대학 내 산업보안활동 활성화 방안

Revitalization Solutions for Industrial Security Activities in Universities

정덕영[*], 정병수[**]
경동대학교 경찰행정학과[*], 동국대학교 경찰행정학과[**]

Duke-Young Jeong(jduke@k1.ac.kr)[*], Byung-Soo Jung(2079bs@hanmail.net)[**]

요약

우리나라의 경제규모가 커지고 첨단과학 기술의 보유가 늘어나면서 산업기술유출의 폐해가 날로 심각해지고 있다. 현재 우리나라의 산업기술유출은 매우 심각한 정도에 이르고 있지만, 산업기술의 유출에 대한 대응은 미비했던 것이 현실이다. 특히 산업기술 개발에 있어서 중요한 한 축을 담당하는 대학의 산업기술 유출방지 노력은 거의 찾아볼 수 없었다고 해도 과언이 아닐 정도로 소극적이고 미온적으로 대처하였다.

따라서 이 연구에서는 산업보안활동의 일환으로서 이러한 대학의 중요성을 피력하기 위하여 지금까지의 전반적인 산업보안활동의 실태 및 주요 사례를 분석하였으며, 대학이 산업보안활동을 활성화하기 위해서 어떠한 노력을 하여야 하는지 모색해 보고자 하였다.

■ 중심어 : | 산업보안 | 산업보안활동 | 산업기술유출 | 산업스파이 |

Abstract

As our nation's economy had grown in size and its possession of the cutting-edge science and technology had increased over the years, the damages received from the outflow of our industrial technology has become a serious issue. As of today, the outflow of Korea's industrial technology has reached a serious level, but in reality there were no adequate countermeasures carried out against it. Also, it is not too much to say that the effort to prevent the outflow of the university-developed industrial technology, which is one of the main pillars for the development of the nation's technological prowess, had been carried out in passive and lukewarm manner.

Therefore, as a part of the industrial security activity, we have analyzed the overall situation and major cases related to industrial security activities that have been carried out so far, in order to emphasize the importance of those universities. Also, we tried to find appropriate solutions for the universities to invigorate the industrial security activities needed.

■ keyword : | Industrial Security | Industrial Security Activities | Industrial Technology Outflow | Industrial Espionage |

Ⅰ. 서론

21세기 우리정부와 시민사회가 지향하는 국가목표중 하나가 '선진화'이다. 정치, 경제, 사회, 문화 등 우리사회 각 분야에서 선진화를 위하여 많은 노력을 하고 있으나, 우리는 선진화의 기본토대인 '보안시스템'이 매우

접수번호 : #100113-001
접수일자 : 2010년 01월 13일
심사완료일 : 2010년 02월 05일
교신저자 : 정덕영, e-mail : jduke@k1.ac.kr

열악하며 후진적이라는 사실을 망각하고 있는 듯하다. 얼마 전 우리나라를 떠들썩하게 만들었던 분산서비스 거부(DDOS)공격으로 사이버 보안이 위협을 받아 몇 일간 인터넷 경제가 마비가 되었음은 물론 중요국가시설의 인터넷 접속이 마비가 되는 등 취약한 보안시스템을 여실히 보여주었다.

보안의 영역이 종래의 군사적 위협으로부터 자국을 보호하는 전통적 보안에서 테러, 사이버테러, 산업스파이, 금융위기, 국가재난 등 초국가적 위협에 대응하는 포괄적 보안으로 확대되고, 새로운 형태의 안보위협이 국내외에서 증대되는 현실 속에서 우리의 보안시스템과 대응역량은 매우 부족하며 취약하기만 한 것이 사실이다.

특히 우리나라의 보안시스템과 대응역량이 취약한 부분은 산업보안으로서 우리나라는 과거와 달리 새로운 기술을 개발하기 위해 연구개발(R&D)에 꾸준히 투자한 결과 세계적으로 경쟁력 있는 최첨단 기술을 다량 확보하게 되었다. 이로 인하여 우리의 산업정보를 빼내려는 산업스파이의 주요 표적이 되고 있다. 첨단기술을 개발하는데는 많은 인력과 자금, 시간이 소요되지만 산업스파이가 기술을 빼내가는데는 단 몇 분이면 충분하다[1]. 막대한 자금과 인력을 투입하여 어렵게 개발한 첨단기술이 보안시스템과 대응역량의 부족으로 인하여 경쟁기업이나 해외로 유출된다면 해당 기업은 물론 국가경쟁력 저하로까지 이어지는 막대한 피해를 가져오기 때문에 산업보안은 매우 중요하다할 것이다.

대학은 첨단 산업기술을 창출하는 무한한 잠재력을 지닌 지식활동의 보고로서 풍부하고 우수한 연구자원(전체 R&D 인력의 52%, 2007년 국가 R&D 예산의 24%)을 바탕으로 원천기술에서부터 상용화기술까지 폭넓은 분야의 다양한 기술개발 단계를 포괄하는 연구성과를 산출하고 있으며, 전문화된 교육을 통하여 미래 성장 동력인 우수 인재를 배출하는 기능을 가지고 있는 매우 중요한 장소이다. 그러나 대학은 자유로운 학문연구의 전당으로써 연구 성과를 공공의 영역에 봉사해야 한다는 순수성에 무게중심을 둔 나머지, 연구 성과 관리와 활용에 관한 보안 시스템이 부족하며, 나아가 최근 우리사회에서 이슈가 되고 있는 우수 연구 성과에 대한 산업기밀보호라는 측면에서 거의 무방비 상태에 노출되어 있었다고 할 수 있다[2].

그러나 대부분의 산업보안에 대한 연구가 주로 산업스파이와 관련된 단속 법규, 대응상의 문제점, 기업의 영업비밀 보호와 관련된 법적 보호제도 등 기업에 대한 산업기밀보호의 측면에서만 연구가 이루어지고 있는 실정이다.

따라서 이 연구에서는 산업보안활동의 일환으로서 이러한 대학의 중요성을 피력하기 위하여 지금까지의 전반적인 산업보안활동의 실태 및 주요 사례를 분석해 보고, 대학이 산업보안활동을 활성화하기 위해서 어떠한 노력을 하여야 하는지 모색하고자 하는데 그 목적이 있다.

II. 연구의 이론적 배경

1. 산업보안활동의 의의

1) 산업보안의 개념

산업보안이라는 용어가 실무에 활용되기 시작한 것은 냉전체제가 붕괴되고 각국의 “자국이익 보호주의”가 팽배하면서부터 라고 할 수 있다. 국제정보전의 양상이 군사·외교 위주에서 국가경제 발전을 위한 정보와 기술수집으로 방향이 전환되면서 선진국을 필두로 대응책을 강구하게 되었고 이 과정에서 민간기업을 비롯한 연구소 등의 국제경쟁력을 갖춘 기술과 산업정보를 국가안보 차원에서 보호해야할 필요성이 대두되면서 ‘산업보안’이라는 용어가 본격적으로 사용되고 있어 행정환경 변화의 산물이라고 할 수 있다[3].

산업보안이라는 용어는 학문적 또는 법적으로 정립된 용어는 아니다. 그러나 최근 들어 첨단산업기술(high-tech industrial technology)이 발달하면서 이 기술이 산업경쟁력을 좌우하게 되었고, 첨단산업기술을 확보하고자 하는 산업스파이의 활동 또한 치열해지면서 첨단산업기술을 보호·관리한다는 의미로 주로 산업보안이라는 용어가 사용되고 있다. 첨단산업이란 일반적으로 가장 앞선 기술을 사용하되, 그 기술이 아직 불안정적이고 시장수요의 크기가 확정적이지 못하면

서, 공급자의 수는 극히 제한적이고 각자의 기술능력에 의해서 시장 등을 지배하는 특성을 내포하는 산업이라고 정의되고 있다[4].

즉 산업보안이란 첨단기술 뿐만 아니라 산업보안활동에 유용한 기술상, 경영상의 모든 정보와 인원・시설・자재 등을 산업스파이나 경쟁기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호・관리하기 위한 대책이나 활동을 의미하는 것으로 정의할 수 있다[5].

산업보안의 정의에서 알 수 있듯이 산업보안활동의 주체는 첨단산업기술을 보유한 기업이라고 볼 수 있지만, 산업사회에서의 기술과 정보 등의 유출은 막대한 국가경쟁력에 큰 손실을 유발할 수 있기 때문에 그 주체도 기업체나 산업체에 국한되지 않고 국가도 제한적이지만 산업보안활동의 주체가 될 수 있다. 산업의 첨단화와 함께 기술유출 시도 방법도 첨단화・글로벌화되고 있기 때문에 산업보안활동은 단순히 한 사람이나 한 기업의 노력만으로는 성공적인 성과를 거두기 힘들다.

따라서 산업보안활동의 주체는 산업기밀을 알고 있는 사람 즉, 기업의 산업활동과 관련하여 산업기밀 생산에 참여한 연구원이나 이를 감독 또는 취급하는 사람, 더 아나가 기업의 이익을 보호해야 할 책임이 있는 사람까지 포함된다. 보안활동의 객체인 보호대상은 산업활동과 관련하여 보호할 가치가 있는 인원・문서・시설 등 유무형의 제반 비밀사항을 포함한 산업기밀이다[6]. 일반적으로 산업기밀이란 부정경쟁방지법상의 영업비밀을 포함하는 넓은 의미의 개념으로서 첨단산업기술, 국가핵심기술, 첨단산업기술개발연구소, 첨단기술개발 관련자료 더 나아가 영업활동에 유용한 기술상 또는 경영상 정보까지 모두 포함된다고 볼 수 있다.

2) 대학 내 산업보안활동의 필요성

급속한 기술의 발달로 기업들은 치열한 생존 경쟁을 겪게 되면서 경쟁적 우위나 이점을 추구하기 위하여 산업스파이와 같은 경쟁적 정보활동에 참여하고 있다. 과거 국가 간의 이념이 대립되었던 냉전체제에서는 국방, 외교 정보나 국가 기반시설 등 국가 안보에 중요한 정보가 중심이 되는 국가 보안이 무엇보다도 중요했었다.

그러나 이제 이념 대립보다는 경제적인 이해관계에 따라 첨단 기술 정보, 경영전략정보, 미공개된 기업 정보 등 산업보안이 국가보안 못지 않게 중요성이 더욱 더 커지고 있다.

즉, 냉전당시에는 국방, 외교, 정치상의 비밀이 중요한 스파이행위의 대상이었고, 이에 대하여는 주로 정부간의 스파이전쟁에 의하여 진행되었으나, 냉전 이후 경제전쟁시대의 스파이활동은 오히려 경제적, 기술적 정보에 집중되고 있다[7].

이렇게 냉전체제가 무너진 이후에 비정상적인 방법으로 경쟁국의 첨단산업기술을 습득하기 위한 첩보전은 총성이 없는 전쟁의 한 유형으로 볼 수 있으며, 첨단기술을 보호하는 것 자체가 국가 안보에 있어서 매우 중요한 요소로 간주되고 있다.

오늘날 지식정보화사회에서 가장 중요한 지적재산의 확보를 위하여 각 국가들은 막대한 R&D자금을 투자하며 이에 힘쓰고 있다. 우리나라의 경우도 이와 마찬가지로 첨단산업기술의 보유를 위하여 많은 자금을 R&D에 투자하고 있는 실정이다.

그러나 각 나라의 첨단산업기술, 국가핵심기술 등과 관련된 연구 성과들은 철저하게 관리하지 않으면 기회비용도 아니고 매몰비용으로 허망하게 사라지게 된다. 대학에서 수행하고 있는 연구 활동의 85% 이상은 주로 R&D자금에 의해 수행되고 있다. 따라서 대학에서 개발된 연구 성과의 대부분은 국가 R&D와의 연관성을 부인하기 어렵다[8].

이렇게 대학에서 개발된 연구 성과의 대부분은 국가 R&D와 많은 관련이 있기 때문에 이에 대한 보안시스템이 취약할 경우, 경쟁국에 첨단산업기술이 유출될 수 있는 소지가 매우 크다. 따라서 대학에서 수행되고 있는 연구 활동, 개발된 연구 성과 등 연구 성과 관리와 활용에 관한 체계적인 산업보안활동이 필요하다.

이러한 대학의 산업보안활동의 필요성에도 불구하고 국내 대부분의 대학은 '산업보안의 사각지대'라는 지적이 많은 것이 사실이다. 대학 캠퍼스의 경우 출입이 자유로우며, 보안 시스템마저 미비한 경우가 대분이다. 또한 지속적이고, 체계적인 보안교육의 미비로 인하여 보안의식도 낮은 것이 현실이다. 각종 첨단 산업기술의

연구과제에 대한 국내·외 기업과의 산학협력이 활발하게 진행되면서 기술유출의 가능성이 더욱 더 높아지고 있는 현 시점에서 적극적인 대학의 산업보안활동이 요구된다.

2. 대학 내 산업기밀 유출 발생원인

1) 연구개발 인력의 불안한 지위

대학의 연구개발 인력은 우수한 산업기술을 기업에 공급함으로써 국가경쟁력을 높이는데 큰 역할을 담당하고 있음에도 불구하고, 그 지위가 불안정한 것이 현실이다. 기업이 경영합리화를 내세우며 구조조정에 들어가거나 긴축재정을 실시할 경우에 R&D 분야의 인력 감축에는 신중을 기해야 한다고 이론적으로는 강조하고 있지만, 실제로는 R&D 분야 인력을 우선 감축하고 있는 것이 우리 사회의 현실이다[9].

실제로 한국고등기술원이 2005년 8월 전국 이공계 대학교수 287명을 대상으로 실시한 설문조사 결과에 따르면 이공계 교수 10명 중 9명은 이공계의 위기가 심각하다고 생각하였으며, 이공계의 위기는 이공계 출신에 대한 사회적 대우가 낮은데서 비롯된다는 답변이 절반에 육박하였다.

최근 3년간 전국 국공립대에서 2만명 가까운 학생이 이공계를 떠나는 등 이공계 기피 현상이 심각해진 것으로 확인되면서[10] 대학의 연구개발 인력이 현장에서 겪고 문제점을 그대로 대변하고 있음을 알 수 있다.

2) 연구개발 성과에 대한 불충분한 보상

연구개발 성과에 대한 충분한 보상이 없다면 어떠한 보안노력도 성과를 거두기 어렵다. 직무발명에 대한 적절한 보상이 없으면 연구원은 자신의 연구 성과물을 기업에 빼앗겼다고 생각하게 된다. 하물며 대학의 경우에는 비영리기관으로서 기술을 직접 실시할 수 있는 길이 매우 제한되어 있으며, 기술거래협상을 통해 확보할 수 있는 수익은 실제 그 기술이 갖는 가치보다 현저히 낮은 경우가 많아 보상금을 지급할 재원의 마련이 일반 기업에 비하여 훨씬 어렵다는 문제가 있다. 대학 직무발명에 대한 불충분한 보상은 대학 연구원들이 국가적으로 매우 중요한 가치를 갖는 첨단 산업기술을 유출하여 금전적 보상을 받고 싶은 유혹에 빠지게 만들 우려가 있다[11].

실제로 산업기술 유출 실태조사에서 산업기술이 유출되는 원인에 '개인적 이익 추구'가 높은 비중을 차지[12]하는 것도 이와 같은 이유로 생각해볼 수 있다.

3) 보안 관리에 대한 인식부족

산업기술을 효과적으로 보호하기 위해서는 사후적인 대책의 마련도 매우 중요하지만, 사전적인 예방책의 마련이 더욱 중요하다. 그동안 대부분의 대학은 산업기술 유출방지와 별다른 상관이 없는 곳으로 여겨져 왔던 것이 사실이다.

그러나 기초와 원천, 응용기술의 구분이 점차적으로 모호해지고, 산·학·연 공동연구가 활성화되고 있으며, 국내의 대학연구진들도 과거와는 달리 세계적인 연구 성과를 잇달아 내놓고 있는 현 시점에서 대학은 보안 관리에 대한 인식을 제고하여야 한다. 기업연구소와 달리 대학연구소는 비교적 개방적이며, 연구인원들의 이동이 많기 때문에 보안측면에서 어려움이 있다. 이를 위해서 대학 교수진이나 연구원, 학생들의 산업보안에 대한 인식을 높이는 것이 무엇보다도 중요하다.

산업스파이에 대한 발생이 매년 증가하는 원인 중에 하나는 산업보안에 대한 인식이 매우 부족하여 철저한 관리가 이루어지지 않았기 때문이다. 효과적인 산업기술 유출 방지를 위해서 대학 연구진들에게 보안 관리에 대한 실무요령, 보안사고 시 대응방안이나 절차 등을 제대로 인식시켜야 할 것이다.

4) 기술적인 보안시스템의 미비

기술적인 보안시스템의 미비는 대학 내 산업기밀 유출의 발생 원인이 될 수 있다. 기술 유출의 수법은 갈수록 교묘해지고 지능화·조직화되고 있다. 또한 인터넷 통신의 발달, 컴퓨터 기능의 대용량화·소형화로 인하여 기술 유출은 더욱 더 용이해지고 있기 때문에 기술적인 보안시스템이 필요하다.

대부분의 대학은 일반 기업과 비교해서 기술적인 보안시스템이 미비한 것이 사실이다. 대학 연구실이나 실험실의 카드키 설치, 문서 세단기, 패스워드 및 이동식

디스크 관리는 어느 정도 기밀관리 시스템이 구축되어 있다고 볼 수 있다. 이는 다른 기밀관리 시스템에 비해 상대적으로 많은 예산이 소요되지 않기 때문에 일반 기업과 비교해서 큰 차이 없이 실행하고 있다.

그러나 상대적으로 예산이 많이 투입되는 네트워크 보안 시스템이나 침입 탐지 시스템 등의 기술적인 보안 시스템이 체계적으로 구축되어 있지 않아 기술 유출의 위험성이 있다. 모든 대학과 연구소를 대상으로 이러한 기술적인 보안시스템을 구축해야 하는 것이 아니라, 국가의 핵심 산업기술을 연구하는 대학 연구실이나 실험실에서는 기술 유출 방지를 위해서 기술적인 보안시스템의 구축이 필요하다.

Ⅲ. 산업기밀 유출 실태 및 주요사건 사례분석

1. 산업기밀 유출 현황

1) 연도별 산업기밀 유출 적발 현황

국가정보원 산업기밀보호센터에 따르면, 2004년부터 2008년까지 총 160건의 산업기밀 유출 사건을 적발하였다고 보고하였다. [표 1]에서 나타난바와 같이 2004년 26건에서 2008년 42건으로 산업기밀 유출 적발 건수는 매년 증가하고 있음을 알 수 있다.

또한 최근에 산업스파이의 주요 표적이 여러 분야에 확대되고 있는 추세에 있으며, 그 행위가 은밀하게 이루어지고 단속이 어려운 특징으로 보아 적발되지 않은 사건을 포함하면 통계에 나온 수치보다 훨씬 더 많을 것으로 생각된다.

표 1. 연도별 산업기밀 유출 적발 현황

연 도	2004	2005	2006	2007	2008
건 수	26	29	31	32	42

2) 분야별 산업기밀 유출 현황

기술유출 분야는 우리나라가 세계적 경쟁력을 가진 휴대폰·반도체 등 전자·정보통신 분야가 총 160건 중 100건으로 가장 많이 차지하였으며, 최근에는 자동차, 조선, 정밀화학 등 다른 분야로까지 확대되고 있는 추세로 기술유출이 어느 특정분야에 한정되지 않고 광범위하게 이루어지고 있음을 알 수 있다.

표 2. 분야별 산업기밀 유출 현황

분 야	전기 전자	정보 통신	정밀 기계	생명 공학	정밀 화학	기타
건 수	73	27	23	6	10	21

3) 신분별 산업기밀 유출 현황

2004년부터 2008년까지 신분별 기술유출 현황을 살펴보면 주로 전·현직 직원(132건)에 의한 생계형 기술유출이 대부분임을 알 수 있다. 기업의 내부자가 정보유출에 깊게 관여하게 되는데 내부자는 보통 목표물인 기술정보를 내장한 저장장치와 이를 입수할 수 있는 인적 네트워크를 소유하고 있으며, 내부통제 및 보안구조의 허점 등에 대해서도 잘 알고 있기 때문에 기술유출을 용이하게 할 수 있다고 생각된다.

또한 협력·용역업체에 의한 기술유출 사례도 점차 증가하고 있어 이들에 대한 보안 관리의 필요성이 증대되고 있다.

표 3. 신분별 산업기밀 유출 현황

신 분	전직 직원	현직 직원	협력 업체	유치 과학자	투자 업체	기타
건 수	89	43	16	6	3	4

4) 유형별 산업기밀 유출 현황

유형별 기술유출 현황을 살펴보면 연구원을 매수하여 기술을 유출하는 유형이 89건으로 가장 많았다. 연구원 매수는 대부분 스카우트 형식으로 고액의 돈을 제시하는 등 금전적 유혹에 의한 매수의 형태로 이루어지고 있다. 그 다음으로는 무단보관 30건, 내부공모 17건, 공동연구 9건, 위장합작 6건, 기타 9건으로 나타내고 있다.

표 4. 유형별 산업기밀 유출 현황

유 형	연구원 매수	무단 보관	공동 연구	위장 합작	내부 공모	기타
건 수	89	30	9	6	17	9

5) 동기별 산업기밀 유출 현황

기술유출 동기로는 개인 영리(68건) 및 금전유혹(52건)에 의한 기술유출이 120건(75%)으로 가장 많은 비중을 차지하였으며, 처우불만(16건)과 인사불만(11건)에 의한 유출이 27건(17%)으로 그 다음으로 높은 비중을 차지하였다. 그 밖에 비리연루 4건, 기타 9건으로 나타났다. [표 5]에서도 나타나듯이 산업기밀 유출은 대부분 금전적 이익과 개인적 이익을 위하여 범죄를 저지르고 있음을 알 수 있다.

표 5. 동기별 산업기밀 유출 현황

동기별	개인 영리	금전 유혹	처우 불만	인사 불만	비리 연루	기타
건 수	68	52	16	11	4	9

2. 산업기술 보호 수준[13]

규모별 산업기술 보호 수준을 살펴보면 규모1(종업원 1,000명 이상)인 기업의 보호수준이 총 4점에서 3.77점으로 가장 높게 나타났으며, 규모2(종업원 300명 이상 999명 이하)가 3.45점, 규모3(종업원 299명 이하) 3.23점으로 규모가 작을수록 보호수준이 낮게 나타나고 있음을 알 수 있다.

규모3 기업의 기술보호 수준이 낮은 원인으로는 보안관리 체계미비와 보안투자의 예산부족이 가장 큰 것으로 조사되었다[14]. 규모3의 경우에 대부분의 대학과 연구소 등이 포함되어 있기 때문에 이에 대한 대책마련이 필요하다. 규모별 산업기술 보호 수준은 [그림 1]과 같다.

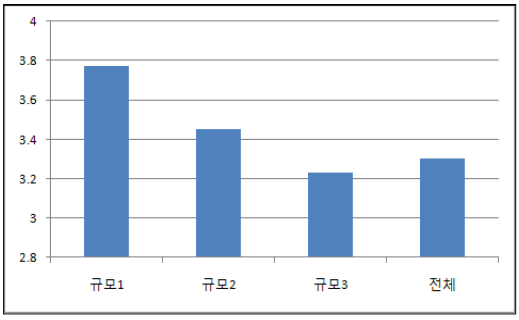

그림 1. 규모별 산업기술 보호 수준

3. 주요사건 사례분석

1) 사례

주요사건 사례에서는 대학연구기관과 관련된 기술유출의 사례를 위주로 구성하였으며, 신문기사의 특성상 알 수 없는 내용이나 부정확한 기사의 경우를 제외시켜 사례를 분석하였다.

【사례 1】 외국인 연구원 기술 유출 적발

대전에 소재한 K대학. 방글라데시 출신 연구원이 실험실 동료 연구원과 교수의 연구 자료가 든 컴퓨터 하드디스크를 통째로 뜯어 출국했다. 이 연구원은 이전에도 연구 자료를 자신이 나온 방글라데시의 대학 교수에게 이메일로 전송했다. 이 연구원은 끝내 모든 연구 자료를 압수당하고 강제출국 되었다.

서울 소재 모 대학에서 기술 전수를 위해 영입한 일본인 연구교수는 그 대학 연구실에서 국가 R&D과제로 수행 중인 나노형광체 관련 최신 연구 성과를 일본의 제조업체로 빼돌려 경고 조치를 받았다[15].

【사례 2】 태양광 산업기술 유출 대학교수 등 적발

수십억원의 연구비를 투자해 개발한 태양광 집광장치 관련 기술을 빼돌린 대학교수와 연구원 등이 경찰에 적발됐다. 경남경찰청 외사과는 3일 신기술 연구 자료를 유출한 대학교수 A씨(49) 등 5명을 부정경쟁방지 및 영업비밀 보호에 관한 법률 위반 혐의로 불구속 입건했다.

경찰은 또 A씨의 연구실에 보관돼 있던 하드디스크와 연구노트 등 증거물을 압수해 유출 경로를 파악하고 있다. 이들은 B사가 8년간 25억원의 연구비를 투자해 상용화 단계에 도달한 국내 유일의 '태양광 집광장치' 기술을 빼돌려 대학 연구실로 유출한 혐의다.

이들은 태양광 집광장치 연구 자료가 지난해 9월 지식경제부의 '신재생 에너지 개발'과제로 채택되면서 60억원의 정부출연금을 지급 받기로 결정되고 시제품 개발 완성 단계에 이르게 되자 이 같은 범행을 저지른 것으로 알려졌다.

A씨는 B사의 전직 이사이며 함께 입건된 겸임교수 C씨(36)는 전직 연구소장, D씨(33) 등 3명은 전직 연구원

이었다. 경찰은 "산학협동 연구과정에서 산업기술이 유출되는 사례가 빈번하다는 첩보를 입수하고 국가정보원과 공조 수사를 벌인 결과 이 같은 사례를 적발했다"며 "국내·외 시장에서 차지하는 기술적, 경제적 가치가 높거나 관련 산업의 성장 잠재력이 높은 국가 핵심기술과 국가첨단 산업기술, 신기술 등 유출사범을 색출하는데 수사력을 집중할 방침"이라고 말했다[16].

【사례 3】 자문 대신 기술 빼돌려 창업

서울지방경찰청은 근무하던 기업의 핵심 기술을 빼내 동종업체를 차린 혐의(부정경쟁방지 및 영업비밀에 관한 법률 위반)로 연구원 오모(34)씨를 구속하고 같은 회사의 기술자문을 맡은 모 대학교수 김모(45)씨 등 4명을 불구속입건했다고 17일 밝혔다. 또 이들과 짜고 허위 거래영수증을 제출하는 방법으로 정부지원과제 연구비를 가로채도록 도운 혐의(횡령)로 부품업체 대표 홍모(37)씨 등 6명을 불구속 입건했다.

경찰에 따르면 2001년부터 2005년 10월까지 군용 및 축산용으로 사용되는 휴대용 엑스레이 생산업체인 A사의 선임연구원과 기술자문교수 등으로 일하던 오씨와 김씨 등은 2005년 10월 제품의 핵심 제조기술을 유출해 김씨가 속한 대학의 창업보육센터에서 동종업체를 창업하고 유사제품을 만들어 수출해 5억여원의 이득을 챙긴 혐의를 받고 있다. A사는 휴대용 엑스레이를 생산하는 국내 5개 업체 가운데 매출액 400억원 규모의 선두 업체로, 이번 기술 유출로 150억원 정도의 피해를 봤다고 경찰은 전했다[17].

2) 사례의 분석

〔사례 1〕의 경우 전형적으로 대학에서의 기술 유출 위험을 여실히 보여주는 사례로서 대학들의 연구원 보안교육의 강화와 대학의 보안시스템 마련의 중요성을 나타내주고 있는 사례이다. 대학은 기업들에 비해 보안의식이 매우 약할 뿐만 아니라 체계적인 보안교육이 이루어지지 않고 있다. 지속적이고 장기적인 관점에서 보안교육이 이루어지지 않는다면 보안교육을 실시하더라도 연구 인력의 이동이 잦기 때문에 그 효과가 매우 미약하다.

또한 대학의 특성 상 외국 유학생이나 외국인 연구원에 의한 기술유출에 대한 정보통신 보안시스템, 물리적 보안시스템 등과 같이 총체적인 보안시스템이 마련되어야 한다. 〔사례 1〕의 경우에도 이러한 보안시스템의 부재로 인하여 기술유출이 용이했음을 알 수 있다.

〔사례 2〕, 〔사례 3〕은 산·학 협동 연구과정에서 기술이 유출된 사례로서 연구에 참여한 교수 및 연구원이 기술을 유출한 사례이다. 이 사례들을 사례분석에 넣은 이유는 많은 대학들이 산·학 협력 중심으로 연구가 진행되고 있으며, 이러한 과정에서 기술유출이 많이 이루어지고 있기 때문이다. 위의 두 사례들은 산·학 협동 연구과정에서 기업의 핵심 기술이 유출된 사례이지만, 또한 이러한 과정에서 대학의 핵심 산업기술이 유출될 수 있는 소지가 있음을 알 수 있다.

산업스파이들은 대부분 '내가 개발한 기술을 내가 이용하는데 뭐가 문제가 되나'라는 식으로 태도를 갖는 것이 하나의 특징으로서 자신의 기술을 자기가 활용한다는 생각으로 인하여 국가적·기업적 손실을 인식하지 못하는 경우가 대부분이다[18].

산업기술이 최초의 개발 기업이 아닌 경쟁업체 특히 외국의 경쟁업체에서 상품화되면 최초의 개발업체가 금전적으로 막대한 손실을 초래할 뿐만 아니라 국가 경쟁력에도 큰 손실을 초래할 수 있기 때문에 연구에 참여한 산·학 연구원들을 대상으로 보안 관리에 대한 인식을 제고시켜야 하며, 체계적인 보안시스템이 구축으로 기술 유출의 가능성을 최대한 미연에 방지하여야 한다.

Ⅳ. 대학 내 산업보안활동 활성화방안

1. 연구개발 성과에 대한 충분한 보상

동기별 산업기밀 유출 현황에서도 나타나듯이 산업기밀 유출은 대부분 금전적 이익과 개인적 이익을 위하여 행하여지고 있다. 연구개발 성과에 대하여 정당하고 충분한 보상을 하지 않는다면 그 어떠한 보안노력도 성과를 거두기 힘들다.

대학의 경우, 대학이 갖고 있는 특성[19]으로 인하여

기술거래협상을 통해 확보할 수 있는 수익은 실제 그 기술이 갖고 있는 가치보다 현저히 낮기 때문에 충분하게 보상금을 지급할 재원의 마련이 매우 어렵다. 대학의 연구원들은 상대적으로 낮은 연구비에 비해 과중한 업무 부담을 가지고 있는 것이 사실이다.

과중한 업무 부담에 비하여 열등한 대우를 받고 있는 대학 연구원의 현실은 연구데이터의 유출 위험을 높이는 대표적인 보안의 취약점이 되고 있다. 일반 기업에서 산업기밀의 유출이 주로 내부인에 의해 일어나고 있는 것처럼 대학에서도 연구데이터의 유출은 그 연구데이터를 얻어낸 내부의 연구원에 의해 일어나기 쉽다[20]. 열심히 개발한 연구개발 성과에 대한 불충분한 보상은 산업기술의 유출로 이어질 수 있기 때문에 이에 대한 대책이 마련되어야 한다. 예컨대, 대학과 공동으로 연구를 수행하는 기업의 경우에 연구 가치에 합당한 연구비를 책정하여 산・학 협동연구가 진행되어야 할 것이다.

2. 보안 관리에 대한 인식제고

보안시설 및 투자의 부족은 보안의식 및 교육의 부재에서 비롯된다. 일부 대기업을 제외한 대부분의 기업은 첨단기술 보호에 대한 인식이 매우 부족하다. 그나마 기업은 산업보안에 투자를 시작했지만 대학은 아직도 보안의식이 거의 없는 상태나 다름이 없다[21].

따라서 대학에서 효율적으로 산업보안활동을 활성화시키기 위해서는 연구원들을 대상으로 보안교육을 정례화 시켜야 한다. 교수 및 대학원생 등을 포함한 대학의 연구원들을 대상으로 지식재산의 중요성에 대한 인식을 제고시켜야 한다. 국가 R&D 사업으로 생성되는 대학의 지식재산은 연구자 개인소유가 아니라 공공재라는 인식을 갖도록 하는 것이 무엇보다도 중요하다.

이를 위해서는 산업보안에 대한 중요성을 연구원들에게 홍보하는 한편 보안 관리를 위한 실무요령, 보안사고시 대응방안 및 절차 등을 지속적이고 체계적으로 보안교육을 실시하여 대학의 보안역량을 강화하여야 한다. 대학은 일반 기업에 비해 보안의식이 약하고 보안교육을 실시하더라도 인력의 이동이 잦아 효과가 적기 때문에 보안교육이 일회성에 그쳐서는 안되며, 지속적이고 장기적인 관점에서 교육이 이루어져야 한다.

또한 대학은 문서화된 기술 보안 지침을 마련하여 이를 철저하게 지키고 있는지를 확인하여야 하며, 정기적인 워크샵과 세미나, 각종 전시회 등을 통해 보안교육이 꾸준히 이루어질 수 있도록 노력하여야 할 것이다.

3. 체계적인 보안시스템의 구축

체계적인 보안시스템을 구축하기 위해서는 크게 두 가지로 살펴볼 수 있다. 첫째, 대학은 산업보안활동을 활성화하기 위하여 제도적인 장치를 마련하여야 한다. 예컨대, 대학은 명문화된 보안 관리 규정을 신설하는 방안을 고려해 볼 수 있다. 보안 관리 규정을 명문화하여 연구원들이 준수해야 할 사항들을 명백히 인지시킴으로써 기술유출의 가능성을 크게 줄일 수 있기 때문이다.

또한 국가의 핵심기술과 관련된 연구원들을 대상으로 보안 서약서 작성을 의무화하는 방법도 생각해 볼 수 있다. 이는 추후 발생할 수 있는 문제를 사전에 차단할 수 있는 가장 현실적인 방법이며, 기술 유출 사건이 발생하더라도 당사자에게 민・형사상 책임을 물을 수 있기 때문이다.

둘째, 국가의 핵심기술을 연구하는 대학 연구실이나 실험실에서는 기술 유출 방지를 위해서 기술적인 보안시스템을 마련하여야 한다. 대부분의 대학은 상대적으로 예산이 많이 투입되는 네트워크보안 시스템이나 침입 탐지 시스템 등의 기술적인 보안시스템이 구축되어 있지 않고 있는 실정에 있다. 이러한 이유로 「산업기술의 유출방지 및 보호에 관한 법률」 제22조에서는 국가핵심기술 보유기관 등 대상기관에 대하여 산업기술 보호설비 구축 등에 필요한 기술 및 경비 등을 지원할 수 있도록 규정하고 있다.

지식경제부가 주최하고 있는 이 사업은 주로 기술유출방지를 위한 보안시스템, 즉 물리적 보안솔루션[22]과 기술적 보안솔루션[23]의 구축을 지원하는 것이다. 따라서 대학에서 국가의 핵심기술을 소지하고 있으나, 예산 등의 문제로 기술적인 보안시스템을 구축하지 못하였을 경우에 정부의 지원금을 활용하여 보안 시스템을 구축하는 방안을 모색해 볼 수 있다.

4. 대학산업보안협의회의 활성화

대학에서도 산업기밀 보호에 대한 관심이 커지기 시작하면서 서울대, 연세대 등 수도권 소재 10개 대학 산학협력단장들이 2007년 7월 30일 국가정보원 국가정보관에서 모여 '대학산업보안협의회'를 설립하였다. 대학산업보안협의회는 대학의 지식재산권에 대한 보안관리 역량 제고를 위해 연 2회 정기총회를 열어 대학의 연구기밀 보호 정책 및 제도, 보안관리 역량 강화를 위한 정보교류 및 공조방안, 대학의 기술윤리, 보안관련 교육 및 보안 컨설팅에 관한 사항, 기타 산업보안업무 발전을 위한 사업 추진방안 등의 논의를 목적으로 하고 있다[24].

2008년 4월 8일에 개최된 대학산업보안협의회 2차 회의에서는 한국과학기술원(KAIST)과 포항공대 등 전국 소재 주요 대학교로 확대하여 각 대학의 연구성과물 보호체계 구축에 대한 논의를 진행하였다[25]. 그러나 실제 대학산업보안협의회를 통해 얻어지는 실질적인 성과가 부족하며, 우리나라 산업보안활동에 중추적인 역할을 하고 있는 경찰과 국가정보원의 협조가 원활하게 이루어지지 않고 있어 형식적으로 운영되고 있는 측면이 있다. 따라서 대학산업보안협의회를 활성화시키기 위한 방안을 구체적으로 제시하면 다음과 같다.

첫째, 대학산업보안협의회는 유관기관과의 공조체제를 강화해야 한다. 국가정보원 산업기밀보호센터의 주요 업무로는 첨단기술 해외유출 방지활동, 산업보안교육 및 컨설팅, 산업보안 설명회 및 워크샵개최, 산업보안 관련 정책자료의 제작·지원 등이 있다. 따라서 국가정보원 산업기밀보호센터에서는 국가핵심기술을 연구하고 있는 대학 연구소의 보안관리를 위해 맞춤형 산업보안교육과 보안컨설팅을 실시하여 적절한 보안대책을 지원할 수 있기 때문에 적극적으로 공조체제를 강화할 필요가 있다. 또한 산업보안관련 범죄의 수사를 담당하고 있는 경찰은 산업보안 수사사례 소개 및 산업스파이 검거 활동에 관한 사항 등에 관하여 대학에 많은 정보를 제공할 수 있기 때문에 유관기관과 긴밀한 공조가 이루어지도록 하여야 한다.

둘째, 대학산업보안협의회는 가능한 많은 대학이 참여할 수 있도록 적극적인 홍보를 하여야 하며, 매년 정기적으로 개최되어야 한다. 대학산업보안협의회 2차 회의에서는 첫 회의에 비해서 전국 소재 주요 대학으로 확대하여 회의가 진행되었다. 그러나 홍보의 부족으로 아직까지 많은 대학들이 참여하지 못하고 있는 실정에 있기 때문에 가능한 많은 대학이 참여할 수 있도록 적극적인 홍보를 할 필요가 있다. 또한 대학산업보안협의회는 매년 정기적으로 개최되어 대학의 지식재산권에 대한 보안관리 역량 제고를 위해 다각적인 방안을 논의하여야 한다.

V. 결 론

시장경쟁력을 갖추기 위해 첨단산업기술을 확보하려는 노력은 세계 곳곳에서 총성 없는 전쟁처럼 치열하게 전개되고 있다. 이러한 시대적 흐름에 따라 우리나라도 과거와 달리 단순한 기술수입국에서 벗어나 상당한 정도의 첨단과학 기술을 보유하고 있으며, 이를 위하여 많은 노력과 투자를 아끼지 않고 있다.

이렇게 우리나라의 경제규모가 커지고 첨단과학 기술의 보유가 늘어나면서 산업기술유출의 폐해가 날로 심각해지고 있다. 현재 우리나라의 산업기술유출은 매우 심각한 정도에 이르고 있지만, 산업기술의 유출에 대한 대응은 미비했던 것이 현실이다. 특히 산업기술 개발에 있어서 중요한 한 축을 담당하는 대학의 산업기술 유출방지 노력은 거의 찾아볼 수 없었다고 해도 과언이 아닐 정도로 소극적이고 미온적으로 대처하였다.

따라서 이 연구에서는 산업보안활동의 일환으로서 이러한 대학의 중요성을 피력하기 위하여 지금까지의 전반적인 산업보안활동의 실태 및 주요 사례를 분석하였으며, 대학이 산업보안활동을 활성화하기 위해서 어떠한 노력을 하여야 하는지 모색해 보았다. 이상으로 대학이 산업보안활동을 활성화하기 위한 방안들을 간략히 정리해보면 다음과 같다.

첫째, 연구개발 성과에 대한 충분한 보상이 있어야 한다. 과중한 업무 부담에 비하여 열등한 대우를 받고 있는 대학 연구원의 현실은 연구데이터의 유출 위험을 높이는 대표적인 보안의 취약점이 되고 있다. 일반 기

업에서 산업기밀의 유출이 주로 내부인에 의해 일어나고 있는 것처럼 대학에서도 연구데이터의 유출은 그 연구데이터를 얻어낸 내부의 연구원에 의해 일어나기 쉽기 때문에 열심히 개발한 연구개발 성과에 대하여 충분한 보상이 필요하다.

둘째, 보안 관리에 대한 인식의 제고이다. 보안시설 및 투자의 부족은 보안의식 및 교육의 부재에서 비롯된다. 대학은 아직도 보안의식이 거의 없는 상태나 다름이 없기 때문에 대학은 보안 관리에 대한 인식을 제고하여야 할 것이다. 이를 위해서 대학은 산업보안에 대한 중요성을 연구원들에게 홍보하는 한편 지속적이고 체계적인 보안교육을 실시하여 대학의 보안역량을 강화하여야 한다. 또한 대학은 문서화된 기술 보안 지침을 마련하여 이를 철저하게 지키고 있는지를 확인하여야 하며, 정기적인 워크샵과 세미나, 각종 전시회 등을 통해 보안교육이 꾸준히 이루어질 수 있도록 노력하여야 한다.

셋째, 체계적인 보안시스템의 구축을 들 수 있다. 체계적인 보안시스템을 구축하기 위해서는 제도적인 장치와 기술적인 보안시스템을 마련하여 한다. 우선, 제도적인 장치로는 대학이 명문화된 보안 관리 규정을 신설하는 방안과 국가의 핵심기술과 관련된 연구원들을 대상으로 보안 서약서 작성을 의무화하는 방안을 고려해 볼 수 있다. 또한 국가의 핵심기술을 연구하는 대학 연구실이나 실험실에서는 기술 유출 방지를 위해서 기술적인 보안시스템을 마련하여야 한다.

마지막으로 대학산업보안협의회가 활성화되어야 한다. 대학산업보안협의회를 활성화시키기 위한 방안으로는 유관기관과의 공조체제를 강화하여야 하며, 가능한 많은 대학이 참여할 수 있도록 적극적인 홍보를 하여야 한다. 그리고 매년 정기적으로 개최되어 대학의 보안관리 역량 제고를 위해 다각적인 방안을 논의하여야 한다.

지금까지 대학 내 산업보안활동 활성화방안에 관하여 살펴보았다. 그러나 이 연구를 진행하는데 있어서 대학의 산업보안활동에 관한 기존의 선행연구가 매우 부족하여 국가정보원의 자료들과 신문기사에 상당 부분 의존한 점은 연구의 한계가 되었다. 산업기술유출의 폐해가 날로 심각해지고 있는 현 시점에서 대학의 산업보안활동의 중요성은 더욱 강조될 수 밖에 없기 때문에 이에 관한 보다 심도 깊은 후속연구가 필요하다고 본다.

참 고 문 헌

[1] 국가정보원, "*첨단 산업기술 보호동향*", 제7호, p.6, 2007a.

[2] http://www.boannews.com/media/view.asp?page=1&idx=8299&search

[3] 민병설, "*산업보안체계의 정립에 관한 연구*", 경희대학교 대학원, 박사학위논문, p.16, 2002.

[4] 최순호, 정우일, "경찰의 산업보안활동 활성화방안", 한국경찰학회보, 제11권, 제1호, pp.230-231, 2009.

[5] 국가정보대학원, "*산업보안실무*", p.1, 2006.

[6] 민병설, "*산업보안체계의 정립에 관한 연구*", 경희대학교 대학원, 박사학위논문, p.23, 2002.

[7] 한상훈, *산업스파이에 대한 형사법적 대응방안*, 한국형사정책연구원, p.34, 2000.

[8] http://www.nisc.go.kr/app/dataroom/referenceview

[9] 국가정보원, "*대학산업기술보호 매뉴얼*", p.41. 2007b.

[10] http://www.emaeil.net/default/news/?nwsid=n3&grpid=000000004&mpart=&uid=16318

[11] 국가정보원, "*대학산업기술보호 매뉴얼*", pp.43-44, 2007b.

[12] 국가정보원, "*첨단 산업기술 보호동향*", 제7호, p.10, 2007a.

[13] 한국산업기술보호협회에서 2008년 4월 1일부터 2008년 7월 3일까지 산업기술보유기관(기업체, 대학, 연구소 등)을 대상으로 첨단산업기술보호 실태 및 관리현황을 파악하였다. 표본크기는 산업기술 보유 기업・기관 중에서 업종별・종업원수별・지역별로 임의 추출한 1,176개 기업・기관

(기업체 1,060개, 대학 79개, 연구소 37개)이며, 면접조사 및 이메일, 팩스 등에 의한 응답자 기입방식으로 설문을 진행하였다.

[14] 국가정보원, "*첨단 산업기술 보호동향*", 제10호, p.49, 2009.

[15] 국제신문, 2008년 12월 18일

[16] 뉴시스, 2009년 6월 3일

[17] 세계일보, 2009년 11월 17일

[18] 정병수, "*산업스파이의 실태분석 및 대응방안에 관한 연구*", 동국대학교 대학원, 석사학위논문, p.68, 2007.

[19] 대학은 비영리기관으로서 독자적으로 연구성과물을 상업화하는데 한계가 있으며, 스스로 산업기술을 통하여 이윤을 추구하는데 제한을 받게 된다. 대학의 산업기술은 별도법인의 설립이나 산학연계를 통해서만 상업화가 가능하다.

[20] 국가정보원, "*대학산업기술보호 매뉴얼*", p.153, 2007b.

[21] 국가정보원, "*대학산업기술보호 매뉴얼*", p.36, 2007b.

[22] 물리적 보안솔루션의 종류

① 영상감시 : CCTV, VCR, DVR, 화상감시용 소프트웨어

② 출입통제 : 리더(카드, 푸시버튼, 태그)등, 잠금장치 등

③ 알람모니터링 : 적외선 센서, 레이저 센서, 도어 및 윈도우스위치 등

④ 바이오인식 : 얼굴, 지문, 홍채, 정맥, 음성, 서명 인식 시스템 등

[23] 기술적 보안솔루션의 종류

① 네트워크보안 : 방화벽(Firewall), 침입탐지시스템(IPS) 등

② 서버보안 : DB보안(데이터 접근제어 암호화) 등

③ 응용시스템 : 문서보안솔루션(DRM), 패치관리시스템(PMS), 스팸차단시스템, 통합사용자인증관리(PKI/SSO) 등

④ 보안관리 : 기업보안관리시스템(ESM), 데이터백업 및 복구 등

[24] http://www.boannews.com/media/view.asp?idx=8299&kind=2&page=10

[25] http://www.dt.co.kr/contents.html?article_no=2008040902011369713002

저 자 소 개

정 덕 영(Duke-Young Jeong) 정회원

- 2000년 2월 : 동국대학교 경찰행정학과(법학석사)
- 2003년 8월 : 동국대학교 경찰행정학과(경찰학박사)
- 2005년 3월 ~ 현재 : 경동대학교 경찰행정학과 교수

<관심분야> : 경찰학, 범죄학, 민간경비

정 병 수(Byung-Soo Jung) 정회원

- 2005년 3월 : 동국대학교 경찰행정학과(경찰학석사)
- 2007년 9월 ~ 현재 : 동국대학교 경찰행정학과(박사수료)
- 2008년 3월 ~ 현재 : 세명대학교 경찰행정학과 강사

<관심분야> : 경찰학, 범죄학, 산업보안