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

The Journal of Society for e-Business Studies
Vol.25, No.3, August 2020, pp.109-130
https://doi.org/10.7838/jsebs.2020.25.3.109

조직의 연구보안 수준평가 모형 연구

Research on the Level Evaluation Model of the Organization Research Security

나원철(Onechul Na)*, 장항배(Hangbae Chang)**

초 록

최근 기술의 혁신을 위한 연구개발의 중요성이 커지고 있다. 연구개발의 급속한 발전은 다양한 긍정적 효과가 있지만, 동시에 정보 및 기술에 대한 유출 범죄를 가속화시키는 부정적 영향 또한 존재한다. 본 연구에서는 점차 심각해지는 연구개발 결과물 유출 사고를 대비하기 위해 조직 차원에서 이루어지는 연구개발 환경을 안전하게 보호할 수 있는 연구보안 수준측정 모형을 개발하였다. 먼저 국내외 연구개발 관련 보안정책들을 분석하고 종합하여, 연구보안 수준평가 항목 10개(연구보안 추진체계, 연구시설과 장비 보안, 전자정보 보안, 주요 연구정보 관리, 연구노트 관리, 지식재산권/특허 관리, 기술사업화 관리, 내부연구원 관리, 인가된 제3자 관리, 외부자 관리)를 전문가 인터뷰를 통해 도출하였다. 다음으로, 도출한 연구보안 수준평가 항목을 조직의 연구개발 환경에 다차원적 관점에서 적용 가능하도록 연구보안 수준평가 모형을 설계하였다. 마지막으로 모형에 대한 타당성을 검증하고, 실제 연구개발을 수행하는 조직을 대상으로 시범 적용하여 연구보안 수준을 평가해보았다. 본 연구에서 개발한 연구보안 수준평가 모형은 실제 연구개발을 수행하고 있는 조직 및 프로젝트의 보안 수준을 적절하게 측정하는 데 유용하게 활용될 수 있을 것으로 기대되고, 연구개발을 직접 수행하는 연구원들이 자체적으로 연구보안 체계를 수립하고 보안관리 대책을 마련하는 데 도움이 될 것이라 판단된다. 또한 연구개발을 수행하는 조직 차원의 보안성 향상뿐만 아니라 프로젝트 단위의 연구개발을 안전하게 수행함으로써, 연구개발 투자에 대한 안정적이고 효과적인 성과를 낼 수 있을 것이라 기대한다.

ABSTRACT

Recently, the importance of research and development for technological innovation is increasing. The rapid development of research and development has a number of positive effects, but at the same time there are also negative effects that accelerate crimes of information and technology leakage. In this study, a research security level measurement model was developed that can safely protect the R&D environment conducted at the organizational level in order to prepare for the increasingly serious R&D result leakage accident. First, by analyzing and synthesizing security policies related to domestic and overseas R&D, 10

이 논문은 2020년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0008703, 2020년 산업혁신인재성장지원사업).

* First Author, Ph.D. Post Doctor, Department of Security Convergence, Chung-Ang University (nastop@cau.ac.kr)

** Corresponding Author, Professor, Department of Industrial Security, Chung-Ang University (hbchang@cau.ac.kr)

Received: 2020-08-10, Review completed: 2020-08-25, Accepted: 2020-08-27

research security level evaluation items (Research Security Promotion System, Research Facility and Equipment Security, Electronic Information Security, Major Research Information Security Management, Research Note Security Management, Patent/Intellectual Property Security Management, Technology Commercialization Security Management, Internal Researcher Security Management, Authorized Third Party Researcher Security Management, External Researcher Security Management) were derived through expert interviews. Next, the research security level evaluation model was designed so that the derived research security level evaluation items can be applied to the organization's research and development environment from a multidimensional perspective. Finally, the validity of the model was verified, and the level of research security was evaluated by applying a pilot target to the organizations that actually conduct R&D. The research security level evaluation model developed in this study is expected to be useful for appropriately measuring the security level of organizations and projects that are actually conducting R&D. It is believed that it will be helpful in establishing a research security system and preparing security management measures. In addition, it is expected that stable and effective results of R&D investments can be achieved by safely carrying out R&D at the project level as well as improving the security of the organization performing R&D.

키워드 : 연구개발, 유출 사고, 연구보안, 보안 수준평가
R&D, Leakage Accident, Research Security, Security Level Evaluation

1. 서 론

최근 4차 산업혁명에 따라 기술혁신의 최전선에서 새로운 시대를 열어가기 위해 연구개발의 중요성이 커지고 있다[60]. 공공 및 민간 영역을 포함한 조직 차원에서 경쟁력을 강화하고 부가가치를 창출하기 위해 연구개발 투자에 막대한 비용을 투자하고 있다[56]. 또한 개방형 연구개발 환경으로의 변화와 디지털화로 인한 연구개발 관리체계의 변화는 기존 연구개발 패러다임을 바꾸고 있다[27]. 한국에서도 정보통신기술(ICT) 산업을 비롯한 다양한 산업분야에 연구개발 투자를 집중하고 있으며, 2018년 기준 총생산금액(GDP) 대비 연구개발 투자비율은 4.81%로 세계 1위권으로 평가되었으며, 연구개발 규모는 약 85조 7,000억 원으로 세계 5위권에 이르렀다[53].

이러한 막대한 연구개발 투자는 신산업 육성, 핵심기술 역량 강화 등의 긍정적인 결과를 보이기도 하지만[14], 이와 동시에 가치 있는 정보 및 기술에 대한 경쟁기업의 유출 범죄가 가속화되는 등의 부정적 영향이 존재한다[48]. 특히 최근 대학 및 기업의 연구소에서 연구개발 수행을 통해 산출된 정보 및 기술(이하 연구개발 결과물)이 유출되는 보안사고가 빈번하게 발생하고 있다[17]. Korean National Police Agency[24]의 자료에 따르면 2019년 4월부터 10월까지 7개월간 기계, 정밀화학, 전기전자, 생명공학 등의 산업현장에서 90건의 연구개발 결과물 유출 사고를 적발하였고, 관련 사범 310명이 검거되었다. 특히 2012년부터 2018년까지 국가핵심기술의 유출 건수는 21건이나 집계되어[15], 국가 차원에서 신속하게 대응해야 하는 상황에 이르렀다. 국가핵심기술이란, 세계 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아 해외로 유출될 경우 국가의 안전

보장 및 국민 경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로서 법에 의해 지정된 산업기술을 말한다[40]. 연구개발 결과물 유출 사고에서 주목할 점은 대부분의 사고가 중소기업에서 발생한다는 점이다[33]. 이는 보안 환경이 안전하게 구축되어 있는 대기업과는 달리, 중소기업은 보안에 대한 활동 및 의식 수준이 상대적으로 부족함을 알 수 있다[7].

이렇듯 점차 심각해지는 연구개발 결과물 유출 사고에 대한 명확한 개념과 전체적인 특징을 파악하기 위해 과거 발생했던 연구개발 결과물 유출 사고 사례[42]를 면밀히 분석하였다.

상기 3개의 연구개발 결과물 유출 사고 사례들은 전체 20여 개의 사례의 세부내용들을 개

사례 1: 바이오기술 유출사건(2010)

- P사에 근무하는 S씨는 동료 C씨와 함께 새로운 동종회사 설립을 목적으로 첨단바이오 기술의 핵심자료를 유출 시도함
- 이들은 P사를 퇴사하면서 핵심기술 자료(연구개발 산출물, 실험 데이터, 연구노트 등)를 이메일과 USB를 이용하여 유출하였고, 유출한 핵심기술 자료를 가지고 특허를 출원해 원천기술로 인정받으려고 하는 도중 구속기소 됨
- 유출하려고 했던 바이오기술인 약물전달시스템은 동물 실험과정에서 암 치료에 효능이 탁월한 것으로 나타났고, 만약 상용화가 되었다면 최대 2조 원의 가치가 있을 것이라고 추정되었음

사례 2: 태양전지 생산장비 제조기술 중국 유출기도 사건(2012)

- J사는 총 2,700억 원의 연구개발비가 투입된 태양전지 생산장비 제조기술을 보유하고 있었음
- J사의 임원 K씨는 보안감시가 상대적으로 소홀한 심야시간이나 휴일에 집중적으로 태양전지 생산장비 제조기술 관련 파일의 암호를 해제한 후, 이를 외장하드에 복사하는 방법으로 외부로 반출하였음
- 그 후 K씨는 중국의 H그룹을 포섭하여 태양전지 생산장비를 제작하여 중국에서 판매하기로 하였으며, 그 대가로 H그룹에 태양전지 생산장비 제조기술을 이전해 주기로 했지만, 제작하는 도중 구속 기소됨
- 해당 기술이 유출되었을 경우, 약 6조 원의 손실을 입을 수 있을 것이라고 보도된 바 있음

사례 3: 유조선 핵심기술 유출사건(2013)

- 선박 부품 제조업체 A사의 대표이사 K씨는 정부출연금이 투입된 국책과제로 수행하고 있는 고속밸브 제조 기술을 빼돌려 동종업체를 세운 뒤, 자신이 발명한 것으로 3개의 특허를 출원하였음
- K씨는 A사에 근무하던 기술연구소장 C씨 등 2명을 자신이 세운 회사에 이직시킨 뒤, 밸브 설계도면과 생산기술 자료, 연구 개발자료 등 5천3백여 개의 핵심기술 관련 자료를 유출하여 부정하게 사용하였음
- 이에 K씨 등 3명을 「부정경쟁 방지 및 영업비밀 보호에 관한 법률」 위반 혐의로 불구속 입건하였음

략적으로 포함할 수 있는 대표 사례이다. 사례를 통해 주목해야 될 특징은 3가지로 요약할 수 있다. 먼저 “연구원”이다. 연구원은 직접 연구개발을 수행하는 연구원, 외국인 연구원, 퇴직자, 용역업체 연구원 등을 포함한다[21]. 연구개발 결과물을 유출하는 범죄자들은 대부분 연구개발 수행에 직접적으로 관련된 사람이었다[29]. 따라서 연구개발을 수행하는 연구원 및 관련자들에 대한 중점적인 보안관리 대책이 필요하다. 다음은 “결과물”이다. 결과물은 연구개발을 통해 마지막으로 산출된 연구개발 결과물뿐만 아니라, 연구개발 수행과정 중에 발생하는 가치 있는 정보 및 산출물들을 모두 포함한다[49]. 연구개발 수행과정 중 발생하는 수많은 정보 및 산출물들의 중요도는 결과물과 비교하여 우열을 가릴 수 없을 뿐만 아니라, 모두 긴밀하게 연결되는 통합적인 종합적 자산으로도 볼 수 있다[61]. 따라서 연구개발 결과물의 안전한 보호를 위해서는 연구개발 수행과정 중 산출되는 모든 것을 대상으로 한 보안관리 대책이 필요하다. 마지막으로 “연구 환경”이다. 연구 환경은 연구개발을 수행하는 물리적 공간(사무실, 장비 등)인 “연구시설 환경”과 연구개발 수행을 위한 사이버 공간(시스템, 데이터, 네트워크 등)인 “연구IT 환경”으로 구성할 수 있다[57]. 4차 산업혁명에 따른 정보통신기술 발전에 따라 연구개발 결과물 유출 범죄자들이 사이버 공간을 통한 공격을 주로 사용할 것으로 예상되지만, 실제로는 물리적 공간을 통한 유출이 더욱 빈번하게 발생하고 있다[45]. 따라서 연구개발을 수행하는 조직에서는 물리적 공간과 사이버 공간을 동시에 안전하게 보호할 수 있는 보안관리 대책을 강구해야 한다.

본 연구에서는 연구개발 결과물 유출 사고를 선제적으로 방지할 수 있도록, 조직 차원에서 이루어지는 연구개발 수행 환경에 대한 보안관리 수준을 평가할 수 있는 모형을 설계하고 검증하고자 하였다.

2. 선행연구

2.1 연구개발 보안

연구개발 수행 환경에 대한 보안관리 수준을 평가하기 위해서는 연구개발 보안이 무엇인지에 대한 개념 이해가 필요하다. 한국에서는 연구개발 수행 환경을 보안관리 하는 활동 및 대책을 연구개발 보안(이하 연구보안)이라 총칭한다[22].

먼저 사전적 정의를 기반으로 연구보안이란, 과학적인 방법을 통해 세계에 대한 지식을 체계적, 구체적, 논리적인 방법으로 얻고자 하는 탐구과정을 뜻하는 “연구”와 인가를 받지 않은 접근, 변경 또는 파괴 등으로부터 자료를 보호하기 위해 취해진 조치를 뜻하는 “보안”의 합성어이다[44]. 정리하면 연구자가 탐구한 내용을 보호하는 조치로 해석할 수 있다.

연구보안에 대한 개념은 대부분 법령을 기반으로 규명하고 있다. Ministry of Trade, Industry and Energy[40]에서는 산업기술과 관련된 국가연구개발 사업을 수행하는 과정에서 개발성과물이 외부로 유출되지 아니하도록 필요한 대책을 수립・시행하는 것으로 정의하고 있다. Ministry of Science and ICT[38]에서는 연구보안을 연구개발과제를 수행하는 과정에서 주요 정보 및 연구개발 결과 등이 무단으로 유출되지 아니하도록 취하는 조치라고 말하고 있다.

또한 다양한 문헌에서도 연구보안에 대한 개념을 정의하고 있다. The Korean Association for Research of Industrial Security[52]에서는 정부의 지원을 받아 국가연구개발 사업을 수행하는 기관에서 연구내용 및 연구결과물이 외부로 유출되지 않도록 관리하는 제반업무라고 정의하고 있다. Korea Institute of Human Resources Development in Science and Technology[22]에서는 연구를 수행하는 자가 연구의 준비 단계부터 연구의 수행과정 및 연구 종료 이후 발생한 주요 연구정보 및 연구성과물이 무단으로 유출되지 않도록 방지하기 위한 제반활동으로 정의하고 있다. Kim[18]은 국가연구개발 사업에서 발생하는 성과물이 산업기술 등으로 지정・보호되기 이전에 주어지는 잠정적 보호라고 정의하고 있다. Kang[12]은 정부의 지원을 받아 국가연구개발 사업을 수행할 때 발생하는 유・무형적 연구성과물, 기술이나 경영상 필요한 정보 및 지식재산을 각종 침해행위로부터 안전하게 보호·관리하기 위한 소극적 또는 적극적인 대책과 활동을 의미한다고 하였다.

상기 연구보안 개념에 따르면, 연구보안의 적용 범위를 연구개발을 수행하는 조직(연구소, 연구기관, 기업 등) 차원으로 설정해야 하는지 연구개발 프로젝트(과제, 사업 등) 단위로 설정해야 하는지 애매한 부분이 있다. 상기 연구개발 결과물 유출 사고 사례 분석결과에 따르면 “연구 환경” 측면에서는 연구보안을 연구개발 프로젝트 단위보다는 조직 차원으로 적용하는 것이 바람직하다. 왜냐하면 조직에서는 다양한 연구개발 프로젝트 동시다발적으로 수행되는데 각각의 연구개발 프로젝트마다 “연구환경”을 따로 구축하는 것은 많은 비용・인력・시간이 소모되기 때문이다. 따라서 “연구환경” 측면에서 연구보안을 적용하기 위해서는 연구개발 프로젝트 단위가 아닌 조직 차원에서 통합적으로 구축해야 한다고 판단된다. 반면 “연구원”과 “결과물” 측면에서는 연구보안을 연구개발 프로젝트 단위로 적용하는 것이 바람직하다. 왜냐하면 연구개발 프로젝트를 직접 수행하는 “연구원”과 연구개발 프로젝트 별로 산출되는 “결과물”은 조직 차원보다는 프로젝트 단위에서 보다 집중적이고 신속하게 대처가 가능하기 때문이다.

이에 따라 본 연구에서는 조직에서의 연구보안 적용 범위를 기본적으로 연구개발 프로젝트 단위로 한정하고, “연구 환경” 측면에서는 예외적으로 조직 차원으로 확대하여 적용하고자 한다.

2.2 연구개발 수행과정

한국에서는 과학기술개발 분야의 효율적인 관리 및 성과창출을 위하여 연구개발 수행과정에 대한 연구를 지속적으로 진행해왔다[10]. 일반적으로 연구개발 프로젝트가 목적하는 바를 생애주기 관점으로 파악하고자 하였으며, 아이디어 발견-연구 지원-실험-결과 배포의 4단계로 구분하였다[26].

Kwon et al.[25]의 연구에서는 연구개발 환경에서 연구자들의 연구 활동을 근본적으로 지원할 수 있는 정보서비스 구축을 위해, 연구개발 수행과정을 심층적으로 조사하였다. 그리고 연구개발 생애주기를 아이디어 생성 및 개발-연구비 확보-실험 및 분석-성과 창출-평가의 5단계로 나타내었다. Bae et al.[2]의 연구에서는 기존 연구보안 수준 평가에 대한 문제점을 제기하고, 연구자의 자율적인 연구보안 평가체계를 수립할 수 있도록 연구개발 수행과정을 새로운 관점

에서 탐구하고 다차원적인 연구보안 평가모델을 제시하였다. 또한 연구개발 수행과정에서 연구보안을 적용하는 수준 평가 지표의 시점을 구분하기 힘들다는 문제점을 지적하고, 이를 해결하기 위해 수준 평가의 영역을 연구 기획-연구 협약-연구 관리-연구 성과의 4단계로 분류하였다. Korea Institute of Human Resources Development in Science and Technology[22]에서는 과학기술 연구개발 현장실태와 개선방향을 연구개발 생애주기 관점에서 제시하고 있다. 또한 연구개발 수행현장에서 연구자 및 보안 관리자가 반드시 습득해야 하는 지식과 고려해야 할 사항 등의 내용을 포함하고 있다. 그리고 연구개발 수행단계를 연구 기획-연구 추진계획 수립-연구 수행-연구 성과 활용의 4단계로 나누었고, 각 단계별로 연구보안 조치사항에 대해 설명하였다.

상기 연구개발 수행과정에 대한 선행연구를 종합 분석하면, 먼저 연구개발 준비 단계에서는 연구개발에서 추진하고자 하는 목적과 업무를 정의하고 구체화하여 문서화한다. 다음으로 연구개발 계획을 수립하고 연구개발 수행을 위한 연구원의 역할과 책임을 정의한다. 연구개발 수행 단계에서는 연구개발 계획을 바탕으로 실제로 연구개발을 수행하는 단계이다. 연구의 신뢰성과 효율성을 향상시키기 위해 연구노트 등의 문서작업을 병행한다. 또한 연구자가 일정 시기마다 주기적으로 중간 검토를 실시하고 산출물 등을 확인하여 연구의 방향성을 잃지 않도록 점검한다. 마지막으로 연구개발 완료 단계에서는 최종 연구개발 보고서를 작성하고 객관적 평가를 통해 연구개발을 종료한다. 또한 최종 산출된 연구개발 결과물의 상태를 안전하게 보존하고, 문제가 발생했을 때 즉시 대처할 수 있도록 운영한다. 필요에 따라 연구개발 결과물에 대한 권리를 확보할 수 있는 지식재산권 등록 또는 기술이전 계약 등의 보안 대책을 마련한다.

본 연구에서는 상기 분석 내용을 연구보안 관점에서 재해석하여, 연구개발 수행과정을 크게 연구 준비-연구 수행-연구 결과의 3단계로 구분하였다.

2.3 연구개발 환경 변화

Huh[9]의 연구에서는 지식창출의 원천이 다양해지고 연구 인력의 유동성이 확대되면서, 자체 연구개발을 통한 기술 확보 전략의 효과성에 한계점을 제시하였다. 또한 이러한 한계점을 극복하기 위해 개방형 연구개발이 새로운 기술 확보 전략으로 주목받고 있음을 설명하였다. 개방형 연구개발은 개방형 혁신이라는 패러다임에서부터 형성되었다[35]. 개방형 혁신은 기업이 연구, 개발, 상업화에 이르는 일련의 과정을 개방하고 외부자원을 활용함으로써, 비용을 줄이고 부가가치 창출을 극대화하는 방법론을 말한다[1]. 이러한 패러다임은 기업 활동에만 국한 되는 것이 아니라 개발자원 및 연구시간을 절감할 수 있는 장점에 따라, 연구개발 활동으로 적용 및 확산되었다[18]. 이에 따라 개방형 혁신 패러다임의 도입을 통한 개방형 연구개발 환경에 대한 조성이 활발히 이루어지고 관련 연구도 수행되고 있다[58].

일반적으로, 연구개발 프로젝트 수행 중에 발생하는 다양한 산출물들과 연구개발 프로젝트 수행 종료 후 생산되는 최종 연구개발 결과물은 연구개발이 종료된 후 지식재산 정리 과정(공개 과정)에서 유출되는 경우가 많다[30]. 향후 선도적인 연구개발 체제로의 전환(개방형

혁신)으로 인하여 공개는 더욱 활발해질 것으로 예상된다. 또한 연구개발 환경의 대형화, 장기화는 산업계, 학계, 연구계의 협업(공동, 위탁)연구 혹은 국제 협업연구로 이어지고, 이는 제 3자에 의한 기술 유출 위험이 증가하는 원인이 되고 있다[59]. 이에 따라 연구개발 참여 연구자를 중심으로 한 새로운 체제의 보안관리 대책이 요구되고 있다[31]. 연구개발 수행을 위한 준비 과정부터 사업화에 이르는 종료 단계까지, 연구개발 수행 전 과정을 대상으로 보안관리 방안을 마련해야 한다. 추가적으로 연구개발을 직접 수행하는 연구원뿐만 아니라, 연구개발 수행과 관련되어 있는 모든 인력들을 포함하는 연구개발 수행 조직 전체를 대상으로 보안관리 대책을 마련해야 한다.

2.4 연구보안 정책

현재 공공 및 민간의 연구개발 활동 보호를 위해 이루어지고 있는 연구보안 정책들은 관련 법령들에 근거하여 적용되고 있다. 하지만 연구보안 정책에 대한 다양한 문제점이 존재하고 있으며, 특히 연구보안에 대한 투자 및 관심이 부족한 상황이다. Society for e-Business Studies[51]에서는 이러한 문제점을 보다 명확히 파악하기 위해 국가연구개발 보안 관리자들을 대상으로 인터뷰를 실시하였다. 인터뷰 결과 법령에서 명시하는 연구보안 정책이 필요 이상의 방대한 양으로 구성이 되어있음을 알 수 있었다. Ministry of Science, ICT and Future Planning[39]에서 제공하는 연구보안 정책의 세부 매뉴얼은 일반 민간기업에서 활용하고 있는 보안 관리항목들보다 상대적으로 많은 항목들을 제공하고 있었다. 이는 연구개발을 실질적으로 수행하는 연구자 및 보안 관리자에게 보안활동에 대한 애매한 기준을 제시하여 혼란을 가중시킬 뿐만 아니라, 연구개발 수행에 부담을 가중시키는 등의 다양한 문제를 야기하고 있다. 따라서 본 연구에서는 기존 연구보안 정책을 축소시키는 방안과 함께 조직 차원에서 연구개발을 수행할 시 연구보안 수준을 객관적으로 측정 가능한 모형을 통합적으로 고려하여 개발하기 위해 선행적으로 국내외에서 시행되고 있는 다양한 연구보안 정책들을 종합하고 분석하여 새로운 연구보안 수준평가 항목들을 도출하고자 하였다.

한국에서는 국가 차원에서 지원 및 관리하는 연구개발을 대상으로 안전한 연구개발 환경을 구축하기 위해 법제도로써 “Manual of Security Management on National Research Development Project”를 마련하였다[39]. 해당 매뉴얼은 연구개발 활동을 수행함에 있어 필수적으로 요구되는 보안관리 대책을 체계적으로 마련할 수 있도록 개발되었다. 보안관리 대책의 영역을 크게 보안관리 체계, 참여연구원 관리, 연구개발 결과 및 내용의 관리, 연구시설 관리, 정보통신망 관리의 5개로 구분하였으며, 각 영역 별로 세부적인 보안관리 조치사항에 대해 제시하였다.

민간 차원에서는 주로 Korea Internet & Security Agency[23]에서 제공하는 “정보보호 관리체계”를 활용하여 연구보안 규정을 수립한다. 해당 체계는 다양한 민간 조직에서의 주요 정보자산을 효과적으로 보호하기 위한 규정으로써, 연구보안 관점에서도 필수적으로 요구되는 보안관리 대책을 포함한 종합적인 보안관리 체계라 볼 수 있다. 또한 보안 정책, 보안 조직, 외부자 보안, 정보자산 분류, 보안 교육, 인적 보안, 물리적 보안, 시스템 보안, 암호통제, 접근

통제, 운영보안, 침해사고 관리, IT재해복구의 13개 영역으로 보안관리 대책이 구분되어 있다.

SANS(SysAdmin, Audit, Network and Security) Institute[50]에서는 연구개발이 수행되는 연구실의 주요 인프라 시설 및 정보 자산을 보호하기 위해 “Lab Security Policy”를 수립하고 있다. 해당 정책은 SANS에서 자체적으로 활용할 뿐만 아니라, 타 연구기관에도 적용될 수 있도록 계속적인 업데이트와 배포를 진행하고 있다. 정책은 크게 일반적 요구사항, 내부 연구실 보안 요구사항, 정책 컴플라이언스의 3개 영역으로 구분되고 있으며, 세부적으로 28개의 보안관리 조치사항을 제시하고 있다.

캐나다 Saskatchewan 주[8]에서는 연구개발 프로젝트 수행에서의 연구보안 활동에 대한 준수 여부를 평가하기 위해 “Security Compliance Assessment Checklist”를 마련하여 활용하고 있다. 해당 체크리스트의 주된 목적은 연구개발 프로젝트를 수행하는 조직과 보안 관리자의 연구보안 준수 여부를 보장하기 위함이다. 체크리스트는 크게 Organizing Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Information Security Incident Management, Business Continuity Management, Compliance의 10개의 영역과 36개의 세부 보안관리 조치항목으로 구성되어 있다.

다국적 산업보안 워킹 그룹(The Multinational Industrial Security Working Group, MISWG)[41]에서는 다국적 협동 프로젝트에서의 “Project Security Instruction”을 제공하고 있다. 이는 연구개발 프로젝트 수행 시 산출되는 정보와 자산이 정상적으로 보호되도록 지원하는 데 목적이 있다. 보안 조치사항은 크게 보안지침, 정보공개, 방문자 관리, 하도급업체 관리, 시설 관리, 보안교육 및 인식제고의 6개 영역으로 구성되어 있다.

핀란드 정부[43]에서 제작하고 배포한 “Industrial Security Manual”에서는 국제 수준의 연구개발 프로젝트에 참여하는 조직을 위한 연구보안 지침을 담고 있다. 국제 수준의 연구개발 프로젝트란 다른 국가 또는 외국 기관에서 연구개발 관련 정보에 대한 접근이 필요할 수도 있는 프로젝트를 의미한다. 해당 매뉴얼에서는 연구개발 프로젝트의 보안을 위한 요구사항들을 정리하고, 연구개발 참여 인력 및 보안 관리자에게 실질적으로 도움이 될 수 있는 내용을 제공하고 있다. 세부적으로 보안 관리, 개인 보안, 물리 보안, 기술정보 보안의 4개 영역으로 구성되어 있다.

상기 6개의 선행연구를 통해 조직의 연구보안 수준평가를 위한 항목 후보군을 도출하였다. 각 정책에서 제공하는 주요 보안관리 대책을 추출하고 정책 별로 통합하여 <Table 1>과 같이 최종 40개의 항목 후보군을 도출하였다.

〈Table 1〉 Comparison of Domestic and Foreign Research Security Policies

	Research Security Level Evaluation Item Candidate	[1]	[2]	[3]	[4]	[5]	[6]
1	Self Security Management Regulations	○	○	○	○	○	○
2	Operation of the Research Security Council	○	○				
3	Security Administrator Designation	○	○	○	○		○

〈Table 1〉 Comparison of Domestic and Foreign Research Security Policies(Continued)

	Research Security Level Evaluation Item Candidate	[1]	[2]	[3]	[4]	[5]	[6]
4	Security Education	○	○		○	○	○
5	Reward and Punishment Measures	○	○				
6	Response to Security Incident Infringement	○	○		○	○	○
7	Regular/Frequent Security Check	○	○		○		
8	Disaster Prevention Measures	○	○		○		○
9	Joint Research Mmanagement	○	○		○	○	○
10	Identification of Responsibility for Information Protection		○	○	○		○
11	Information Asset Identification		○	○	○	○	○
12	Structure of Research Security Governance System		○		○		
13	Recruitment Management	○	○		○		○
14	Retirement Management	○	○				
15	Temporary Visitor Management	○		○	○	○	○
16	Management of Suspected Leakage	○					
17	Researcher Overseas Business Trip Management	○			○	○	
18	Foreign Researcher Management	○			○		○
19	Document Security Level Indication	○	○		○	○	○
20	Patent/Intellectual Property Rights	○	○		○		
21	Management in Case of Public Disclosure	○	○		○	○	○
22	Technology Transfer/Commercialization	○			○	○	
23	Third Party Technology License Prohibition Agreement	○					○
24	Research Equipment Control	○	○	○	○	○	○
25	Management of Major Facilities	○	○		○	○	○
26	Separate Management of Protected Areas	○	○		○		
27	Control of Access to Research Facilities	○	○	○	○	○	
28	Intrusion detection System Management	○	○	○	○	○	○
29	User Authentication	○	○		○		○
30	Information Asset Management	○	○	○	○	○	○
31	Wireless LAN Security	○	○		○		
32	Portable Storage Media Management	○	○		○		
33	Data Backup Management	○	○		○	○	
34	PC Management	○	○	○	○		
35	Log Management	○	○		○		○
36	Information System Access Control	○	○	○	○	○	○
37	Network Data Management	○	○	○	○		
38	Computer Equipment Disposal Management	○	○		○	○	○
39	Whether to Implement Internal Network	○	○		○		
40	Email Management	○	○	○	○		

[1] Manual of security management on national research development project
[2] Information Security Management System
[3] Lab Security Policy
[4] Security Compliance Assessment Checklist
[5] Project Security Instruction
[6] Industrial Security Manual

3. 연구보안 수준평가 모형 개발

3.1 연구보안 수준평가 항목

연구보안 수준평가 후보군 항목들 중 조직 차원에서 이루어지는 연구개발 수행 환경에 대한 보안관리 수준을 평가하기에 적합한 항목을 보다 세부적으로 추려내기 위해, 다음의 사항들을 고려하여 연구를 진행하였다. 첫째, 연구개발을 수행하는 연구원이 직접적으로 관리할 수 있도록 연구자 중심 보안관리 대책을 마련해야 한다. 둘째, 연구개발 수행을 통해 최종적으로 산출되는 연구개발 결과물의 보호(Object) 뿐만 아니라, 연구개발 수행 도중 산출되는 모든 연구개발 결과물을 보호(Process)할 수 있는 보안관리 대책을 마련해야 한다. 셋째, 안전한 연구개발 수행 환경의 구축을 위해 연구시설 환경과 연구IT 환경을 통합하여 균형적인 관점에서 접근해야 한다. 넷째, 연구보안의 적용범위를 연구개발 프로젝트 단위로 하되, 연구 환경은 조직 차원에서 고려해야 한다. 다섯째, 연구개발 수행 환경 변화에 유연하게 대응할 수 있도록, 연구개발 수행 주체뿐만 아니라 연구개발 수행을 보조하는 협력 조직을 포함하여 보안관리 대책을 수립하고, 기존 연구보안 정책에 비해 보다 간략화하여 연구자들이 간편하게 운용할 수 있는 보안관리 대책을 마련해야 한다.

또한 연구보안 수준평가 항목을 보다 객관적인 관점에서 도출할 수 있는 학계 및 산업계의 연구보안 전문가를 대상으로 포커스 그룹 인터뷰(FGI)를 실시하여 연구보안 수준평가 항목 선정에 대한 신뢰성을 높이고자 하였다[4]. FGI의 구성은 위해 연구개발 수행에 대한 경험이 풍부하고, 보안에 대한 이해가 깊은 공공기관 및 민간기업의 보안 담당자, 대학의 보안 전공 교수를 대상으로 하였다. 사전에 특정 공간 대여하여 인터뷰를 진행하였으며, 질문의 구성은 시작 질문(연구보안 수준평가), 핵심 질문(연구보안 수준평가 항목 도출), 마무리 질문(연구보안 수준평가 모형)으로 구성하였다[28]. 인터뷰 내용으로부터 정보를 추출하고, 추출한 정보를 가감 없이 분석하였다. 본 인터뷰로 연구보안 수준평가 항목에 대한 신빙성(Credibility), 적합성(Fitness), 감사성(Auditability), 확인 가능성(Confirmability)을 준거로 타당성을 확보하였다[46].

결과, 상기 도출한 연구보안 수준측정 항목 후보군들에 대해 5개 고려사항과 인터뷰 결과를 정리하여, <Table 2>와 같이 최종 연구보안 수준측정 항목 10개를 도출하고, 항목별 세부 보안관리 대책을 정리하였다.

〈Table 2〉 Research Security Level Evaluation Item and Detailed Security Management Measures

	Research Security Level Evaluation Item	Detailed Security Management Measures
1	Research Security Promotion System	• Self Security Management Regulations • Security Administrator Designation • Research Security Education
2	Research Facility and Equipment Security	• Management of Protected Areas • Control of Access to Research Facilities • Research Equipment Control

〈Table 2〉 Research Security Level Evaluation Item and Detailed Security Management Measures(Continued)

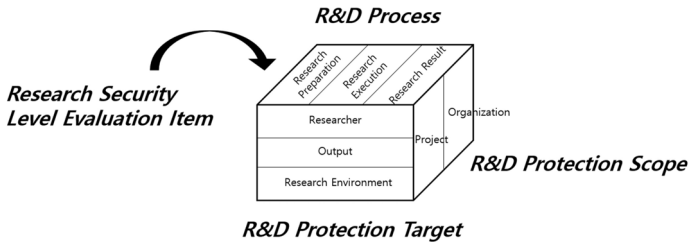
	Research Security Level Evaluation Item	Detailed Security Management Measures
3	Electronic Information Security	• PC Management • Network Security • User Authentication • Information System Access Control • Log Management
4	Major Research Information Security Management	• Information Assets Classification • Document Security Leveling • Research Output Management • Joint Research Output Management
5	Research Note Security Management	• Assignment of Rresearch Note Management Number • Designation of Research Note Storage Location • Granting Permission to Read Research Notes
6	Patent/Intellectual Property Security Management	• Patent/Intellectual Property Rights Security • Management in Case of Public Disclosure • Prepare Security measures for the Attribution of Joint Research Output
7	Technology Commercialization Security Management	• Security Management During Technology Transfer • Priority to Sign Contracts for Domestic Targets • 3rd Party Technology License Prohibition ASgreement Signed
8	Internal Researcher Security Management	• Recruitment Management • Retirement Management • Overseas Business Trip Management
9	Authorized Third Party Researcher Security Management	• Joint Researcher Management • Management of Commissioned Researchers
10	External Researcher Security Management	• Temporary Visitor Management • Regular Access and Dispatch Management

3.2 연구보안 수준평가 모형 설계

조직의 연구보안 수준을 객관적이고 다차원적으로 평가하기 위해 선행연구에서 분석한 연구개발의 개념, 수행과정, 환경, 정책을 기반으로 <Figure 1>과 같이 연구보안 수준평가 모형안을 설계하였다.

연구개발 수행과정에 따라 연구개발 환경에서의 보호해야 하는 대상과 보호하는 주체를 고려하여 모형을 구조화하고, 해당 모형에 상기 도출한 연구보안 수준평가 항목 10개를 적절히 적용하여 모형을 개발하고자 하였다.

세부적으로 연구개발 수행과정을 통해 연구개발 수행 단계별로 업무 및 보안 요구사항을 정의하고, 이에 따른 보안관리 대책을 마련함으로써, 연구개발 전 주기에 걸친 유기적이고 통합적인 연구보안을 적용할 수 있다. 연구개발 보호의 대상을 구분함에 따라 연구개발 수행에서 보호해야 할 대상별로 요구되는 보안관리 대책을 구성함으로써, 차별화된 위험요소를 인식하고 이를 근거로 위험 기반 보안관리 대책을 수립할 수 있다. 연구개발 보호의 범위를 고려함에 따라 연구보안을 실질적으로 적용하는 주체를 명확하게 구분하여 연구개발을 수행하는 연구원, 관련 보안 관리자, 조직 등의 주체별 보안관리 대책을 효율적으로 구성할 수 있다.



〈Figure 1〉 Research Security Level Evaluation Model Design

3.3 연구보안 수준평가 모형 검증

연구보안 수준평가 항목의 타당성을 검증하기 위해 설문조사를 통한 통계분석을 실시하였다. 설문조사의 대상자는 연구개발을 다수 수행한 경험이 있으면서 보안에 대한 전문적 지식을 갖고 있는 전문가를 대상으로 하였다[62]. 설문지 배포는 대면을 통한 오프라인 방식과, 메일을 통한 온라인 방식을 동시에 활용하였다. 조사 대상자 수는 40명이고 회수한 설문지 수는 38건이다. 조사 대상자 수인 표본크기에 대한 적절한 설정을 위해여 Park et al.[47]의 연구를 참고하여 본 연구와 유사한 연구에서 사용한 표본 크기를 적용하고자 하였다. 수에 대한 조사 대상자의 세부 정보는 정부출연기관 연구소 보안 관리자 11명, 대학교 보안 전공 교수 19명, 민간 기업 보안 책임자 8명으로 나타났다.

설문의 응답 척도는 5점 척도이며, 5점이 가장 바람직한 수준이고 1점이 가장 바람직하지 않은 수준으로 설정하였다[54]. 이들 타당성과 중요성에 대한 기초 통계량은 평균이 4.07로서 대부분의 항목에서 보통 이상으로 바람직하다고 응답되었다. Kim[19]의 연구를 참고하여 지표의 타당성 수준은 절대적 수준을 사용하여 판단하였고, 3.0을 기준으로 사용하였다. 분석결과 평균 3.0 이하인 항목은 나타나지 않았고 모두 타당한 것으로 도출되었다. 연구보안 수준 측정 보안수준 측정항목별 분석결과는 <Table 3>과 같다.

〈Table 3〉 Research Security Level Evaluation Item Feasibility Result

	Research Security Level Evaluation Item	Feasibility Result
1	Research Security Promotion System	4.36
2	Research Facility and Equipment Security	4.00
3	Electronic Information Security	4.18
4	Major Research Information Security Management	4.29
5	Research Note Security Management	4.11
6	Patent/Intellectual Property Security Management	3.57
7	Technology Commercialization Security Management	3.71
8	Internal Researcher Security Management	4.14
9	Authorized Third Party Researcher Security Management	4.11
10	External Researcher Security Management	4.18

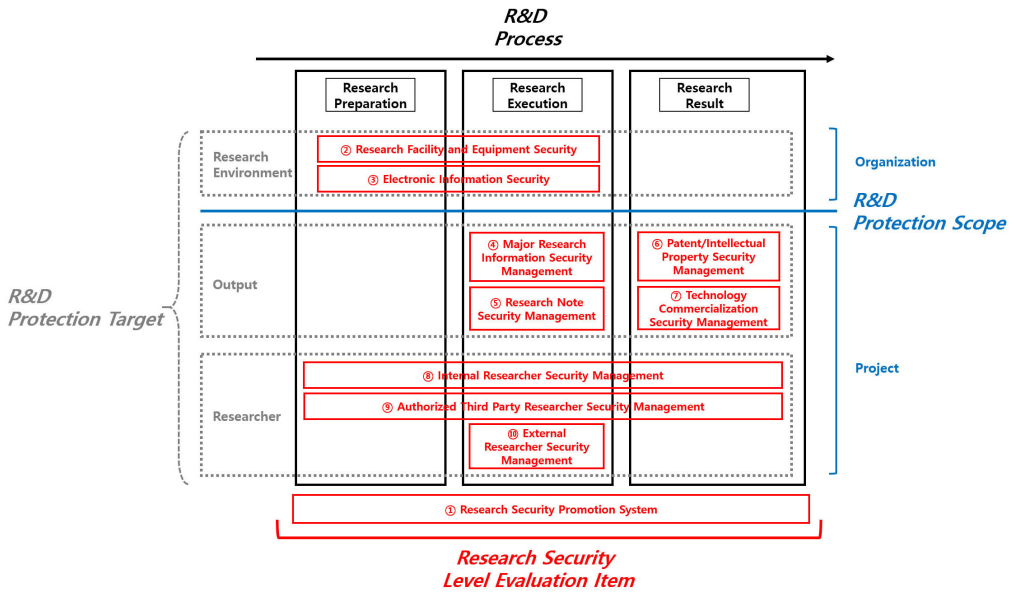
다음은 상기 설계한 연구보안 수준측정 항목들의 구조적 타당성을 검증하기 위해 요인분석을 실시하였다[6]. 요인분석을 통하여 관측된 변수들의 내재된 요인들이 어떻게 연결되었는지를 탐색하여 요인들 간 구조를 파악하고자 하였다[37]. 이를 통해 도출된 요인들이 연구보안 수준평가 모형의 연구개발 보호 대상(연구환경, 성과물, 연구원)과 일치하는지 파악하고, 이를 통해 모형 설계의 적절성과 타당성을 검증하고자 하였다. 연구보안 수준측정 항목에 대한 요인분석 결과는 <Table 4>와 같다.

요인분석 결과, 요소들의 응집도가 매우 높은 것으로 나타났다. 아이겐 값 1 이상에서의 3개 요인이 추출되었으며, 본 요인분석에서의 KMO 값은 0.679로 일반적인 기준치인 0.5 이상으로써, 요인분석의 의미가 크다고 할 수 있다[55]. 또한 Barett의 구형성 검정이 150.083, 유의도는 0.000으로 도출되어 요인분석의 사용이 적합하며, 합당한 공통요인이 존재한다고 결론지을 수 있다[11]. 요인의 신뢰도를 나타내는 크론바흐 알파 값은 모두 0.7 이상으로서 추출된 요인은 신뢰도가 높다고 할 수 있다[3]. 연구보안 수준평가 항목 중 “Research Security Promotion System”을 제외하고는 기 설계한 모형의 연구개발 보호대상인 연구 환경, 성과물, 연구원 별로 적절하게 응집하는 것을 확인할 수 있었다. 연구보안 추진체계의 경우는 연구개발 보호대상 전체를 대상으로 적용되는 것이기 때문에 영역별 군집이 되지 않은 것으로 판단된다. 마지막으로, 연구보안 수준평가 항목들을 기 설계한 모형의 연구개발 수행과정, 연구개발 보호 범위, 연구개발 보호 대상의 영역에 선행연구 분석 결과와 설문을 통한 통계분석 결과를 근거로 적용 및 배치하여, <Figure 2>와 같이 최종 연구보안 수준평가 모형을 개발하였다.

<Figure 2>의 연구보안 수준평가 모형은 연구개발 수행과정을 기반으로 수행 전부터 종료 후 까지 적용해야 할 연구보안 수준평가 항목을 도출하였다. 또한 연구개발을 수행하는 환경 측면에서 보호해야 할 범위에 따라 조직과 프로젝트를 구분하고자 하였다. 마지막으로 연구개발 수행에서 보호해야 하는 대상을 환경, 연구자, 결과물의 3가지로 설정하여 수준평가 측정의 효율성을 높이고자 하였다.

〈Table 4〉 Research Security Level Evaluation Item Factor Analysis Result

Factor	Research Security Level Evaluation Item	Factor Coefficient	Reliability Coefficient
Research Environment	Research Facility and Equipment Security	0.826	0.734
	Electronic Information Security	0.792	
Output	Major Research Information Security Management	0.816	0.828
	Research Note Security Management	0.815	
	Patent/Intellectual Property Security Management	0.849	
	Technology Commercialization Security Management	0.799	
Researcher	Internal Researcher Security Management	0.819	0.736
	Authorized Third Party Researcher Security Management	0.830	
	External Researcher Security Management	0.616	



〈Figure 2〉 Research Security Level Evaluation Model

본 연구에서 제안하는 연구보안 수준평가 모형은 기존 연구보안 체계와 달리 다음과 같은 특징과 차별성이 있다. 첫째 다양한 연구개발 결과물 유출 사고 사례를 분석하여 연구개발 보호의 대상을 “연구원”, “결과물”, “연구 환경”으로 구분함으로써, 연구개발 환경에 연구보안을 적용하는 데 있어 직접적으로 관련 있는 보호 대상을 명확하게 특정하여 연구보안 수준을 측정 가능하게 하였다. 둘째 연구개발 수행과정을 간략화하기 위해 관련 선행연구를 종합 분석하여 연구준비, 연구수행, 연구결과로 구분하였으며, 이를 통해 연구개발을 수행하는 연구자들이 직접적으로 연구보안 수준을 평가할 수 있는 시점을 제시하였다. 셋째 연구개발 보호의 범위를 “조직”과 “프로젝트”로 구분하여, 연구개발 수행 시 조직 차원에서 관리해야 할 보안관리 대책과 프로젝트 단위에서 조치해야 하는 보안관리 대책을 차별화함으로써, 연구개발을 직접 수행하는 연구원과 연구개발을 환경을 통합적으로 관리하는 조직 간 유연한 보안대책 수립이 가능하도록 설계하였다. 마지막으로 기존의 방대한 연구보안 정책과는 달리 국내외 다양한 정책들에 대한 분석 및 전문가 인터뷰와 설문을 통해 연구보안 수준측정 항목을 대폭 간략화하였으며, 이를 통해 연구개발 보안 관리자들이 연구보안 수준을 보다 간편하고 효율적으로 측정 가능하도록 모형을 제안하였다.

3.4 연구보안 수준평가 모형 시범 적용

연구보안 수준평가 모형을 실제 연구개발 수행 환경에 적용함으로써 모형의 실용성과 활용 가능성을 확인하고자 하였다. 현재 연구개발 프로젝트를 수행하고 있는 연구기관을 평가대상으로 선정하고, 연구개발 수행 전에 모형에 대한 설문을 적용하여 연구보안 수준평가를 진

〈Table 5〉 Research Security Level Evaluation Model Apply Result

	Research Security Level Evaluation Item	Score	
		“A” Institution Research Team	“B” Institution Research Team
1	Research Security Promotion System	Medium	Medium
2	Research Facility and Equipment Security	High	Low
3	Electronic Information Security	High	Medium
4	Major Research Information Security Management	High	Medium
5	Research Note Security Management	Low	Low
6	Patent/Intellectual Property Security Management	High	Medium
7	Technology Commercialization Security Management	Low	Low
8	Internal Researcher Security Management	High	High
9	Authorized Third Party Researcher Security Management	Medium	Low
10	External Researcher Security Management	Low	Low

행하였다. 해당 설문 방식은 자체 평가 방식으로써, 관련 선행연구로부터 점수화 방안을 참고하여 진행하였다[20]. 본 설문에서는 연구보안 수준측정 항목 별로 상, 중, 하 3단계로 구분하여 항목의 수행 정도를 파악하였다[5, 13, 20]. “상”은 해당 연구보안 수준측정 항목이 매우 타당하게 수행되었음을 나타내고, “중”은 부분적으로 수행되었음을 나타내며, “하”는 전혀 수행되지 않았음을 나타내고자 하였다[32, 34].

평가결과, 우선 전자정보 보안, 주요 연구정보 관리, 내부연구원 관리 항목에 대한 평가는 비교적 높게 나타났으며, 연구노트 관리, 기술사업화 관리, 인가된 제3자 관리, 외부자 관리 등의 항목은 낮게 평가되었다. 이는 연구개발을 직접 수행하는 조직 내 연구원에 대한 관리와 연구개발 수행 도중 발생할 수 있는 가치있는 정보에 대한 보안관리 대책을 철저히 준비하고 실행되었음을 알 수 있다. 하지만 최근 연구개발 환경 변화에 따른 공동연구나 협업 과정에서 나타나는 외부 인력에 대한 보안관리 대책이 매우 부족함을 알 수 있다. 이를 대비하기 위해서는 공동으로 연구개발을 수행할 시 보안관리 대책을 따로 마련하는 방안이 요구된다. 또한 연구개발이 종료된 후 발생하는 기술 및 결과물에 대한 연구보안 실태가 부족하였다.

4. 결 론

최근 연구개발 수행에 있어 보안에 대한 중요성이 커지고 있다. 하지만 지속적인 연구개발 결과물 유출 사고가 발생함에도 불구하고, 연구개발을 수행하는 연구원의 보안의식은 부족한 상태이며 실질적으로 활용 가능한 보안관리 대책도 마련되어 있지 않다. 따라서 본 연구에서는 연구개발 환경을 효과적으로 보호할 수 있도록 조직의 연구보안 수준을 평가할 수 있는 모형을 개발하고, 모형에 대한 타당성과 신뢰성을 검증하였다.

우선 연구개발 보안사고 사례 분석을 통해 연구보안 강화를 위한 고려사항(연구원, 결과물, 연구 환경)을 도출하였다. 다음으로 연구보

안의 개념에 대한 선행연구를 분석하여 연구보안이 적용되는 범위를 파악하고, 연구개발 수행과정을 분석을 통해 프로세스 관점의 연구보안에 대한 필요성을 제기하였다. 그리고 국내외 연구보안 정책 연구를 종합하여 비교분석 후 40개의 연구보안 수준평가 항목 후보군을 1차로 도출한 후, 연구보안 전문가를 대상으로 심층 인터뷰를 진행하여 최종 연구보안 수준평가 항목 10가지(연구보안 추진체계, 연구시설과 장비 보안, 전자정보 보안, 주요 연구정보 관리, 연구노트 관리, 지식재산권/특허 관리, 기술사업화 관리, 내부연구원 관리, 인가된 제3자 관리, 외부자 관리)를 도출하였다.

도출한 연구보안 수준평가 항목들을 실제 연구개발 환경에 적용 가능하도록 연구개발 수행과정, 연구개발 보호 대상, 연구개발 보호 범위를 고려하여 다차원적 구조의 연구보안 수준평가 모형을 개발하였다. 이에 대한 타당성 검증을 위해 보안 지식을 갖고 있으면서 가수의 연구개발 수행 경험이 있는 학계 및 연구계의 전문가들을 대상으로 설문조사를 실시하였다. 조사 결과, 본 연구에서 제시한 연구보안 수준평가 항목은 모두 바람직한 것으로 나타났다. 또한 각 항목이 영역별로 적절하게 묶여있는지에 대한 구조적 타당성을 검증하기 위해 요인분석을 실시하였다. 요인분석 결과, 본 연구에서 선제적으로 제시한 연구보안 강화를 위한 고려사항(연구원, 결과물, 연구 환경)에 적합한 형태로 3개의 요인으로 도출되었으며, 각 영역마다 높은 응집도를 나타내어 구조적 타당성도 적절함을 검증하였다. 이를 기반으로 최종 연구보안 수준평가 모형을 개발하였고, 실제 연구개발을 수행하고 있는 조직을 대상으로 시범 적용하여 파일럿 테스트를 진행하였다. 이를 통해 개발한 모형에 대한 실용성과 활용 가능성을 확인하였고, 조직의 연구보안 수준을 점수로 파악할 수 있었다.

본 연구에서 개발한 연구보안 수준평가 모형은 실제 연구개발을 수행하고 있는 조직에서 실질적으로 활용 가능하며, 프로젝트 단위에서도 유연하게 적용 가능하다고 판단된다. 또한 기업이나 기관을 포함한 다양한 조직 안에서 연구개발을 직접적으로 수행하는 연구원과 보안 관리자들이 자체적으로 연구보안 수준평가 체계를 수립하고 대책을 마련하는 데 실무적으로 도움이 될 것이라 판단된다. 그리고 기존 연구보안과 관련된 선행연구가 부족한 가운데, 본 연구에서 제시하는 연구보안 수준평가 모형은 기업, 대학, 공공기관 등의 연구개발 수행 시 보안 정책을 수립하는 데 참고할 수 있는 이론적 모형으로 활용될 것으로 기대된다. 마지막으로 연구개발을 수행하는 조직 전체의 보안성 향상뿐만 아니라 프로젝트 단위의 연구개발을 안전하게 수행 가능도록 함으로써, 조직의 경영상 목표를 달성하는 데 도움을 주고 연구개발 투자에 대한 안정적이고 효과적인 성과를 낼 수 있을 것이라 기대한다.

본 연구의 한계점으로는, 기존 연구보안 관련 선행연구가 극히 부족하여 국가 차원에서 제공하는 연구보안 컴플라이언스를 기반으로 연구보안 수준평가 항목을 설계하였기 때문에, 수준평가 항목의 적용 범위가 광범위하다는 문제점이 있다. 또한 모형의 시범 적용을 통한 모형의 수준평가 방법을 상, 중, 하의 3단계로 단순하게 구분하여 점수화함에 따라, 수준평가의 정밀성이 다소 감소할 수 있다고 판단된다. 향후 연구에서는, 연구보안 수준평가 항목 및 모형에 대한 계층화 분석(AHP)을 통해 가중치를

도출하여, 보다 정밀하고 실용성 높은 연구보안 수준평가 방안을 제시하고자 한다.

References

[1] Ahn, C. and Lee, Y., “An empirical analysis of the influence factors on open innovation activities in Korea,” Journal of Korea Technology Innovation Society, Vol. 14, No. 3, pp. 431-465, 2011.

[2] Bae, S. T. and Kim, J. H., “A study on development of the evaluation model about level of security in national R&D program,” The Journal of Korean Association of Computer Education, Vol. 16, No. 1, pp. 73-80, 2015.

[3] Bland, J. M. and Altman, D. G., “Statistics notes: Cronbach’s alpha,” Bmj, Vol. 314, No. 7080, p. 572, 1997.

[4] Brits, H. and du Plessis, L., “Application of focus group interviews for quality management: An action research project,” Systemic Practice and Action Research, Vol. 20, No. 2, pp. 117-126, 2007.

[5] Choi, S., Hwang, H. J., and Shin, H. K., “Research and development of achievement and assessment standards for school mathematics based on the 7th national curriculum,” Journal of Educational Research in Mathematics, Vol. 12, No. 1, pp. 145-162, 2002.

[6] Gim Chung, R. H., Kim, B. S., and Abreu, J. M., “Asian American multidimensional acculturation scale: Development, factor analysis, reliability, and validity,” Cultural Diversity and Ethnic Minority Psychology, Vol. 10, No. 1, pp. 66-80, 2004.

[7] Gong, B., “The situation and security measures of industrial technology security management of SMEs,” The Korean Society of Private Security, Vol. 18, No. 1, pp. 1-26, 2019.

[8] Government of Saskatchewan, Project Security Compliance Assessment Checklist, 2011.

[9] Huh, Y. D., “A study on the determinants of and relationship between technology import and R&D,” Korean Management Review, Vol. 25, No. 3, pp. 83-110, 1996.

[10] Hwang, K., “R&D accountability and dilemma within the Korean science and technology context,” Korean Public Administration Review, Vol. 50, No. 2, pp. 189-213, 2016.

[11] Kang, H., “A guide on the use of factor analysis in the assessment of construct validity,” J Korean Acad Nurs, Vol. 43, No. 5, pp. 587-594, 2013.

[12] Kang, S. J., Research Security Theory, Korean Studies Information, 2014.

[13] Kim, B. R., “Building evaluation structure for selecting contractor in local government’s contracting-out of welfare service,” Journal of Regional Studies, Vol. 14, No. 2, pp. 69-94, 2006.

[14] Kim, H. and Kim, B. K., “Analyzing the

effectiveness of public R&D subsidies on private R&D expenditure," Journal of Korea Technology Innovation Society, Vol. 15, No. 3, pp. 649-674, 2012.

[15] Kim, H. and Koo, N., "Prevention of divulgence and protection of national core technology," Journal of the Korean Society of Automotive Engineers, Vol. 42, No. 5, pp. 21-24, 2020.

[16] Kim, S., "A review on security management of government-sponsored R&D program," Korean Journal of Industry Security, Vol 1, No. 1, pp. 75-91, 2009.

[17] Kim, S., Park, J., and Park, G., "Research of dealing with Industrial technology disclosure crime," The Journal of Korean Association of Security and Safety, Vol. 9, No. 1, pp. 91-109, 2013.

[18] Kim, S., "Strategic implications of open innovation for the public sector," STEPI Insight, Vol. 28, pp. 1-28, 2009.

[19] Kim, Y., "Development of indicators for evaluating the web credibility by goodness-of-fit analysis," Journal of the Korean Society for Information Management, Vol. 25, No. 4, pp. 185-204, 2008.

[20] Kim, Y. O., "A study on the development of prosocial behavior scale for young children," Korean J Child Stud, Vol. 24, No. 5, pp. 105-118, 2003.

[21] Korea Institute of Human Resources Development in Science and Technology, An Introduction of R&D Management in Science and Technology, 2019.

[22] Korea Institute of Human Resources Development in Science and Technology, Understanding Research Security, 2015.

[23] Korea Internet & Security Agency, Information Security Management System, 2018.

[24] Korean National Police Agency, stats statistical data, 2020.

[25] Kwon, N., Lee, J., and Chung, E., "Understanding scientific research lifecycle : based on bio and nano scientists' research activities," Journal of the Korean Society for Library and Information Science, Vol. 46, No. 3, pp. 103-131, 2012.

[26] Kwon, W. H., "A study on the concept of R&D phases: From basic research to product development," KAST Research Report, Vol. 73, pp. 1-68, 2010.

[27] Kwon, Y. and Lim, J., "New business development of small venture firms through open innovation strategy: A case of acquiring technology from university," The Journal of Intellectual Property, Vol. 8, No. 2, pp. 151-177, 2013.

[28] Lederman, L. C., "Assessing educational effectiveness: The focus group interview as a technique for data collection," Communication Education, Vol. 39, No. 2, pp. 117-127, 1990.

[29] Lee, H., "A study on counter-measures on the technology leakage crimes an their enhancement," The Korean Society of Private Security, Vol. 11, No. 2, pp. 283-301, 2012.

[30] Lee, H. Y., “A study on the raised problems related to complementing the industrial technology outflow prevention and protection law,” Inha Law Review: The Institute of Legal Studies Inha University, Vol. 11, No. 3, pp. 67-95, 2008.

[31] Lee, J., “researcher-centric security management system”, Ph.D. Thesis, Chung-Ang University, 2018.

[32] Lee, K. and Yeom, D., “A study on the establishment of weight for sustainability assessment indicators and test scoring for super high-rise residential complexes,” Journal of the Architectural Institute of Korea Planning & Design, Vol. 24, No. 3, pp. 23-32, 2008.

[33] Lee, S., “A study on the effective method for the prevention of industrial secrets leakage,” Chung_Ang Law Review, Vol. 21, No. 1, pp. 39-80, 2019.

[34] Lee, S. B. and Kim, M. S., “The method of evaluating the validity in making the checklist of statistical method,” Journal of the Korean Data And Information Science Society, Vol. 9, No. 2, pp. 323-336, 1998.

[35] Lee, Y. and Kang, D., “Empirical study on the determinants of improving open innovation performance: Based on new product development collaboration with suppliers,” Journal of Korea Technology Innovation Society, Vol. 21, No. 3, pp. 1050-1076, 2018.

[36] Lisa, M. and Tina, M., “Chemical laboratory safty and security,” The National Academies Press, pp. 59-70, 2011.

[37] Ludvigson, S. C. and Ng, S., “The empirical risk-return relation: A factor analysis approach,” Journal of Financial Economics, Vol. 83, No. 1, pp. 171-222, 2007.

[38] Ministry of Science and ICT, Regulations on the Management, Etc. of National Research and Development Projects, 2020.

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

[40] Ministry of Trade, Industry and Energy, Act on Prevention of Divulgence and Protection of Industrial Technology, 2020.

[41] MISWG(The Multinational Industrial Security Working Group), Project Security Instruction, 2007.

[42] National Intelligence Service, Industrial Security White Paper, 2015.

[43] National Security Authority, Industrial Security Manual Finland, 2011.

[44] NAVER, “research,” “security,” https://dict.naver.com, May 2020.

[45] Park, C. and Hwang, J. H., “Countermeasures against national outflows,” STEPI Insight, Vol. 120, pp. 1-33, 2013.

[46] Park, K. H. and Jang, M. H., “Exploring decision-making factors of psychiatric nurses in the application of seclusion and restraint: Applying focus group interviews,” Journal of Korean Academy of Psychiatric and Mental Health Nursing,

Vol. 27, No. 4, pp. 380-393, 2018.

[47] Park, W., Son, S. Y., Park, H., and Park, H. S., "A proposal on determining appropriate sample size considering statistical conclusion validity," Seoul Journal of Industrial Relations, Vol. 21, pp. 51-85, 2010.

[48] Roh, H., "A study on the countermeasure of industrial technology outflow," Korean Association of Public Safety and Criminal Justice Review, Vol. 17, No. 1, pp. 45-77, 2008.

[49] Ryoo, W. and Jung, H., "Defining and tailoring R&D standard process to improve the quality of R&D outcomes," Journal of the Korean Institute of Industrial Engineers, Vol. 43, No. 2, pp. 112-119, 2017.

[50] SANS(SysAdmin, Audit, Network and Security) Institute, Lab Security Policy, 2014.

[51] Society for e-Business Studies, A study on the Improvement of the National R&D Programs Security Management System and the Revision of the Standard Manual, Science and Technology Comprehensive Coordination Support Project Report, 2017.

[52] The Korean Association for Research of Industrial Security, Industrial Security Studies, 2019.

[53] Um, I., Hong, C., and Hwang, W., "Optimal ratio of r&d investment and improvement methods for sustainable economic growth," Kistep Issue Paper, Vol. 17, pp. 1-64, 2019.

[54] Vagias, W. M., "Likert-type scale response anchors," Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management, Clemson University, 2006.

[55] Williams, B., Onsman, A., and Brown, T., "Exploratory factor analysis: A five-step guide for novices," Australasian Journal of Paramedicine, Vol. 8, No. 3, 2010.

[56] Yang, C. J., Hong, J. S., and Ko, S. W., "Impulse Responses Analysis of Government and Public Sector R&D in IT Industry," Korean Management Science Review, Vol. 25, No. 3, pp. 13-26, 2008.

[57] Yim, S. and Jung, U., "A study on the strategic management of the public R&D facilities: The direction of service quality improvement and managerial role reformation," Journal of Korea Technology Innovation Society, Vol. 12, No. 2, pp. 388-412, 2009.

[58] Yoo, I., Seo, B., and Park, D., "The role of open innovation for SMEs R&D success," Journal of Intelligence and Information Systems, Vol. 24, No. 3, pp. 89-117, 2018.

[59] Yoon, C., "A study on the improvement of product management system in international collaborative research," Journal of Korea Technology Innovation Society, Vol. 12, No. 3, pp. 499-524, 2009.

[60] Yoon, H., Hong, A., and Jung, S., "The effects of R&Ds, technology innovation

capability and the innovation support system of small- and medium-sized businesses on the company performance," Innovation Studies, Vol. 13, No. 2, pp. 209-238, 2018.

[61] You, Y. C., "The study of applying the indices of performance evaluation on the research and development in agricultural science and technology," Korean Public Administration Quarterly, Vol. 24, No. 1, pp. 27-49, 2012.

[62] Yun, S. and Kim, J., "A study on security requirments analysis through security threat modeling of home IoT appliance," The Journal of Society for e-Business Studies, Vol. 24, No. 2, pp. 113-124, 2019.

저 자 소 개

나원철 (E-mail: nastop@cau.ac.kr)
2020년 중앙대학교 융합보안학 (박사)
2020년～현재 중앙대학교 융합보안학과 (박사 후 연구원)
관심분야 산업보안(Industrial Security), 연구보안(Research Security), 기업정보 보안(Corporate Information Security)

장항배 (E-mail: hbchang@cau.ac.kr)
2006년 연세대학교 정보시스템관리 (박사)
2014년～현재 중앙대학교 산업보안학과 교수
관심분야 산업보안(Industrial Security), 보안 데이터 분석(Security Data Analyzing), 인간중심 보안(Human-Centric Security)