 직결되는 기술패권 경쟁의 흐름 속에서 연구개발 투자뿐만 아니라 연구개발에 대한 보안중요성이 강조되고 있다. 그러나 연구개발 보안사고 발생이 가져오게 되는 위험성에도 불구하고 연구산출물에 대한 유출사고는 계속해서 발생하고 있다. 본 연구는 이러한 문제를 해결하고자 연구개발 산출물에 대한 유출사고의 사례를 분석하여, 연구기관 중심의 거시적인 보안관리체계보다는 연구현장에 있는 연구자에 대한 규정 개발이 시급하다는 1 차적 결론을 도출하였고, 그 다음 현장 관찰방법론을 통해 연구자 중심의 보안대책 설계 방향을 크게 4 가지로 세분화하였다. 본 연구를 통해 도출된 연구자 보안대책 설계 방향은 향후 연구현장에 특화된 규정 및 연구기관 보안 관리 체계 개발을 위한 기초자료로 활용될 것으로 기대한다.

Abstract

Recently, the importance of Research and Development(R&D) security as well as R&D investment is emphasized in the flow of technology hegemony competition, where technology is directly related to national competitiveness.However, despite the enormous impact of the R&D security failure results, research output leakage accidents continue to occur.To solve this problem, this study analyzed leakage accidents and cases of R&D output and concluded that it is priory to develop regulations to raise security awareness at the field researcher level rather than the macroscopic security management system. In addition, in order to design the direction of the researcher security measures, observational study was conducted at the university research site, and four directions were presented, including case analysis and integration. The direction for designing researcher security measures will be used as a basis for developing security regulations specialized in future research sites and security management systems for research institutes.

Keywords: *Observational study, Research Security, Security Countermeasures, National Advanced Strategic Industry Technology, National Core Technology*

[1] 오산대학교 컴퓨터소프트웨어과 교수 (ykkim@osan.ac.kr)
[2*] Corresponding Author 중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)

Received: Oct. 07, 2022, Revised: Nov. 21, 2022, Accepted: Nov. 23, 2022

I. 연구보안 출현배경과 중요성

코로나-19 를 통해 국가 간 교류가 어려워지고, 자원이 한계에 다다르면서 기술이 요새화되고 있다. 이러한 흐름은 국가가 보유하고 있는 기술이 국가 경쟁력으로 이어지는 현시점에서 더욱 더 가속화되고 있으며, 연구개발에 대한 집중적인 투자와 함께 보호대책 마련 또한 강조되고 있다. 국내에서도 “국가핵심기술”, “첨단전략산업기술” 등으로 특정 기술을 설정하고, 이에 대한 진흥정책을 추진하는 한편 해당 기술들에 대한 연구개발 과정 및 산출물에 대한 안전한 보호체계 구축을 제시하고 있다. 그러나 연구개발 현장에서의 연구자 보안의식은 매우 낮은 상태이며 이러한 이유로 인해 다양한 형태의 연구 산출물 유출 사고가 발생하고 있다[1]. 본 연구에서는 최근에 발생된 연구 산출물 유출 사고를 분석함으로써 개방(연구협업)과 보안(산출물 보호)이 공존하는 연구 현장에 대한 지속가능성을 확보하고자 한다.

II. 이론적 배경 및 선행연구

2.1 연구개발과 보안

국가적 수준의 보호대상 기술 식별과 보호대책 마련을 위해 국가핵심기술 보호를 위한 기존 “산업기술보호법”과 함께 최근 “국가첨단전략산업법”이 제정되었다. 우선 “산업기술보호법”에서 설명하고 있는 국가핵심기술은 국내외 시장에서의 가치가 높고 해외 유출 시 안보 · 경제적 악영향을 줄 수 있는 기술로써, 반도체, 디스플레이, 전기전자 자동차 · 철도, 조선, 원자력, 정보통신 기술 등의 분야를 대상으로 보호대상 기술을 설정하고 있다[2].

최근 제정된 “국가첨단전략산업법”은 국가첨단전략산업의 혁신 생태계 조성과 기술 역량 강화를 통하여 산업의 지속가능한 성장 기반을 구축함으로써, 국가 · 경제안보와 국민경제 발전에 이바지하고자 2022 년 시행되었다. 국가첨단전략 기술은 동법 제 2 조에서 국가 · 경제안보에 미치는 영향 및 국민경제적 효과가 크고 파급효과가 현저한 기술로 명시하고 있으며, 법 제 11 조를 통해 전략기술로 지정하기 위해 고려해야 할 종합적인 요소로서 해당 기술이 산업 공급망 및 국가 · 경제안보에 미치는 영향, 해당 기술의 성장 잠재력과 기술 난이도, 해당 기술이 다른 산업에 미치는 파급효과, 해당 기술이 가지는 산업적 중요성, 해당 기술이 수출 · 고용 등 국민경제에 미치는 영향을 제시하고 있다. 앞서 제시한 과정을 통해 선정된 국가첨단전략기술은 반도체, 디스플레이, 이차전지 분야로 구성되며 디램 적층형성 기술, 이미지 센서 기술 등 총 15 개 기술이 해당된다. 동법 제 3 조에서는 이러한 기술을 보호하기 위해 전략기술을 보유하거나 관련 산업을 영위하는 사업자가 전략기술의 발전에 필요한 연구 · 개발 기반 조성과 전략기술의 유출 방지를 위하여 노력해야 함을 명시하고 있으며, 법 제 12 조와 13 조에서는 전략기술의 수출 또는 인수 · 합병, 외국인 투자 등을 진행하려는 경우의 유출을 방지하기 위해 산업통상자원부장관의 승인을 받도록 명시하고 있다. 동법 제 5 조와 6 조를 통해서는 전략산업 등 육성 · 보호 기본계획 및 실행계획에 포함되는 내용과 수립 등에 관한 절차를 규정함으로써 주요 산업에 대한 강력한 육성과 보호체계를 마련하고자 하였다[3].

2.2 연구보안 정의와 범위

연구보안은 연구 환경에 존재하는 연구자료, 연구시설과 장비, 연구원 등과 같은 보호대상에 대해 연구자료 유출과 위·변조, 연구시설 및 장비 훼손과 탈취, 연구인력 대상 불법 스카우트 등과 같은 위험요소로부터 안전하게 보존하기 위한 활동을 의미한다[4]. 다시 정리하면, 연구보안 대상은 명시적인 연구개발 정보인 연구 장비와 시설을 비롯하여, 암묵적인 연구개발 정보인 연구 산출물과 성과물, 그리고 연구원 등을 포함한다. 그리고 연구 수행기관과 연구자 등으로 정리되는 연구보안 주체들이 보안규정, 보안장비, 보안시스템을 구축하고 운영하게 된다.

이러한 개념의 연구보안은 기존에 알고 있는 보안과는 차별적인 특성을 가지고 있다. 먼저 연구보안은 기술이 내재화된 제품 또는 서비스와 같은 최종 산출물에 대한 보안 뿐만 아니라, 기술개발 과정에 대한 보안활동을 포함한다. 다시 말하면 연구보안은 기술이 완성되기까지, 연구개

발 기획과 협약, 연구개발 수행, 연구개발 결과물 산출과 활용 등 전 과정에 대한 보안활동을 의미한다. 또한 연구보안은 관련 법령에 근거한 보안활동으로서 준거성과 함께, 발생된 보안 사고에 대한 사후 조치보다 사고 예방이 절대적으로 중요시되는 예방적 특성을 가진다[5].

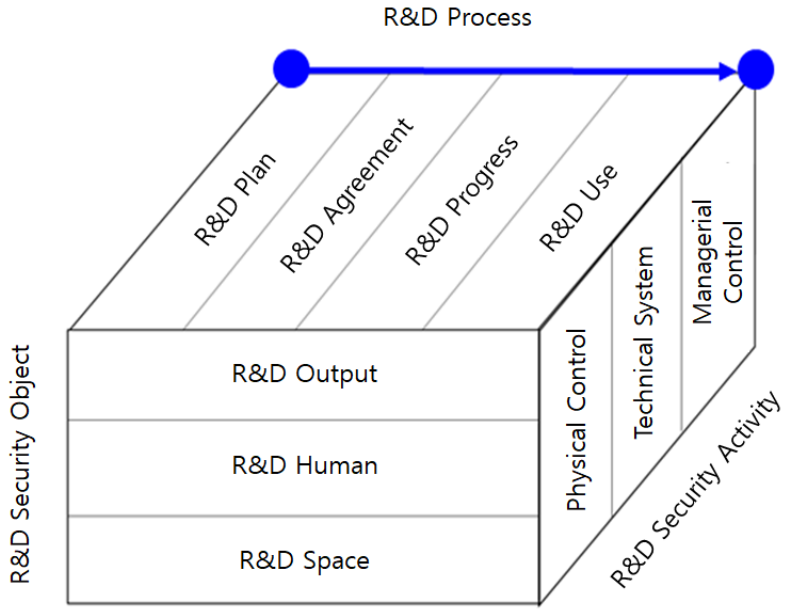

Figure 1. Research Security Concepts and Scope
그림 1. 연구보안 개념과 범위

아울러 이러한 내용을 법령으로 담은 내용이 “국가연구개발 혁신법”이다. 동법은 국가연구개발사업의 추진 체제를 혁신하고 자율적이고 책임 있는 연구환경을 조성함으로써, 국가혁신역량을 제고하고 국민경제의 발전과 국민의 삶의 질 향상에 이바지함을 목적으로 하고 있다. 제 21 조 제 1 항에서 “관계 중앙행정기관의 장 및 연구개발기관의 장은 소관 연구개발 사업 및 연구개발과제와 관련하여 연구개발성과 등 대통령령으로 정하는 중요정보가 유출되지 아니하도록 보안대책을 수립·시행하여야 한다.”고 명시하고 있다[6].

동법 시행령 제 45 조에서는 연구보안 활동이 집중적으로 적용되어야 할 보안과제 범위에 대해 정리하고 있고, 시행령 제 46 조에서는 전체적인 연구보안 대책을 설명하고 있으며, 세부적인 내용은 다음과 같다[6].

- 연구실에 대한 보호구역 설정
- 연구자의 연구실 출입권한 차등 부여 및 출입 현황 관리
- 연구자에 대한 보안교육 실시 및 보안서약서 제출 요청
- 외국인 연구자의 연구수행에 대한 연구개발 기관장의 승인 및 중앙행정기관의 장에 대한 보고
- 연구개발기관이 운영하는 연구관리 시스템에 대한 보안관리 조치
- 연구개발 정보처리 과정 및 그 결과에 대한 보안관리 조치

마지막으로 시행령 제 48 조는 연구보안 사고가 발생할 경우, 이에 대한 조치사항을 명시하고 있다[6].

2.3 연구산출물 사고·사례 분석

연구산출물 가치가 증대함에 따라 세계 주요 기술국을 대상으로 한 경쟁국가의 유출행위가 증가하고 있다. 우선 미국에서는 하버드대 저명 교수가 중국의 우수 인재 영입 프로그램인 천인계획(千人計劃)에 참여하여 중국으로부터 금전적 지원을 받는 대신 우한 이공대를 대신해 특허를 내고 국제회의를 조직하며 논문을 발표하는 역할을 담당한 사유로 유죄판결을 받았다[7]. 보스턴 대학교에서는 연구를 수행하던 중국 유학생이 중국 공모자의 지시에 따라 미국 프로젝트를 조사하고 공모자가 자신의 계정을 이용해 대학의 VPN 을 사용할 수 있도록 제공한 사례가 있다[8]. 다음으로 일본에서는 중국 연구자 9 명이 일본에서 유체역학 등을 연구한 뒤 귀국하여 중국 군수 관련 기업 산하 연구기관에서 극초음속 무기 개발의 핵심 기술인 풍동 실험 장치를 개발하였다[9].

또 다른 사례로는 중국 유학생이 중국 군인의 아내로부터 금전적 지원을 받고 일본 국내 렌탈 서버에 가입해 ID, PW 를 중국에 보냄으로써 해당 서버가 일본 200 여기관의 기밀을 노린 사이버 공격에 이용되어 큰 사고로 연계될 위험이 있었던 것이 해당된다[10]. 독일에서는 대학에 재직 중이던 러시아 출신 연구원이 현금을 대가로 러시아 정보 요원에게 자신이 대학에서 취득한 정보를 전달한 사례가 있으며, 호주에서는 325 명 이상의 학자 및 과학자가 자국의 군사 및 보안 프로그램 관련 기술을 중국에 이전하고 상용화할 것이 권고되는 천인계획 프로그램의 혐의자로 확인되었다[11][12]. 이처럼 해외에서의 기술유출 사고가 지속적으로 발생하고 있으며, 국내에서는 K 대학 A 교수가 중국의 천인계획에 참여하여 자율주행 관련 국가핵심기술을 중국으로 유출한 사례가 존재한다[13]. 이러한 연구산출물 유출 사고 · 사례에서 주목할 특징은 연구기관 중심의 보안관리체계보다는 연구현장에서 직접 연구를 수행하는 연구자 중심의 보안규정 개발이 선행되어야 함을 의미한다. 따라서 본 연구는 거시적 수준의 연구보안 관리체계 개발에 앞서 미시적 수준의 연구자 보안규정 개발 방향을 정리하고자 한다.

III. 연구자 보안대책 설계 방향

현재 또는 미래에 발생할 수 있는 보안위험을 예측하고, 이에 대한 보안대책을 마련하는 방법론을 활용하여 연구자 보안대책 설계 방향을 설정하고, 일부 세부적인 내용을 개발하였다. 세부적으로 실제 연구현장에서 진행되고 있는 연구 과정에 대한 관찰방법을 진행하여 보안관점의 특성과 쉽게 노출된 보안 취약점을 정리하였다. 관찰연구는 관찰을 통해 연구대상의 특성을 파악하고 분석하는 연구방법이다[14]. 관찰방법을 적용한 이유는 현재 연구보안과 관련된 연구수준과 규모는 매우 초기 상태인 관계로 관련 전문가는 절대적으로 부족한 상태이며, 연구보안에 대한 연구 현장에서의 인식내용도 매우 낮기 때문에 연구원 대상 설문수집이나 연구보안 전문가 대상 인터뷰 등을 통한 실증 연구 진행이 실제적으로 어렵기 때문이다. 참고로 관찰연구는 연구자가 관찰 상황 참여 여부에 따라 참여관찰과 비참여관찰로 구분되며, 본 연구는 실제 대학 연구실에서 수행되고 있는 연구에 1 개월 동안(2022 년 8 월 1 일 ~ 8 월 30 일) 직접 참여하는 과정에서 연구자 보안대책 설계 방향성을 도출하였다.

우선 보안대책 설계 방향을 도출하기 전에 연구 현장에서 관찰된 주요한 보안 위험 요소는 다음과 같이 정리할 수 있다. 연구과정 본연의 특성 중 하나인 개방성이 편의성과 매개하면서 보안관점의 취약점으로 노출되고 있다.

- 연구문서(정보)에 대한 분류와 중요도가 평가되지 않음
- 연구정보 공유와 연구자료 관리의 편의성을 위해 공유 폴더를 사용
- 개인용 스마트 폰이나 태블릿 PC 를 사용하여 정보를 공유
- 연구자료가 인터넷을 통해 다양한 방법으로 외부에 전송
- 타 연구공간에 자유로운 출입이 가능

이를 바탕으로 앞서 분석된 사례분석과 보안관점에서의 연구 현장 관찰을 통해 정리된 보안 대책 설계 방향을 크게 4 가지로 정리하였다. 무엇보다 연구개발과정은 다양한 이해관계자와의 개방형 협업연구를 지향하기 때문에 개방과 조정(제한과 통제) 사이에 적정선을 찾는 것이 중요하다. 더구나 최근 학제 간 융합연구와 함께 국제 공동연구 등을 통해 기존에 존재하지 않은 혁신적인 가치기술이 개발되기 때문에 연구의 깊이와 함께 너비가 확장되고 있으며, 연구 협업은 필수적인 절차로서 자리매김하고 있다. 안전한 연구개방 환경조성이 이루어질 수 있도록 연구보안 대책이 설계되어야 한다. 둘째로 수용성 높은 연구보안 대책이 마련되어야 한다. 특정 분야별 높은 수준의 지식을 보유하고 있는 연구자를 대상으로 보안규정이 내재화될 수 있도록 단방향의 딱딱한 보안교육보다는 공감대 형성을 통한 보안문화 환경이 조성되어야 한다. 참고로 보안문화는 단편적인 지식습득의 과정을 넘어서 보안의 중요성에 대한 인식, 보안에 대한 지식, 인지된 보안지식에 대한 실제적 행위 등이 반복적으로 환류 되면서 비로소 형성된다. 셋째로 연구자 보안활동을 지원할 수 있도록 지원체계 구축이 필요하다. 가치사슬 관점에서 조직의 사업내용이 생산공정에 따라 차별화되듯이 연구개발 과정도 학문 분야에 따라 다르고, 진행하고 있는 연구개발 기술성숙도에 따라 달라지기 때문에 연구특성을 고려한 연구보안 대책이 마련되어야 한다. 예를 들어, 제조 중심의 응용기술 개발과정과 기초과학 중심의 원천기술 개발과정은 공통의 보안규정과 함께 업(業)의 특성을 고려한 차별성 있는 보안규정이 마련되어야 한다. 마지막으로 규정(문헌) 중심보다는 사례 및 현장 중심의 보안규정을 설계할 필요가 있다. 연구기관이 추진하여야 하는 거시적 수준의 보안관리체계와는 달리 연구자에게는 핵심적인 보안규정 내재화가 효과적이기 때문에 방대하고 장황한 수준의 보안규정보다는 간략하고 쉽게 실행에 옮길 수 있는 보안규정 마련이 요청된다.

IV. 결론

미래 혁신성장을 지원하는 제품과 서비스를 제공하기 위해서는 속도감 있는 선도적 수준의 연구개발 진행이 선행된다. 그러나 연구개발 과정에서 산출물이 유출되는 경우에는 연구개발 투자자원의 손실은 물론, 연구된 기술이 실제적으로 적용되는 제품과 서비스의 시장 출시 기회 자체를 잃게 될 수도 있다. 그럼에도 불구하고 현재 학문 및 실무적 수준의 연구보안 수준은 여전히 미흡한 상태이며, 일부 규정들만 산재되어 있다. 본 연구에서는 개방형 혁신을 중시하는 연구현장에서 좀 더 실제적이고 내재화될 수 있는 연구자 보안대책 설계를 위한 방향성을 관찰방법을 통해 제시하였다. 본 연구에 있어 관찰내용은 대학이라는 일부의 연구 현장에 한정되어 있다는 한계성을 가지고 있으나, 향후에는 정부출연연구소 및 기업부설연구소 등으로 확장을 진행할 예정이다. 아울러 연구자 보안대책 설계 방향을 근거로 현재 규정 중심의 보안대책이 좀 더 자연스럽게 자리매김할 수 있는 연구 현장에 특화된 보안규정 개발과 연구기관의 보안관리체계를 개발할 계획이다.

V. 감사의 글

본 연구는 2022 학년도 오산대학교 교내 연구비 지원에 의하여 이루어졌음

VI. 참고문헌

[1] J. Lee, O. Na, H. Chang, “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.
[2] Act On Prevention Of Divulgence And Protection Of Industrial Technology
[3] Act On Special Measures for Strengthening and Protecting the Competitiveness of National Advanced Strategic Industries
[4] NST, NIS, “Research Security Management Guide for Researchers”, 2022

[5] https://www.etnews.com/20220616000192
[6] National Research And Development Innovation Act
[7] https://www.joongang.co.kr/article/25034603#home
[8] https://www.boston.com/news/crime/2020/01/31/former-boston-university-student-wanted-by-the-fbi-for-alleged-counterintelligence/
[9] https://www.yna.co.kr/view/AKR20211224039900501
[10] https://news.yahoo.co.jp/articles/215f9b2b5b940d99cb55e953d6a579ff7a3b7bff?page=1
[11] news.kmib.co.kr/article/view.asp?arcid=0015975266&code=61131611&sid1
[12] https://www.theepochtimes.com/mkt_app/325-australian-based-scientists-researchers-identified-as-recruits-for-beijing_3665336.html
[13] https://www.news1.kr/articles/?4415521
[14] N. Yu, Y, Choi, “A Study on GUI Design of Learning Applications for Young Children,” The Journal of Digital Contents Society, vol. 23, no. 3, pp.389-397, 2022.

저자소개

김영권(Youngkwon Kim)

1995 년 3 월~현재 오산대학교 컴퓨터소프트웨어과 교수

관심분야 : 인공지능, 기계학습, 보안

장항배(Hangbae Chang)

2014 년 3 월~현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 융합보안, 연구보안