연구보안 수준측정 모형 설계에 관한 연구

이효직*, 김자원**, 나원철**, 장항배***
*중앙대학교 기술경영 및 보호 연구실
**중앙대학교 융합보안학과
***중앙대학교 산업보안학과
e-mail : {*leehyojik, **jjawon, **nastop, ***hbchang}@cau.ac.kr

A Study on Design of Model for Research Security Level Measurement

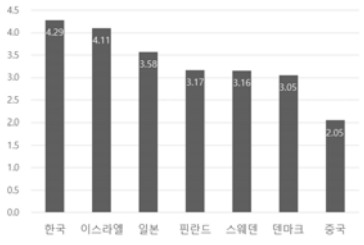
Hyojik Lee*, Jawon Kim**, Onechul Na**, Hangbae Chang***
*Management of Technology and Security Lab., Chung-Ang University
**Department of Security Convergence, Chung-Ang University
***Department of Industrial Security, Chung-Ang University

요 약

최근 국가연구개발사업은 개방형 연구환경으로 변화되어지고 있다. 이러한 변화는 연구개발 자원 및 시간 절감, R&D 투자효과 증대 등 긍정적인 효과를 동반하지만 연구 수행 과정, 연구성과물 유출과 같은 역기능이 발생하고 있다. 따라서 본 연구에서는 연구환경 변화에 따른 연구성과물 유출 가능성을 줄이기 위해서 자체적으로 보안관리 및 평가를 할 수 있는 연구보안 수준측정 모형을 설계하고자 한다. 이는 연구기관의 보안 수준 파악과 향상을 위해 유용하게 활용될 것으로 기대된다.

1. 서론

최근 세계 각국은 국가 당면과제 해결과 부가가치를 창출하기 위해 연구개발 투자에 막대한 비용을 투자하고 있다. 우리나라도 선제적 미래를 대비하기 위하여 기존에 집중적으로 투자하고 있는 ICT 산업을 비롯하여 에너지 산업, 문화기술, ICT 융복합을 통한 신농수산산업 등 다양한 산업분야에 많은 연구개발 투자를 진행하고 있다. 우리나라는 2014년 국내 총생산금액(GDP) 대비 연구개발 투자비율은 4.29%로 세계 1위이며, 연구개발비 규모는 약 605억 달러로 세계 6위의 수준에 다다랐다. 이러한 국가적 차원의 연구개발 투자는 신기술 개발뿐만 아니라 신산업 발굴 및 일자리 창출, 민간기업 투자 유도 등 국가 경쟁력 강화를 위한 중추적인 역할을 담당하고 있다[1].



(그림 1) 2014년 국내 총생산금액(GDP)대비 연구개발 투자비율

막대한 연구개발 투자로 인해 첨단기술의 발전이 매우 빠르게 진행되고 있지만, 이와 동시에 국내기술이 국내외 경쟁기업의 유출대상이 됨에 따라 연구개발 기술의 유출범죄도 비례하여 증가하고 있다. 최근 대학 및 기업의 연구소에서 휴대폰, 디스플레이, 반도체 등과 같은 첨단 기술 및 연구성과물이 유출되는 사고가 빈번하게 발생하고 있다. 또한 유출범위 및 유출방법도 다양화되어짐에 따라 유출사고에 대한 탐지 및 수사가 더욱더 어려워지고 있는 실정이다[2].

2. 개방형 연구환경

정보통신연구진흥원[3]은 지식창출의 원천이 다양해지고 연구 인력의 유동성이 확대되면서 자체적인 연구개발을 통한 기술 확보 전략의 효과성에 한계점을 제시하였다. 또한 이러한 한계점을 극복하기 위해 개방형 연구개발이 새로운 기술확보 전략으로 주목받고 있음을 설명하다. 본 연구에서는 개방형 R&D를 외부의 아이디어 ,지식, 기술을 활용하고 내부에서 개발된 기술을 외부로 보내 새로운 시장을 개척하는 기술확보 방식이라고 설명하고 있다. 개방형 R&D는 내부지식과 외부지식을 인소싱(In-Sourcing)을 통해 결합하여 기술의 혁신을 높이고 원천을 다양화 할 수 있으며, 내부의 기술을 외부화하여 자체 개발한 기술의 효율성을 극대화 할 수 있다고 설명하였다. 안치수[4]는 기존의 포괄적이고 개념적인 접근만 집중적으로 하는 개방형 혁신 연구의 한계점을 극복하기 위하여 개방형 혁신에 영향을 미치는 다양한 요인들을 종합적으로 분석하여 제시하였다. 또한 이러한 영향요인들이 개방형 혁신활동과 혁신성과에 어떠한 영향을 갖는지를 규명하기 위한 실증연구를 실시하였다. 본 연구에는 영향요인들을 환경, 기업,

제도적 특성 등의 3가지 영역으로 구분하였으며, 10가지 영향요인에 대한 변수를 도출하여 실증연구를 진행하였다.

민현구(2012)는 개방형 혁신 환경에서의 AHP-DEA 산정모형을 이용하여 객관적인 자료기반의 성과분석을 실시하였으며, 거래비용관점에서 연구개발 투입비율에 따른 개방형 혁신활동과 연구성과 간의 관계를 분석하고자하였다. 본 연구에서는 분석결과를 통해 개방형 연구개발 활동이 기존 연구개발 효율성보다 높게 평가되었으며, 너무 많이 개방형 혁신에 의존하게 되면 내부 연구능력을 개발하는데 장애가 되어 오히려 음(-)의 효과가 나타날 수 있다고 설명하였다.

3. 연구보안과 컴플라이언스

국가과학기술인력개발원[2]은 연구개발을 수행하고 있는 연구자를 위한 연구보안 가이드북을 제작하였다. 본 문헌에서는 연구참여자가 국가연구개발 과정 동안 연구결과물 유출 방지를 위해 수행해야 할 보안조치사항에 대해 자세히 설명하고 있다. 또한 연구보안을 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. 김성원[5]은 국가연구개발 관련 보안에 관한 규범과 내용을 분석함으로써, 현재 각 규정이 적용되어지는 대상 범위 및 조치사항에 대한 문제점 및 한계를 제시함과 동시에 이를 해결할 수 있는 개선책에 대해 연구하였다. 본 연구에서는 연구보안을 국가연구개발 사업에서 발생하는 성과물이 산업기술 등으로 지정/보호되기 이전에 주어지는 잠정적 보호라고 정의하고 있다. 강선준[6]은 개방형 혁신 시대에서 국제공동연구가 진행되어짐에 따라 현재 연구보안관련 규정 및 지침에 대한 적용의 문제점 및 한계를 분석하고 이에 대한 개선점에 대해 논의하였다. 본 연구에서는 연구보안을 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.

국가연구개발사업 보안관리 표준메뉴얼은 국가연구개발사업을 수행하는 기관이 체계적인 연구보안 규정을 수립할 수 있도록 연구보안 관련 인원이 기본적으로 지켜야하는 연구보안 관련 조치사항에 대해 제시하고 있다. 본 컴플라이언스는 기존 국가연구개발사업 보안관리 규정의 문제점과 미흡한 점을 파악하여 이를 보안하고 체계적인 내부규정 마련을 할 수 있도록 개발하였다. 본 컴플라이언스에서는 크게 분류영역을 보안관리체계, 참여연구원관리, 연구개발결과 및 내용의 관리, 연구시설관리, 정보통신망 관리 등 5가지 분야로 구분 하였으며, 총 44가지 보안 조치사항에 대해 제시하였다. SysAdmin, Audit, Network and Security(SANS) 연구소는 1989년에 정부와 기업 단체간의 보안연구 및 그 소속 사람들의 IT보안 교육을 목적으로 설립된 조직이다. SANS연구실은 자체 연구실에 대한 주요 인프라시설 및 정보자산을 보호하기 위하여 Lab security Policy를 수립하고 있다. 또한 이를 자체적으로 사용할 뿐만 아니라 타 연구기관에도 적용될 수 있도록 계속적인 업데이트와 배포를 진행하고 있다. 본 컴플라이언스는 일반적 요구사항, 내부연구실 보안요구사항, 정책 컴플라이언스 등의 3개 영역으로 구분하고 있으며, 총 28개의 보안조치사항을 제시하고 있다. The National Academics Press(NAP)는 미국 의회에서 승인한 헌장에 따라 미국국립과학원(National Academy of Science)에서 운영되는 발간지이다. NAP는 안전한 연구환경을 구축하기 위하여 연구실 내 안전 및 보안을 수행할 수 있는 지침사항과 가이드라인을 제시하고 있다. 본 컴플라이언스는 공간관리, 장비관리, 재료관리, 실험 시 유의사항 및 안전한 환경구축을 위한 문화형성 등의 다양한 연구실 관리지침을 제시하고 있다. 또한 연구실 내 주요 정보 및 시스템을 보호하기 위한 연구보안도 다루고 있으며, 연구실 내 보호해야할 주요자산을 분류하고 보호대상 중점의 리스크 기반 연구보안 지침사항에 대해 자세히 설명을 하고 있다. 본 컴플라이언스는 연구내용 및 연구환경에 따른 보안수준등급을 분류하고 있으며, 각 등급별 보안조치사항에 대해 자세하게 설명을 하고 있다. 한국인터넷진흥원(Korea Internet & Security Agency, KISA)의 정보보호 관리체계(Information security Management System, ISMS)는 조직의 주요정보자산을 보호하기 위해 정보보호 관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리/운영하기 위한 종합적인 체계이다. ISMS 인증 점검항목은 정보보호 5단계 관리과정 요구사항의 12개 통제사항과 정보보호 대책 13개 분야의 92개 통제사항 등의 총 104개 통제사항으로 구성되어 있다.

4. 연구보안 수준측정 모형 설계

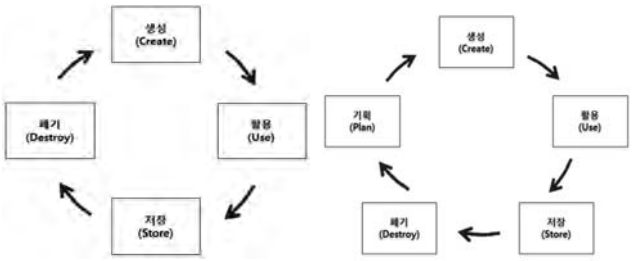
본 연구에서는 기존의 선행연구 분석을 통해 연구보안의 정의를 국가연구개발과제를 수행하는 과정에서 발생하는 모든 연구내용과 최종 연구성과물이 무단으로 유출되지 않도록 관리하는 보안활동이라고 정리하겠다. 위 연구보안의 정의를 살펴보면 가장 크게 두 가지 특징을 가지고 있는 것을 알 수 있다.

첫 번째는 국가연구개발과제를 수행하는 과정상에서 수행해야 하는 보안활동이란 점이다. 국가연구개발과제는 국가차원에서 연구개발이 요구되는 분야의 과학기술문제를 해결하기 위해 특정한 지향성과 목표를

설정하고, 연구개발자원을 전략적으로 집결하여 추진하는 사업을 뜻한다. 국가연구개발과제는 1개의 기관이 참여하는 단독연구과제부터 여러 기관이 참여하는 공동연구과제까지 다양한 형태로 진행되어지고 있다. 또한 국가연구개발 과제의 총 연구기간은 짧게는 3개월에서 길게는 5년까지 진행되고 있으며, 연구지원비는 3천만원에서부터 10억이상까지 차지하고 있다. 이를 통해 알 수 있듯이 국가연구개발과제는 국가기술개발을 위해 정부출연을 중심으로 중/소규모 단위의 프로젝트 운영이 진행되고 있으며, 기업과 달리 장기적인 관점에서 운영되는 것이 아니라 단기적 목표지향 중심의 운영이 되고 있다. 따라서 연구보안을 수행하기 위해서는 국가연구개발과제의 특징을 반영하여 기존의 기업에서 활용되고 있는 정보보안 관리체계가 아닌 중/소규모 단위의 프로젝트 운영에 적합할 수 있는 연구보안 보안관리체계의 도입이 필요하다.

두 번째는 연구보안의 보호대상이 국가 연구 개발 과정상에서 발생하는 모든 연구내용과 최종 연구결과물이라는 점이다. 앞서 말한 바와 같이 연구보안의 보호 대상은 크게 연구성과물(기획, 중간결과물, 연구성과 산출과정)과 최종 연구결과물(특허, 논문, 보고서 등)로 구분될 수 있다. 연구성과물은 연구개발 기간 동안 최종성과물이 만들어질 개연성이 매우 높음으로 그 최종결과물만큼이나 중요하다. 그렇기 때문에 최종성과물에 대한 보호뿐만 아니라 연구개발 과정 및 중간 성과물의 보호를 중요시 생각해야하며, 이에 대한 효과적인 보호를 위해 특별한 규정 및 지침을 두고 연구개발 과정에서 발생하는 모든 산출물을 보호해야할 필요가 있다.

위의 연구보안의 특징을 분석해본 결과, 정보보호 및 산업보안과 연구보안의 가장 큰 차이점은 보호대상 범위에서 발생 할 수 있다. 우선적으로 정보보호의 경우 보호대상은 정보이다. 정보는 크게 생성, 활용, 저장, 삭제 등 4가지 일련의 과정을 거치는 생명주기가 존재한다. 다음 그림은 정보의 생명주기에 대한 흐름도이다. 그림 2와 같이 생성된 정보는 그 자체가 최종 산출물(End Product)로서 직접 사용자 목적에 의해 활용되며, 하나의 독립적인 기능을 수행하게 된다. 이에 따라 정보보호는 정보생명주기의 각 단계별로 보안요구사항을 정의하고 이에 맞는 보안조치사항을 제시함으로써 정보를 보호하고자 한다. 하지만 연구보호의 대상인 연구정보는 실질적인 정보가 생성되기 이전에 개발하고자 하는 최종정보를 생성하기 위해 기획 단계를 거치게 된다. 그리고 기획단계에서 생성한 아이디어 및 계획을 기반으로 연구를 실시하며, 계속적인 연구를 통해 생성된 중간산출물을 활용하여 최종산출물이 생성되어진다. 이에 따라 연구보안의 보호대상은 최종결과물(End Product)뿐만 아니라, 최종결과물을 생성하기 위한 기획(아이디어), 중간결과물, 연구 프로세스 등의 연구과정에서 발생하는 모든 산출물을 포함시켜야한다.



(그림 2) 정보생명주기(좌), 연구정보 생명주기(우)

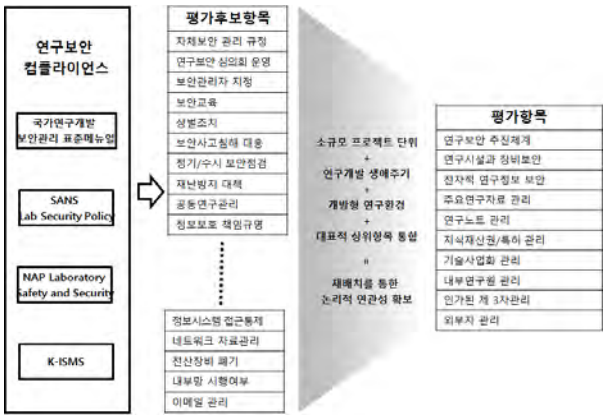
다음으로 산업보안의 경우 보호대상은 산업보안의 법적 토대가 되고 있는 산업기술유출방지법에서 자세히 설명되고 있다. 산업기술유출방지법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내 산업의 경쟁력을 강화하고, 국가의 안전보장과 국민경제의 발전에 이바지하고자 2006년 제정되어진 법이다. 산업기술유출방지법의 보호대상은 산업기술로 명시하고 있다. 해당 법안에서는 산업기술을 크게 국가핵심기술과 비 핵심기술로 나누며 개념 또한 달리 정의하고 있다. 국가핵심기술은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나, 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 될 수 있는 기술로 정의하고 있다. 또한 비핵심기술은 연구소가 창안·관리하고 있는 기술 중 국가핵심기술의 범주에 들지 않아 '산업기술보호법'의 적용을 받지 아니하는 일반기술을 말한다. 이러한 산업기술은 국가연구개발 사업과제를 통해 개발되어지는 경우가 많이 존재한다. 즉 국가연구개발의 성과물이 산업기술로 지정·고시되면 산업기술로서 보호를 받게 되고, 나아가 국가핵심기술로 지정·고시되면 산업기술보호법에 의해 핵심기술로서 보호를 받을 수 있다. 다음 그림은 산업기술유출 방지법의 법률적 분석을 통해 정리한 연구보안과 산업보안의 보호 범위 대상 차이점에 대한 내용이다. 따라서 국가연구개발의 성과물은 국가핵심기술 또는 일반산업기술이 될 수 있는 가능성으로 인해 산업기술유출방지법에 잠정적인 보호대상으로 적용될 수 있다. 이는 실질적으로 해당 법안 12조에서 국가연구개발사업의 보호관리에 대해 규정하고 있다.

본 연구는 우선적으로 연구보안 수준측정 항목을 개발하기 위하여 기존 4개 연구보안 컴플라이언스를 분석하여 평가 후보항목을 도출하였다. 연구보안 컴플라이언스의 비교분석을 통해 도출한 후보 측정항목을 연구보안 측정에 적합한 지표로 도출하기 위하여, 기 분석한 연구보안의 정의와 보호대상 범위가 반영된

측정항목을 도출하고자 하였다.

연구보안 측정항목을 도출한 기준은 다음과 같다. 첫 번째로 연구보안 측정항목은 국가연구개발 과정에서 적용되어져야 하기 때문에 기존의 타 보안의 수준측정이 조직 대상으로 이루어지는 것과 달리, 소규모 프로젝트 단위에서 적용되어지는 평가항목을 도출해야한다.

두 번째로 연구보호 대상의 범위는 국가연구개발 사업의 수행과정 상에서 발생하는 모든 산출물이 되기 때문에, 연구보안 측정항목은 연구기획 단계에서부터 연구결과물의 연구활용까지 각 단계에서 요구되어지는 보안평가항목을 도출해야한다. 세 번째로 개방형 연구환경의 변화에 따른 공동연구 과정에서 발생할 수 있는 보안위험을 관리할 수 있는 평가항목을 도출하고자 하였다. 마지막으로 유사하거나 중복된 통제항목은 대표적인 상위 평가항목으로 통합하여 중복성을 제거하고자 하였다. 위 기준으로 연구보안 측정항목을 도출한 과정은 다음의 그림과 같다.



(그림 3) 연구보안 수준측정 항목 도출과정

5. 결론

최근 국가연구개발은 개방형 연구환경으로 패러다임이 변화함으로써, 외부 연구자와 협업을 통한 공동연구를 수행하는 과정에서 연구성과물에 대한 노출이 쉽게 이루어져 무단으로 기술이 유출될 가능성이 높아지고 있다. 하지만 이러한 계속적인 기술유출사고가 발생함에도 불구하고 국가연구개발 투자에 비해 연구결과물 유출방지를 위한 연구보안에 투자는 상대적으로 미흡하다. 또한 국가연구개발을 수행하는 연구자의 보안의식이 부족하고 실질적으로 연구보안에 적합한 보안조치사항 및 평가체계의 부재로 인해, 연구성과물 보호를 위한 연구보안 수행체계가 적절하게 수행되지 않고 있다. 이러한 필요성에 입각하여 본 연구는 연구보안 수준을 효과적이고 효율적으로 측정할 수 있는 실천적인 보안수준 측정 모형을 개발하는 목적으로 시작되었다. 우선적으로 연구보안 수준측정 모형을 개발하기 위해 기존의 국가연구개발과 연구보안에 대한 정의 및 선행연구 분석을 통해 국가연구개발 구조 및 연구보안의 특성을 도출하고자 하였다. 다음으로 이러한 특성을 반영하여 국내외 연구보안 컴플라이언스를 기반으로 연구보안 수행에 적합한 평가항목을 도출하고자 하였다. 본 연구에서 개발된 측정모델을 사용할 경우 기대효과는 다음과 같다. 첫째, 현재 대부분의 국가연구개발을 수행하고 있는 정부출연기관이나 대학교에서 연구보안 수준을 적절하게 측정하고 수준을 파악하는데 유용하게 활용 될 수 있다. 둘째, 연구개발을 수행하고 있는 연구자들이 자체적으로 연구보안 관리체계를 수립하고 실천적인 보안활동을 수행할 수 있을 것이다. 셋째, 기존의 기업단위에서 많이 적용하고 있는 정보보호체계가 아닌 소규모 프로젝트 단위의 연구보안 평가항목을 적용함으로써, 평가측정의 효율성이나 사용성을 증가할 수 있을 것이다. 넷째, 보안성 향상뿐만 아니라 안전한 환경에서 연구수행을 하게 됨에 따라 연구개발 투자의 안정적인 성과를 기대할 수 있게 된다. 본 연구의 한계점은 기존의 연구보안에 대한 선행연구가 부족하고 연구보안 컴플라이언스 기반으로 모형을 설계하였기 때문에 도출한 측정항목이 광범위하다는 점이다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (H8501-17-1018)

참고문헌

[1] 미래창조과학부, 2017년도 정부연구개발 투장방향 및 기준(안), 2016

[2] 국가과학기술인력개발원, 연구보안의 이해, 2015

[3] 한국통신연구진흥원, 주간기술동향 통권 제 1347호, 2008

[4] 안치수, 이영덕, 우리나라 개방형 혁신활동의 영향요인에 관한 실증분석 연구, 한국기술혁신학회지, 14, 3, 431-465.

[5] 김성원 국가R&D관련 보안관리제도에 관한 검토, 한국산업보안연구학회논문지, 1, 1, 75-91

[6] 강선준, 국가연구개발사업 보안관련 법적체계 개선에 관한 연구, 법학논총 1, 1, 89-138