情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

핵심 기술 관리 체계(CTMS) 수립을 위한 통제 항목 모델링 연구 및 제도적 개선 제안

신 동 혁,† 심 미 나,‡ 임 종 인
고려대학교 정보보호 대학원

Control items modeling methodology to establish core technology management system and successfully operating suggestions for institutional improvement

Dong-hyuk Shin,† Mina Shim,‡ Jong-In Lim
Graduate School of Information Security, Korea University

요 약

최근 지속적으로 증가하고 있는 핵심 기술 유출은 기업의 경쟁력뿐만이 아니라 대한민국의 국가 경쟁력과 연관된 큰 이슈로 지적되고 있다. 이에 따라 전 세계적으로도 기술유출 방지에 대한 관심이 매우 높으며, 세계 각국은 핵심 기술 유출 방지를 위한 제도 및 정책을 지속적으로 발전시키고 있다.

본 논문에서는 최근 국내에서 발생했던 기술 유출 사건의 개요와 시사점을 분석해보고, 세계 각국의 핵심 기술 유출 방지를 위한 법제도 등의 정책 동향 분석은 물론, 최근 국내에서 개정된 산업기술 유출 방지법 등 최신 법제도의 개정안을 분석해보고자 한다. 또한 기존 발전된 정보보호 관리 체계 인증을 보완하여 핵심 기술 관리 체계에 적용이 가능한 통제 항목 모델링 방법론을 연구하고, 구현해 보고자 한다. 마지막으로 핵심기술 관리 체계(CTMS)가 성공적으로 안착하기 위한 제도적 미흡점을 분석해보고, 이에 대한 개선 방안을 제안하고자 한다.

ABSTRACT

Recently the core technology leakage continues to increase. It is critical issue relating to national competitiveness rely on the company's competitiveness as well as both survival and competitiveness of company. So other countries have impyz roved their laws consistently to solve these problems. And recently our country amended the law. In the paper, we will analyze world's various laws and institutions relating industrial core technologies. And this paper will provide the suggestion to settle and to develop our country's industrial core technology's protection by refer to other laws.

Keywords: Seucurity Policy, Core Technology, Industrial Technology, Security Threats

I. 서 론

최근 글로벌 경제위기와 중국의 급부상 등에 따라 한국에서 주력으로 추진하는 산업에 대한 국제적인 경쟁이 더욱 치열해질 것으로 예상되고 있다. 이러한 분위기임에도 불구하고 대기업의 핵심 IT 기술이 국외로 유출되는 등 핵심 기술의 유출 사고가 지속적으로 증가하고 있다. 또한 피해액이 90조원에 이르는 것은 물론이고, 유출된 핵심 기술이 적용된 제품이 아직 출시도 되지 않은 상태라는 점에서 그 문제는 더욱 심각

접수일(2013년 1월 4일), 수정일(2013년 1월 29일), 게재확정일(2013년 2월 8일)
† 주저자, 008sdh@korea.ac.kr
‡ 교신저자, mnshim@korea.ac.kr

하다고 볼 수 있다. 따라서 첨단 기술의 유출은 단순히 기업의 경쟁력 상실의 문제가 아닌 국가 경쟁력의 문제로 대두되고 있다.

이러한 기술 유출 사고가 빈번해짐에 따라 세계 각국은 최신 IT 기술 등 첨단 기술을 개발하는 것 뿐 만이 아니라 이러한 핵심 기술들이 유출되지 않도록 어떻게 관리할 것인가 하는 법제도 또는 정책적인 문제에 대해 지속적으로 연구하고 있다. 그 이유는 다른 나라보다 얼마나 많은 신기술을 가지고 있는가가 국가 경쟁력과 신성장 동력과 직결되는 매우 중요한 문제이기 때문이다.

최근 국내에서도 외국인투자, 인수·합병(M&A) 과정에서 발생하는 국내기업의 기술유출에 대한 우려가 확산되고 있다. 그러나 국내에 유입된 외국자본들이 여전히 정부의 각종 혜택 속에서 국내 핵심 기술을 빼가는 등 기술 유출 피해로 확산되고 있어 문제가 심각하다. 특히 신흥 강대국으로 부상하고 있는 중국의 산업스파이 위협이 증가되고 있다. 미국 FBI 산업 스파이 법에 의해 제소된 건의 약 80퍼센트가 중국과 관련된 기소 건이라는 점은 한국뿐만 아니라 세계적으로 중국에 대한 경각심을 시사해주고 있다.

그럼에도 불구하고, 한국의 경우 핵심 기술 유출 방지를 위한 산업기술 유출 방지법 등의 법률 개정이 5년 만에 이루어지는 등 국가 보안 정책이나 법제는 여전히 개선해야 될 점이 많고, 핵심 기술 유출에 대한 대응 해답을 전통적인 기술 유출 방지 모니터링 솔루션, 매체 차단 기술 등 기술적인 부분에 의존해 왔던 것도 사실이다. 그러나 최근에 발생되는 대기업의 사고들이 기술적 조치로 충분한 투자가 선행된 국내 최고 수준이었다는 점에서 현 시점에서는 기술적인 통제가 아닌, 관리 체계 또는 법률 대응 강화 등 새로운 답안을 필요로 하고 있는 시점이 되었다.

이 논문에서는 한국의 핵심 기술 관리 체계 수립을 위해 다음과 같은 것을 논의해보고자 한다. 첫째, 한국의 법률 및 해외의 사례 등의 분석을 통해 현 시점에서 산업기술 유출 방지법이 갖는 의의를 분석해보고자 한다. 둘째, 컴플라이언스 준수를 위해 기업과 국가가 수립할 수 있는 현실적이고, 실효성 있는 핵심 기술 관리 체계 수립을 위한 연구를 진행해보고자 한다. 특히 기존에 도입되어 활성화된 정보통신망법, 개인정보보호법 등 기타 보안 관련 법률을 분석하여 핵심기술 관리 체계를 운영할 수 있는 관리 방법론을 도출 및 제안해보고자 한다. 셋째, 핵심 기술 관리를 위한 공공 및 교육 기관 등의 현실 및 근본적인 취약점에 대해서도 개선을 제안해보고자 한다.

II. 선행 연구 분석 및 본 논문 연구 방향

2.1 선행 연구 분석

앞에서 언급한대로 정부 차원에서 핵심기술의 지정 및 개정하고, 법률을 개선하는 등의 제도적인 노력을 하고 있는데도 불구하고, 핵심 기술 유출에 대한 사고 및 유출 시도는 끊이지 않고 있다는 것은 법률을 준수해야 하는 기업과 관리 및 점검을 할 수 있는 새로운 관리 체계의 제시가 필요하다고 말할 수 있다.

또한 기술유출 방지를 위한 모니터링 체계 수립 등 기술적 차원의 투자가 부족함이 없는 대기업의 사고 등은 이제 더 이상 기술적인 차원의 접근이 아닌 핵심 기술 관리 인력의 배출 등 사회 및 제도적인 개선에 대한 근본적인 노력을 필요로 한다는 시사점을 제시해주고 있다고 말할 수 있다.

본 논문 연구에 앞서 산업기술 유출과 관련한 논문들을 분석해본 결과 다음과 같은 선행 연구 결과를 얻을 수 있었다. 첫째, 핵심 기술과 관련한 대부분의 논문들의 초점이 이번에 개정된 산업기술 유출 방지법 개정에 필요한 형사 처벌 강화, M&A를 통한 핵심 기술 이전 취약점 보완 등 법제도적인 보완에 관련된 부분에 대해 분석하고 제안한 것이었다. 즉, 2011년도 이전 논문들은 외국의 법제도와 국내 법제도를 비교하여 국내 법제도가 가질 수 있는 취약한 부분에 대해서 지속적으로 언급을 한 논문이 대다수였다.

둘째, 최근에 발간된 핵심 기술 방지를 위한 관리체계와 관련해서는 '중소기업 산업기술 유출 방지를 위한 정보보호 관리 체계 설계'라는 논문이 2010년도에 게재된 바는 있다. 이를 분석해 본 결과 핵심 기술 유출 방지를 위해 중소 기업들이 어떻게 해야 할 것인지에 대한 방법론을 제시하고, 기업들이 적용해야 될 관리적, 기술적 방법론에 대해서 언급은 되어 있다. 그러나 실제 관리 체계를 국가, 기업적으로 어떻게 활성화하고, 기업에 효과적으로 적용하고 내재화할 수 있을지에 대한 방법론, 행정 및 제도적 프레임에 대한 부분은 제시가 되어 있지 않았다.

2.2 기존 논문과 본 논문의 차별화 및 연구방향

이에 따라 본 논문은 기존에 대부분의 논문에서 논의되었던 단순한 법제도적인 취약점을 언급하거나, 기

업 등에 적용될 수 있는 관리 체계 수립이 필요하다는 등의 단순한 필요성에 대한 개선 제안을 하고자 하는 것이 아니다.

본 논문에서는 다음과 같은 부분을 집중으로 연구하고 제안해보고자 한다. 첫째, 산업기술 유출 방지법 등 법률을 기업에 적용하고, 국가가 이를 관리할 수 있는 제도적인 프레임은 무엇인가에 대해서 고민해보고자 한다. 이를 위해서는 기존 정보보호 관련 컴플라이언스 준수를 위해 기업에서 활용하고 있는 정보보호 관리 체계(ISMS) 등의 사례를 참고해서 기업의 핵심 기술 관리 체계에 활용할 수 통제 항목 설계 등 모델링 방법론 등은 제시해보고자 한다.

둘째, 사회적으로 국가 핵심 기술 관리 체계를 수립하기 위한 근본적인 인력양성을 위한 교육 제도 개선 및 이를 위한 공공 기관의 역할도 개선 제안해보고자 한다. 본 논문에서 언급할 주제 범위와 내용에 대한 논문과의 차별화를 요약한 표는 다음 〔표 1〕과 같다.

〔표 1〕 기존 연구와 본 논문의 주제 범위와 내용 비교

구분	기존	본 논문 내용
주제 범위	기업 관리체계 수립 집중	1. 타법령 활성화된 정보보호관리 체계 분석을 통한 기술유출방지 시사점 도출 2. 교육+법제도체계적인 조화 언급
활성화 방안	중소기업 예산확보 등	1. 기존 인증 제도의 보완 언급 2. 교육 (민간 및 대학 등)의 노력 제안 3. 처벌 강화 등 법제도 개선 제안

III. 핵심 기술 관련 이론적 배경

3.1 한국의 핵심 기술 현황 및 조직 체계

3.1.1 핵심기술의 정의

핵심기술이란 '산업기술의 유출방지 및 보호에 관한 법률' 9조에 따라 지정된 산업기술을 말한다. 즉, 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 수 있는 산업기술을 말한다. 핵심기술은 국가 안보 및 국민경제에 영향을 미치는 파급효과와 관련 제품의 국내외 시장 점유율, 해당분야의 연구 동향 및 기술 확산과의 조화 등을 종합적으로 고려하여 선정하고 있다〔1〕. 한국은 2007년 9월 산업기술 보호위원회에서 40개의 핵심 기술을 선정한 이후 2011년, 2012년에 걸쳐서 핵심기술을 재조정하는 최근 2년에 걸쳐 2차례 핵심 기술이 재조정되는 등 〔표 2〕 같이 국가 차원에서도 많은 논의가 이루어지고 있다.

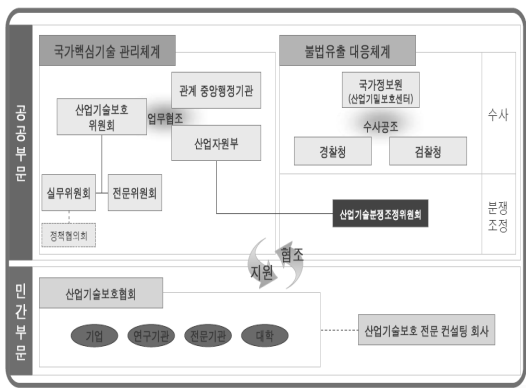
〔표 2〕 핵심 기술 지정 연혁

년도	내용
07년 8월	산업기술보호위원회가 개최되어 아래 7개 분야 총 40개 기술을 국가핵심기술을 분야별로 선정함 (전기·전자 (4), 자동차 (8), 철강 (6)
11년 2월	자동차 기준변경, 정보통신 추가지정 등 8개 분야 총50개 국가핵심기술 재조정
12년 1월	정보통신 기준변경 및 추가지정 등 8개 분야 총 58개 기술로 국가핵심기술을 재조정됨 (전기전자 (8), 자동차(8), 철강 (6), 조선 (7), 원자력 (4), 정보통신 (17), 우주 (5), 생명공학 (3) 등 총 59개)

3.1.2 한국 핵심 기술 보호 조직 체계

한국의 핵심 기술 보호 조직 체계는 산업기술 보호위원회 아래로 국가 정책 과제에 대해 사전에 협의하는 정책 협의회가 있으며, 전문 위원회와 실무 위원회 등 2개의 위원회를 통해서 핵심 기술을 지정, 변경, 해제 처리하고 있다. 핵심 기술 유출 방지를 위한

공공 및 민간의 업무 영역은 아래 〔그림 1〕과 같으며, 각 위원회 및 기관의 역할은 〔표 3〕과 같다.



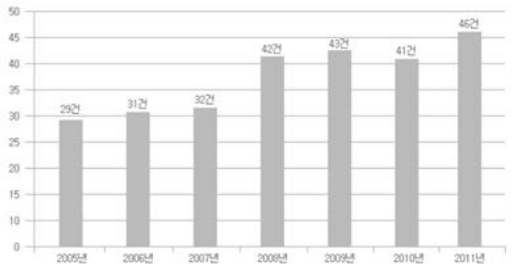
〔그림 1〕 핵심 기술 보호 조직 체계

〔표 3〕 핵심 기술 관련 위원회 및 관계 기관의 역할

조직	역할 업무
산업기술 보호위원회	산업기술보호위원회는 금년 4.28일 발효된「산업기술의 유출방지 및 보호에 관한 법률」(이하 "법"이라 함)에 의한 최고의사결정기구임 국가 핵심 기술을 지정, 변경, 해제 및 심의를 함
실무위원회	국가 핵심 기술 지정, 변경, 해에 대한 안건을 사전검토하거나 조정하는 역할을 수행함
전문위원회	국가 핵심 기술 지정 변경 해제에 관한 전문적인 검토를 수행함
정책협의회	국가 정책 과제에 대한 사전 협의와 조정을 수행함
관계중앙행정기관	지정 대상 기술을 선정하고 통보하며, 국가 핵심 기술 변경, 해제를 요청함

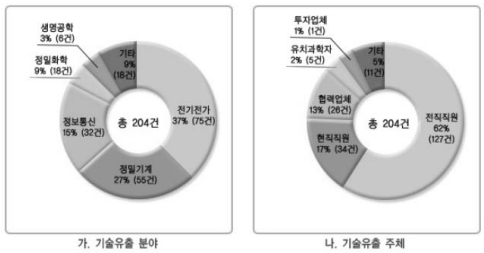
3.2 한국의 기술 유출 관련 통계 분석

2005년부터 2011년까지 한국에서 발생한 기술 유출 사례는 2005년 29건, 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건, 2010년 41건, 2011년 46건으로 총 264건이 발생하였다. 특히 매년 산업스파이로 인한 기술 유출이 증가추세에 있어 이에 대한 대비책이 시급한 것으로 드러났다.

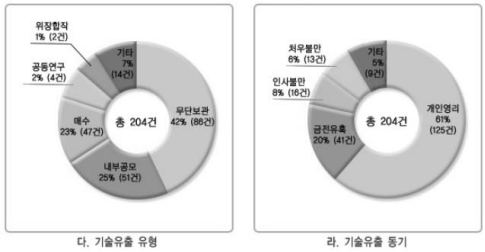


〔그림 2〕 핵심 기술 유출 연도별 현황〔2〕

기술 유출 분야에서는 전기 및 전자 분야가 37%를 차지했고, 정밀 기계 분야가 27%, 정보통신 분야가 15%로 그 뒤를 이었으며, 기술 유출 유형을 분석한 결과 무단보관으로 인한 기술 유출이 전체 42%, 내부 공모 25%, 매수 23%에 의한 것으로 드러났다. 기술을 유출한 동기는 개인영리를 위한 목적이 61%로 가장 높았다. 또한 기술 유출은 외부보다는 내부 직원에 의해서 이루어지고 있음을 확인해볼 수 있었다.



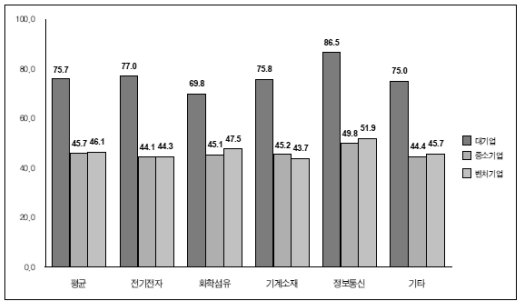
〔그림 3〕 핵심 기술 유출 분야 및 주체〔2〕



〔그림 4〕 핵심 기술 유출 유형과 동기〔2〕

3.3 산업기술 유출 방지 기업의 노력 현황 통계

2011년 산업기술 보호를 위한 실태조사 보고서에 따르면 전체 기업의 산업보안 역량 수준은 48.9점으로 취약한 수준으로 분석이 되었다. 또한 대기업의 보안 수준이 91.9점인데 비해서 60.9점에 머물고 있는 것으로 조사되어 중소기업에 대한 대책은 더 시급한 것으로 드러났다〔3〕.



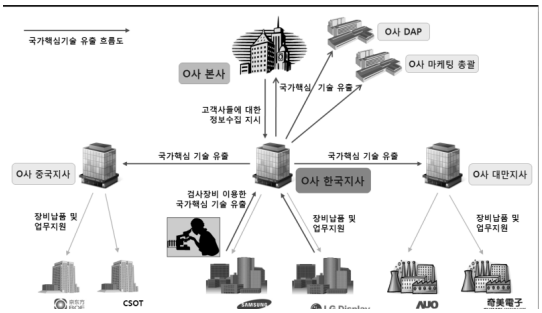
〔그림 5〕 업종별 기업유형별 산업보안 역량 점수

특히 중소기업의 경우 대기업에 비해 재정적으로 열악하기 때문에 이에 대해 시사하는 바는 크다고 할 수 있다.

IV. 한국 핵심 기술 사고 사례 및 법제도 현황

4.1 최근 기술 유출 대표 사고 사례 분석

서울중앙지검 첨단범죄수사 제1부(부장검사 김영종)는 국가정보원과 공조하여 국내 및 세계 최대의 디스플레이 제조 회사들인 S사 및 L사 보유하고 있는 핵심기술인 아몰레드 (AM-OLED) 기술을 신용카드형 USB 등에 담아 몰래 빼내 본사 및 해외 경쟁업체 담당 외국 직원에게 전달하는 등 해외로 유출시킨 협력업체 O社 한국지사 직원 3명을 산업기술의유출방지 및보호등에관한법률위반 등 혐의로 구속기소하는 등 직원 6명을 기소하고, O社 한국지사를 양벌규정에 의해 같은 죄로 기소하였다.



〔그림 6〕 대기업 보유 핵심 기술 유출 경로 현황 〔4〕

아몰레드 기술은 산업 기술의 유출 방지 및 보호에 관한 법률에 근거한 산업 발전법 제5조에 따라 지정된 첨단 국가핵심 산업기술이었으며, 기술개발 투자비만 S사는 약 1조 3,800억 원, L사는 약 1조 270억 원 소요되었다. 유출된 기술은 시장에 출시되지 아니한 S사와 L사의 55인치 TV용 대형 아몰레드 패널을 구성하는 레이어별 실물 회로도 이미지, 각 레이어별 구조가 담긴 회로도 등으로 S사와 L사의 극비 자료이자 핵심기술이었다. 외국 경쟁업체에 유출될 경우 국내 아몰레드 기술을 단기간에 따라 잡을 수 있을 정도의 중요한 기술로 막대한 국가적 손실로 이어지고, 세계 시장 판도를 뒤바꿀 수 있을 정도였다.

피고인들은 아몰레드 패널 생산현장에서 검사장비를 점검하면서 시장에 출시되지 아몰레드 패널의 레이어별 실물 회로도를 촬영 후 USB에 담아 무단 유출하였다. 실물 회로도는 기술이 집약되어 있어 회로도만 입수하면 경쟁업체에서 단기간에 기술격차를 줄일 수 있는 상황인 매우 큰 이슈의 사건이었다〔5〕.

4.2 국내 법제도 현황 분석 (과거)

4.2.1 부정경쟁방지 및 영업 비밀에 관한 법률 (2004년 7월)

이 법률은 국내에 널리 알려진 타인의 상표, 상호 등을 부정하게 사용하는 등의 부정 경쟁 행위와 타인의 영업 비밀을 침해하는 행위를 방지하여 건전한 거래 질서를 유지함에 의의가 있다. 특히 이 법률은 특히 침해자에 대한 형사 처벌을 강화했다는데 의의가 크다. 영업 비밀 주체를 해당 기업의 전, 현직 임직원으로부터 '누구든지'로 대상 범위를 확대하여 영업 비밀을 침해한자는 누구든지 처벌이 가능하도록 하였다. 또한 기술뿐만이 아닌 경영상 영업 비밀을 보호대상에 포함시켜, 형사적으로 보호해야 할 영업비밀의 범위를 확대하였고, 영업 비밀을 해외로 유출한 자에 대해서는 '부당이익의 최대 10배까지의 벌금'으로 부당이익을 환수할 수 있는 '부당이익 환수제'를 도입하였다. 이를 통해 경제적 목적으로 영업 비밀을 침해하는 자에 대한 목적을 차단에 제거하였다.

처벌과 관련한 규정을 살펴보면 친고죄를 폐지하여 영업비밀 침해자에 대한 고소 및 고발이 없더라도 처벌할 수 있도록 법률을 개정하였고, 영업비밀 침해에 대한 예비, 음모, 미수 행위도 처벌이 가능하도록 개정하여 영업 비밀을 침해한 개인은 물론이고, 조직(기업)도 함께 처벌할 수 있는 양벌 규정을 신설했다.

그러나 이 법률은 부정경쟁방지법은 정부에서 출연한 연구소 또는 대학 등에서 개발한 기술들이 해외로 유출될 경우 규제할 수가 없었다. 즉, 핵심기술 유출 방지에 대한 취약점을 가지고 있었다.

4.2.2 산업기술의 유출방지 및 보호에 관한 법률 (2007년 4월)

이 법은 핵심 기술을 수출 시에는 수출승인 및 사전 신고를 하도록 하는 내용을 골자로 하는 법이다. 따라서 이법은 산업기술 유출에 대한 보호체계를 종합적으로 마련하였다는데 의의가 있다.

기존 부정경쟁방지 및 영업 비밀에 관한 법률 개정안은 2000년도에 들어 국내에서 2가지 대표 합병 관련 이슈를 다루는데 한계를 드러냈다. 2000년도에 포드 자동차의 대우자동차 인수 시도 사례를 예를 들어보면 포드사는 막대한 정보를 입수만 하고 인수를 하지 않았다. 또한 2004년에는 중국 상하이 자동차가

쌍용 자동차를 인수하고, 이를 통한 완성차 제작 기술 및 하이브리드 카 정보를 유출했다는 의혹이 있었지만, 이 법률로는 해외 기업이 국내 자동차 산업 등 핵심 기술을 보유한 기업을 인수하거나, 합병 시에 핵심 기술을 획득하는 것을 규제하는데 한계가 있었다.

4.2.3 외국인투자촉진법 시행령 (2008년 2월)

산업기술의 유출방지 및 보호에 관한 법률은 기존 법제도에서 지적된 해외 기업의 국내 회사 인수 시 기술 유출 등의 법률적 한계를 보완할 필요로 제정되었다. 이 개정된 시행령은 M&A 발생 시 합법적으로 산업 기술 유출을 규율할 수 있도록 하고 있어서, 해외인수 또는 합병 시에 핵심기술이 유출되는 것을 방지하기 위해 활용되었다.

그러나 위의 시행령은 방위산업과 관련된 해외투자에 대해서만 규제가 가능했다. 「대외무역법」 및 「기술개발촉진법」 상의 전략물자 및 전략기술 등 '국가안보위해'를 발생시키는 핵심기술에 대한 외국인 투자만 대상으로 한다는데 한계가 존재하였다. 미국이나 일본의 경우 기간산업 및 인프라에 대한 외국인 투자 또는 경제의 원활한 운영에 현저한 악영향을 미치는 외국인 투자에 대해서도 사전심사를 할 수 있도록 한 것에 비하면 해당 법이 실제로 규제할 수 있는 범위는 매우 제한적이라고 할 수 있다[6].

4.3 산업기술 유출방지법 발의 (2011년 7월)(현재)

4.3.1 법률 발의 배경 및 의의

[표 4] 국내 산업 기술 유출 방지법 관련 개정 이력 분석'에서 언급한 것처럼 국내 기술 유출 방지 관련 법안이 가지고 있는 취약점은 M&A를 통한, 기술 유출 방어에 대한 한계와 방위산업 이외 투자 건에 대한 유출 대책이 미흡하고, 사전 심사 제도 관련 내용이 없어 규제 범위가 매우 제한적이라는 것이다.

기존 법률안으로는 앞에서 언급했던 2004년 중국 상하이자동차의 쌍용자동차를 인수 등 최근 핵심기술의 유출이 불법적인 방법 외에도 핵심기술을 보유한 국내기업과 국외 인수·합병 등을 통해 국가핵심기술을 간접적으로 이전받으려는 시도에 대한 방어 대책이 부족했다. 이에 따라 해외인수·합병 등을 통해 시도되는 기술 유출에 대해 규제할 수 있는 제도가 필요했다. 결국 핵심 기술에 대한 국가 차원의 정책 및 제도적인

[표 4] 국내 산업 기술 유출 방지법 관련 개정 이력 분석

법명	시기	특징	한계점
부정경쟁방지 및 영업비밀에 관한 법률 개정안	04년 7월	특허 침해자 형사 처벌 강화 친고죄를 폐지 (영업비밀 침해시 고소, 고발 없더라도 처벌 가능) 및 부당이익 최대 10배까지 환수	부에서 출연한 연구소 또는 대학 등에서 개발한 기술들이 해외로 유출될 경우 규제할 수 없음
산업기술 유출방지 및 보호 관한 법률	07년 4월	핵심 기술 수출시 사전 승인 제도	M&A 합병 통한 기술 유출 방어 한계
「외국인투자촉진법 시행령」	08년 2월	M&A 합병 시 기술 유출 대응 한계 일부 극복 (단, 방위산업에 관련한 투자에 한함)	방위 산업 이외 방어 대책 미흡 및 미국, 일본 등에 존재하는 사전 심사 내용 없어 실제 규제 범위 매우 제한

관리와 지원이 필요하게 되었고, 지난 2007년 4월 시행된 산기법이 5년 만에 개정되었다.

새로 개정된 법률로 인하여 기술 유출을 효과적으로 방지·차단할 수 있는 법적 수단 마련과 변화된 환경에 맞춘 위한 새로운 관리체계에 대한 개선이 반영되었고, 2011년 7월 국내 산업기술의 해외 유출을 막기 위해 '산업기술 유출 방지 및 보호에 관한 법률' 개정안이 발의되었다. 산기법의 법률' 개정은 핵심기술의 해외유출을 목적으로 한 외국인투자를 사전에 방지·차단할 수 있는 최소한의 법적 장치를 마련했다는데 큰 의의가 있다고 평가된다[7].

4.3.2 법률 주요 내용

첫째, 개정된 산기법 제 11조 (핵심기술의 수출 등)의 제 2항에 의거하면 '지식경제부장관은 제1항의 규정에 따른 승인신청에 대하여 핵심기술의 수출에 따른 국가안보 및 국민경제적 파급효과 등을 검토하여 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 승인할 수 있다'고 명기하고 있다. 외국인들이 투자를 통한 한국 내 핵심 기술의 유출에 대한 리스크를 사전 방지할 수 있을 것으로 기대된다.

이것은 기존 쌍용자동차를 인수하여 기술을 유출한 사례처럼 인수 및 합병에 따른 핵심 기술 유출이 국외로 유출 되는 등 국익에 반하는 경우를 고려한 것이다. 이에 따라 해외인수·합병 등에 따른 핵심기술의

유출이 국가안보 등에 심각한 영향을 줄 수 있다고 판단되는 경우 심의를 거쳐 중지·금지·원상회복 등의 조치를 취할 수 있게 되었다.

둘째, 개정된 산기법 제 14조 2(산업기술 침해 행위에 대한 금지 청구권 등)에 의하면 '① 대상기관은 산업기술 침해행위를 하거나 하려는 자에 대하여 그 행위에 의하여 영업상의 이익이 침해되거나 침해될 우려가 있는 경우에는 법원에 그 행위의 금지 또는 예방을 청구할 수 있다. ② 대상기관이 제1항에 따른 청구를 할 때에는 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거, 그 밖에 침해행위의 금지 또는 예방을 위하여 필요한 조치를 함께 청구할 수 있다.'라고 명기되어 있다. 즉, 산업기술 침해행위에 대한 금지청구권 집행이 가능해져, 산업기술 침해행위를 하거나 하려는 자에 대해, 그 행위에 의하여 영업상의 이익이 침해되거나 침해될 우려가 있는 경우 법원에 그 행위의 금지 또는 예방을 청구할 수 있다.

셋째, 제 2조 (정의) 1항에 명기된 내용을 살펴보면 산업기술의 정의를 각 법률 또는 해당 법률에서 위임한 명령(대통령령·총리령·부령에 한정한다. 이하 이 조에서 같다)에 따라 지정·고시·공고·인증하는 다음 각 목의 어느 하나에 해당하는 다음을 기술을 명확히 명시하고 있다. 따라서 보다 많은 중요 기술을 핵심기술로 보호할 수 있게 되는 실효성을 확보했다.

넷째, 산기법 제 7조 (산업기술보호위원회의 설치 등)에서는 산업기술보호위원회의 기능 및 권한 범위를 명시하고 있다. 현행 산업기술보호위원회의 심의대상 중 시행계획의 수립·시행, 산업기술 보호지침의 제정 등 일반안건을 제외함으로써 위원회가 종합계획의 수립, 핵심기술의 지정 등 산업기술보호에 관한 중요정책 심의에 집중하도록 그 기능 및 권한 범위를 조정하였다. 다섯째, 산기법 제 15조 (산업기술침해신고 등)에 의거하면 산업기술 유출 및 침해행위가 발생한 경우 기업 등의 요청이 없더라도 지경부 장관 및 정보수사기관 장이 직권으로 기술유출 방지에 필요한 방어적 긴급조치를 할 수 있도록 하였다.

〔표 5〕 부정경쟁방지법과 산업기술 유출방지법 비교

구분	부경법	산기법
의의	영업비밀의 침해행위에 대하여 형사처벌과 피해자에 대한 구제수단을 규정하고 있어 사후조치적임	IT분야 기술 해외유출 급증과 경제의 소프트화에 따른 국제적인 기술거래 등 종합적 대응
적용 대상	주로 일반기업 대상으로 적용	기업 뿐 아니라 국가, 연구기관, 대학 등 산업기술의 개발·보급 및 활용 관련되는 모든 종사자들의 산업 기술 유출 행위 대상
처벌 관련	부경법이 영업 비밀 침해 행위에 대한 민사적 구제 수단을 규정	형사 처벌 + 별도의 민사적 구적 구제는 기존과 같이 부경법을 근거로 이루어질 것 전망

V. 외국의 기술 유출 사례 및 법제도 분석

국내 법제도의 취약한 부분을 분석하고 이를 반영하기 위해서는 외국의 기술 유출 관련 방지 제도에 대해서 분석해보는 것이 중요할 것이다. 여기서는 미국, 일본 등 선진국의 기술 유출 제도를 분석해보고자 한다.

5.1 미국의 기술유출 방지 법제도 분석

5.1.1 엑슨-플로리오법

엑슨-플로리오법은 1986년 캘리포니아에 있는 페어차일드사(Fairchild Semiconductor)'가 일본 후지츠사(Fujitsu Ltd.)에 매입되려는 문제를 계기로 제정되었다. 페어차일드사가 가진 첨담 기술이 국외로 이전시 국가안보를 손상시킬 위험이 있고, 국방부장관 및 상무부 장관이 반대했지만, 당시 독과점 금지법 및 기타 관련 법으로는 이러한 매수를 반대할 수 있는 합법적인 수단은 없었다. 따라서 후지츠사의 페어차일드사에 대한 인수에 대응하기는 역부족이었다. 다행히도 후지츠사는 부정적 평판을 염려하여, 페어차일드사 인수를 포기했지만, 이 사건을 통해서 미국은 외국 기업이 미국 기업을 인수하려고 할 때 이를 저지할 수 있는 권한이 명시되어 있지 않다는 것을 큰 문제로 인식하게 되었고, 미국 대통령이 인수를 중단할 수 있는 권한의 부여가 필요하다는 것을 깨닫게 된다.

1988년 민주당의 James Exon 상원 의원과 공화당의 James Florio 하원 의원이 외국인투자와 관련된 포괄적 조사 및 규제를 규정한 엑슨-플로리오법(Exon-Florio Act)을 제안하였다. 이 법의 핵심 요지는 국가안보를 위해서 미국 기업에 대한 외국인의 지배를 방지하는데 그 목적이 있었다. 이 법안은 "1988년 종합무역법"(the Omnibus Trade and Competitiveness Act of 1988)에 5021조로 편입

되었다. 이후 엑슨-플로리오법의 제정에 따라 "방위생산법"(the Defense Production Act of 1950) 제721조도 개정되었다. 엑슨-플로리오법 저촉 여부는 〔표 8〕 과 같이 재무부, 국무부, 상무부, 국방부, 국토안보부 장관과 미국무역대표부(USTR) 대표, 경제자문위원회 의장, 검찰총장, 기획예산실 실장, 과학기술정책실 실장, 대통령 국가안보보좌관 및 경제정책보좌관으로 구성되는 CFIUS가 조사한다.

재무부장관이 의장을 맡는 위원회는 당초 외국인투자와 관련된 부처간 정책 조정을 위해 포드 대통령 재임기간인 1975년에 설치되었으나, 레이건 대통 령 재임기간인 1988년 엑슨-플로리오법 제정을 통해 심사권한이 확대, 강화된 셈이다〔8〕.

심사기구인 'CFIUS'는 미국 재무부 장관과 국무부 장관, 상무부 장관, 법무부 장관, 미국 무역대표부, 대통령 경제자문위원회, 미국중앙정보국(CIA) 등으로 구성된다. CFIUS는 일단 문제가 된다고 판단되면 30일간의 검토를 실시한다. 이후 45일간 조사 및 실사를 거친 후 문제가 된다는 최종 판단이 서면 대통령에 공고한다. 대통령은 15일내 CFIUS의 보고 내용에 대해 검토, 인수허용에 대한 입장을 표명한다〔9〕.

이 제도는 심사방식 등 심사기준이 없고 인수대상이 된 자국 기업의 신고를 토대로 조사 및 실사를 하기 때문에 외국기업에게 유리한 결론이 나오기 힘들다는 게 전문가들의 설명이다. 이 때문에 외국인에 의한 적대적 M&A 위협을 방어하는 강력한 무기로 그 역할을 하고 있다는 평가다. 사후적으로 투자 철회 판정을 받을 경우 막대한 피해를 입게 되기 때문에 외국인 인수자들이 자발적으로 인수를 철회할 수 밖에 없는 실정이다. 또 심사개시가 결정될 경우 법적 절차에 따른 시간 지연과 정보제출 등의 부담 때문에 인수를 포기하는 사례도 발생한다. 가장 좋은 사례는 홍콩 허치슨-암포와 사의 사례로 이 회사는 미국의 통신기술업체인 글로벌 크로싱사 인수를 추진했으나 미국이 심사개시를 결정함에 따라 인수계획이 백지화 되었다.

5.1.2 외국인투자 및 국가안보에 관한 법률 (Foreign Investment and National Security Act of 2007」 (FINSA)

이 법은 미국의 안보를 위협하는 특정한 거래를 지정하여 이에 대한 규제와 규제 절차 등에 관하여 규정하는 법이다. 이 법은 다음과 같은 조항들을 포함하고 있다. 첫째, 미국의 안보증진을 위하여 특정 거래를 지정하여 특정거래의 당사자가 그 내용을 통지하도록 하고 있고, 거래의 내용을 검토와 조사 하여 미국의 국가 안보에 위협이 되는 요인이 있는지를 검토하는데 여기에 관한 요건을 규정하고 있다. 둘째, 미국에서 외국인이 투자하는 경우 거래에 관한 규제 등을 행할 위원회의 설립에 관하여서 규정한다. 또한 외국인과의 특정거래가 미국의 국가 안보를 위협하는 경우에 이를 경감하는 등의 조치를 위해 당사자와 협상하는 절차와, 당사자와 협상 이후 그리고 거래내용의 검토와 조사 이후의 이행 등을 규정하는 방법에 관하여 규정하고 있다. 셋째, 미국의 국가안보를 위하여 대통령만이 할 수 있는 특별한 조치들을 규정하고 있다. 마지막으로 전체 규제에 대한 의회의 감독을 규정하고 있으며, 의회의 감독권한은 이 법에 의해서 이전의 방산물 생산에 관한 법에서보다 더 강화되어 미국 국가 안보를 위한 위원회는 국회에 연간 보고서를 제출해야 하며, 이러한 내용은 기밀로서 유지되어야 함을 이 법에서 규정하고 있다.

요약하자면 FINSA는 엑슨-플로리오법에서 보다 그 대상을 확대시켰고 또한 보다 강력한 통제수단을 정부에 부여하고 있다. 미국의 엑슨-플로리오법과 이를 수정한 FINSA는 모두 국가안보를 해칠 우려가 있는 외국인의 인수・합병 등 해외투자에 대한 사전규제를 주된 내용으로 하고 있다. 반면 한국의 산업기술유출방지법과 비교하면 핵심기술의 해외 매각 및 기술이전에 대한 사전규제를 골자로 하고 있다는 점에서 근본적인 차이가 있다.

5.2 미국의 기술 유출 판례 동향

2011년 회계연도에 법무부 (DOJ) 및 미 연방수사국(FBI)의 경제 스파이 및 영업비밀 절도 관련 수사는 2010년 회계연도에 비해 약 29% 증가한 것으로 드러났다〔10〕.

미국의 주요 기업들을 대상으로 한 외국의 경제정보 수집활동 및 산업 스파이 활동이 점차 가속화되고 있는 것이다. 외국 정부 소유의 기업들과 제휴하고 있는 미국 기업들의 외국 경쟁기업들은 영업비밀이나 지식 재산을 훔치기 위한 노력을 점차 증대시키고 있다. 최근의 연방수사 및 기소에 따른 증거들은 중국 소재 기업들을 대신해 경제 스파이 활동을 하거나 영업 비밀을 훔치는 경우가 증가하고 있다는 것을 보여준다. 특히, 중국 정보기관 및 민간 기업들은 회사 네트워크에 접근하여 이동식 미디어 장치나 이메일을 이용해

영업 비밀을 훔칠 수 있는 중국계 미국인이나 중국과 연계가 있는 가족들을 가진 사람들을 이용하기 위해 빈번하게 노력하고 있다. 실제로 2010년 회계 연도에 경제 스파이 법(Economic Espionage Act) 제 1831조 및 1832조를 근거로 법원이 심리한 7건의 사건 중 6건이 중국과 관련이 있다. 미국 기업 및 사이버 보안 전문가들은 중국에 인터넷 접속주소(IP)를 둔 공격자 들이 컴퓨터 네트워크를 침해했다고 보고하였고, 민간부문 전문가는 이를 "집요하게 계속되는 고도의 공격(advanced persistent threats)"이라고 지칭한 것은 지속적인 중국에 대한 경각심을 높여야 된다는 것을 시사하고 있다. 여기서는 실제 미국에서 발생한 몇 가지 대표적인 기술 유출 사례를 살펴보고자 한다.

5.2.1 Former Dow Chemical Co. employeecharged with economice spionage'(2011년 10월)

2011년 10월, Cargill 및 Dow Chemical에서 근무했던 전직 직원 Kexue Huang은 경제 스파이 범죄를 저지른데 대해 유죄 판결을 받았다. Huang은 이 두 개 기업들로부터 영업비밀을 유출하여 중국 정부를 대신해서 유기 살충제를 개발하고 있는 중국 대학에 넘겼다. Huang은 Cargill에서는 생명공학자로 근무했으며 Dow Chemical에서는 유기살충제 연구원으로 근무했다. Kexue Huang의 영업비밀 절도로 인해 이 두 개 기업들에서 발생한 경제적 손실은 7백 만 달러 이상이었다. 연방수사국(FBI)과 사이버범죄 수사국(CCIPS), 인디아나주 검찰청 및 미네소타주 검찰청이 실시한 수개월에 걸친 수사 끝에 연방 법원은 12월에 Huang에게 법정 최고형인 87개월의 징역형을 선고했다

5.2.2 Yu Xiangdong, a former Ford Motor engineer, was arrested on Oct (2009년 10월)

Yu는 Ford Motor Company의 전직 직원으로서 외장 하드 드라이브를 이용해 4,000부가 넘는 포드의 기밀문건을 복사하여 중국으로 가져가 Ford의 경쟁업체인 Beijing Automotive Company에 넘기고 그 기업에서 근무하기 시작했다. 미국에서 체포된 Yu의 사무용 컴퓨터를 조사한 결과 Ford의 영업기밀 41건이 발견되었는데, 이 영업 기밀은 Yu가 Beijing Automotive Company에서 근무하는 동안 Ford에 접속해서 유출한 것들이었다. Ford는 이 영업비밀 손실을 5천만 달러로 평가하였다. 2011년도 피의자 Xiang Dong Yu은 징역 70개월 및 12,500불의 벌금형을 선고받았다[11].

5.2.3 Former Technical Director of Wheeling Paint Company Indicted for Alleged Theft of Trade Secrets Before Joining Competitor (U.S. v. David Yen Lee, Northern District of Illinois (2009년 6월)

대표적 Wheeling 제조회사인 Valspar Corp.의 직원이었던 David Yen Lee(52)는 경제스파이 법을 위반하고, 영업 비밀을 훔친 혐의로 연방배심원에 의해 기소되었다. 피의자는 2006부터 Valspar사에서 근무하기 시작하였고 회사로부터 지적재산보호의무와 관련하여 지시를 받았는데, 2008년9월에 2009년 2월 사이에 피의자는 중국 상하이에 있는 페인트 관련 기술개발, 제조회사인 Nippon Paint사로부터 스카우트 제의를 받아 2009년 4월부터 근무를 하기로 협상하였다. 2008년11월에서 2009년 3월 사이에피의자는 Valspar사의 영업비밀인기술관련문서와자료를내부보안네트워크에접속하여 다운로드 받았다. 피의자는 2010년 10개월의 징역형을 선고받았으며, 약 3000만 불의 벌금형을 선고받았다.

5.3. 일본의 기술유출 방지 법제도 분석

5.3.1 부정 경쟁 방지법

일본의 경우 부정 경쟁 방지법을 통해 영업 비밀을 보호하고 있으며, 영업 비밀의 보호요건, 침해 태양, 민사적 구제 수단 등에 대한 내용은 우리 법과 유사하다. 이법은 영업 비밀을 보호하기 위해 영업비밀의 보호요건, 침해 행태, 민사적 구제수단 등이 포함된 법이며, 미국, 독일 등 외국의 영업비밀보호 강화 추세에 따라 일본도 법률을 개정하게 되었고, 2005년 6월 「부정경쟁방지법」을 개정하여 2005년 11월부터 산업스파이에 대한 형사 처벌 강화, 영업비밀 침해죄 형벌수준 강화(10년 이하의 징역 또는 천만엔 이하의 벌금), 영업비밀 국외사용 및 공개행위 처벌, 퇴직자에 의한 영업 비밀의 사용·공개행위 처벌, 법인도 처벌 가능토록 규정하고 있다.

5.3.2 영업 비밀 관리 지침

일본 경제 산업성은 2003년 1월 각 기업이 실무적으로 활용할 수 있도록「영업 비밀 관리지침」을 제정하였으며,2005년 6월 부정 경쟁 방지법의 개정에 따라 2005년 10월 '영업 비밀 관리지침'을 개정하였다. '영업비밀 관리 지침'은 기업이 자사의 영업 비밀을 보호하고 타사의 영업 비밀을 침해하지 않기 위한 실질적인 관리 방침을 제시하고, 기업의 영업비밀이 법률상의 보호를 받기 위해 필요한 관리수준과 영업비밀 취급시의 유의 사항 등을 설명하고 있다. 이지침은 영업 비밀의 바람직한 관리 기준을 4가지 측면에서 제시하고 있다.

첫째, 물리적·기술적 관리 측면의 기준을 살펴보면, 기록 매체 관리(물리적 관리) : 정보구분과 표시, 접속 권한자 특정, 매체의 보관, 반출제한, 폐기, 시설 등의 관리 기준 항목을 제시하고 있다. 둘째, 정보자체의 관리(기술적 관리)에서는 매뉴얼 등의 설정, 접속 및 접속 관리자의 특정, 외부 침입에 대한 방어, 데이터 소거·폐기에 대해서 제시하고 있다. 셋째, 인적 관리 영업 비밀 취급에 관한 규정 등에 대해 일상적으로 교육·연수실시 임직원, 파견사원, 퇴직자, 전직자, 거래처 등 상대방에 따른 적절한 법적 관리, 기업과 종업원 및 퇴직자와의 적절한 비밀 유지 계약을 언급하고 있다. 마지막으로 조직적 관리 측면에서는 물리적·기술적 관리 및 인적관리를 효율적으로 추진함으로써 문제 발생시 적절하게 대응하는 가를 제시하고 있다[12].

5.3.3 기술 유출 방지 지침

일본 경제 산업성은 2003년 3월 해외에서 활동하는 기업들의 의도하지 않은 기술유출을 방지하기 위하여 기업이 실무적으로 활용할 수 있는 「기술유출방지지침」을 제정하였으며, 지침 내 포함되어 있는 각 조항을 요약하면 다음과 같다. 이 지침은 제 2장에서는 의도하지 않은 기술 유출이 발생하는 주요 유형을 기술라이선스, 기술원조와 관련한 기술 유출 사례부터 사람을 통한 기술 유출 사례까지 7가지 유형으로 구분하여 설명하고 있다. 제 3장에서는 기업이 참고해야 할 대책을 다음 표와 같이 설명하고 있다. 이 지침은 의도하지 않은 기술유출이 발생하는 주요 유형을 설명하고 있다.

5.4 독일 기술유출 방지 법제도 분석

5.4.1 독일 불공정 경쟁 방지법 (UWG)

독일에서는 1909년에 제정된 이래 독일의 불공정 경쟁 방지법(UWG)은 1932년에 개정되어 영업비밀을 보호하고 있다. 세계에서 가장 엄격한 법 중의 하나로 알려져 있는 법이나, 이에 근거한 영업비밀보호 조항은 근로계약을 맺고 있는 자의 누설행위만을 처벌하도록 하고 있었고, 제3자, 특히 산업스파이의 영업비밀 탐지행위 자체는 처벌되지 않았다.

오늘날 독일부정경쟁방지법 제17조, 제18조, 제20조는 영업비밀의 침해행위에 대한 형사적 처벌을 규정하고 있으며, 제19조는 민사적 손해배상청구권을 규정하고 있다. UWG 제17조 제1항은 "사업체의 피용자, 근로자 또는 견습생으로서, 고용관계(Dienstverhältnis)에 기하여 위탁받거나 접근하게 된 영업상 또는 경영상의 비밀(Geschäfts- oder Betriebsgeheimnis)을, 고용관계의 계속 중에 권한 없이(unbefugt) 경쟁의 목적으로, 자신의 이익을 위해 또는 제3자를 위하여, 또는 사업주에게 손해를 가할 목적으로 타인에게 누설(mitteilt)한 자는 3년 이하의 자유형 또는 벌금형에 처한다."고 규정하고 있다. 행위자가 누설 시에 당해 비밀이 외국에서 이용된다는 사실을 알고 있거나, 또는 행위자 스스로 외국에서 이용한 경우에는 5년 이하의 자유형 또는 벌금형에 처할 수 있다고 규정하고 있다.

5.5 중국의 기술 유출 방지 법제도 분석

중국은 기술 유출 방지와 관련하여 2008년 6월 5일에 《국가지식재산권전략요강》 발표하는 등 2011년 상반기까지, 지식재산권관련 법률법규 76개 제정, 주요한 정책조치 176개 실시, 전문적인 단속활동 54번 실시, 동시에 지식재산권관련 홍보활동 및 대외교류 활동을 다량 실행하고 있다. 중국은 자국의 기술유출 방지와 관련하여 '반부정당 경쟁법'과 '국가 기밀법'으로 크게 두 가지의 법률로 대응하고 있다.

5.5.1 중화 인민 공화국 반부정당 경쟁법

중국에서는 기술 유출에 대한 규제는 부정 경쟁 방지법에 의해서 이루어지고 있다. 이 법은 시장경제의 건전한 발전 및 공정한 경쟁을 보호하고, 소비자를 보

호하기 위하여 1993년 9월 2일 제정되고, 1993년 12월부터 시행되었다. 해당 법의 보호대상은 기술상, 경영상의 정보가 대상이 되며, 피해기업의 신고가 없이도 조사 및 처벌할 수 있도록 소추 요건을 완화하여 기술 보호를 강화하였다.

5.5.2 중국 국가 기밀법

중국 정부는 중국의 국가 기밀법을 개정했다. 2009년도 원자바오(溫家寶) 총리의 '정부 공작보고서'를 포함한 중국의 기밀문서들이 수록된 컴퓨터가 대만 출신으로 추정되는 해커에 의해 해킹당한 사건이 발생한 이후 국가기밀법의 내용을 확대해 인터넷과 통신 회사들도 고객들에 관한 정보를 당국에 제출하도록 의무화했다. 중국 전국인민대표대회 법률위원회가 2010년 개정한 국가 기밀법은 인터넷과 공공정보 망을 통해 전달되는 정보에 국가기밀이 담겨 있을 경우 운영자는 정보 전달을 즉각 중단하고 이를 관계 당국에 보고해야 하며 필요할 경우 조사에 응해야 한다는 내용을 담고 있다[13].

5.6 주요 국가의 제도 분석 및 시사점

주요 국가의 제도를 통한 시사점을 분석한 도표는 〔표 6〕과 같다. 처벌 규정 및 시사점을 통해 국내 법 제도도 처벌 수위에 대한 고민이 필요할 것이다.

VI. 핵심 기술 관리 체계 수립을 위한 전문 인력 양성 등 교육 제도 개선 제안

6.1. 전문 인력 양성 프로그램 취약점 분석 및 발전 방향 제안

6.1.1 대학 및 민간 인력 양성 프로그램 취약점

첫째, 국내 주요 대학과 대학원의 정보보안학과 및 대학원의 이수 교과목을 각 대학의 홈페이지 교육 과목 현황을 확인해 보았다. 아래 〔표 7〕을 보면 국내 주요 4년제 대학 13개 대학의 정보보호관련 학과의 최종 업데이트된 홈페이지를 통해 전국 각 대학의 교

〔표 6〕 주요 국가 제도 분석 및 시사점

국가	법령명	제정목적	처벌규정	시사점
미국	통일영업비밀보호법 (UTSA)	영업비밀 보호에 관한 각주 판례의 불균형 및 보호 수준 차이 시정을 위해 제정	징벌적 손해 배상을 채택하여 고의 또는 악의에 의한 침해행위는 손해배상의 2배까지 청구가능하며, 별도 형사적 처벌 규정 없음	영업비밀 유출 피해시 금지 청구권과 손해 배상 청구권 인정
	산업스파이방지법(EEA)	산업스파이 행위를 형사 범죄로 규정하여 정보기관이 직접 수사할 수 있는 근거 마련	* 산업스파이 죄 개인 15년 이하 징역 또는 50만불 이하 벌금 및 기업 1천만불 이하 벌금 * 영업비밀 절도 (개인) 10년 이하 징역 또는 벌금 (기업) 500만불 이하 벌금	외국정부, 기관 등과 연계된 영업비밀 유출 행위에 대한 가중 처벌
일본	부정경쟁방지법	산업스파이에 대한 형사 처벌 강화, 영업비밀 침해죄 형벌수준 강화하기 위해 제정	5년 이하의 징역 또는 500만엔 이하벌금	자국의 첨단기술 유출에 대한 심각성을 인지하고 한국, 미국, 독일 등 외국의 영업 비밀 보호 강화 추세에 따라 2005년 6월 「부정경쟁방지법」을 개정, 2005 년 11월부터 산업스파이에 대한 형사 처벌을 강화함
독일	불공정경쟁방지법(UWG)	특히 산업스파이의 영업 비밀 탐지행위 자체는 처벌	3년 이하 징역 또는 벌금 부과 국외 유출시 5년이하 징역	한국 '부정경쟁방지법'과 유사하나 친고죄 (단, 공공 이익 위해 필요하다고 생각되는 경우만 고소 없이 기소 가능) 미수범은 처벌 가능하지만, 예비,음모자는 처벌 불가함

과 과정을 직접 분석해 보았다. 그 결과 주요 대학 중 고려대학교, 경기대학교, 서울여자 대학교에서만 산업보안과 관련된 이론 교과 과정이 있는 것으로 확인되었고, 나머지 학교는 산업보안과 관련한 이론을 다루지 않는 것으로 조사되었다. 조사과정에서는 정보보호학과의 일부인 사이버 경찰 관련 학과는 제외하였다. 정보보호를 전문적으로 공부할 수 있는 주요 대학 중에서 고려대 등 4개 대학만이 산업 보안과 관련된 이론을 다루고 있다는 것은 시사하는 바가 매우 크다.

둘째, 민간의 경우 정보보안과 관련하여 진행되었던 민간 자격증인 CPPG (개인정보 관리사)의 경우에도 국가 공인으로 전환이 되었지만, 기존 취득자에 대한 자동 전환이 불가한 문제점이 있었다. 최근에 정보보안 기사 등의 자격증이 추가되었지만, 민간차원에서 진행되는 산업보안 전문 자격 등을 국가차원에서 관리할 필요성이 있다.

6.1.2 인력 양성 프로그램 발전 제안

첫째, 개인정보 유출 사고 등이 지속적으로 발생함에 따라 사내 보안 조직의 주요 업무 자체가 개인정보를 보호하는 기술적 관리적 인력에 치중되어 있는 것이 현실이다. 대학 교육도 이 부분에 초점이 맞추어져 있는 것이 사실이다. 그러나 개인정보 및 정보보안은 물론 핵심기술의 보호까지 커버할 수 있는 전문가를 양성하고, 기업 내 전문 인력 공급을 위해 대학 및 대학원 등에서 지속적으로 전문가를 양성할 수 있는 인력 육성에 대한 제도적 지원에 대한 고민이 필요한 시점으로 보인다. 특히 향후 산업보안 전문가의 양성이 필요한 이 시점에서 각 대학 및 정부 차원의 관심이 더욱 필요하다고 본다.

〔표 7〕 각 정보보호 학과 산업보안 교과 과정 분석

학교	산업보안교과 포함 여부	비고 (교과목명)
고려대학교	O	산업보안 특론
경기대학교	O	산업보안
서울여자대학교	O	정보보호산업 기술최신동향
숭실대학교	O	
세종대학교	X	
순천향대학교	X	
대전대학교	X	
건양대학교	X	
우석대학교	X	
호서대학교	X	
중부대학교	X	
영동대학교	X	
동명대학교	X	

둘째, 전문 자격 프로그램의 국가 통합 관리 필요하다. 우선 민간 차원에서 진행 중인 산업보안 관리사를 국가 공인 수준으로의 격상을 제안하고자 한다. 따라서 산업보안 관리사는 개인정보관리사와 유사한 절차를 밟지 않기 위해서라도 시행 초기 적극적인 국가 공인 제도에 대한 검토가 필요할 것으로 보인다.

6.2 기존 ISMS 인력 POOL 활용 제안

6.2.1 기존 ISMS 인력 구성의 한계

앞의 통제항목 검토에서도 살펴본 것처럼 일반적으로 ISMS 등 정보보호 관리 체계는 핵심 기술 보호에 필요한 물리적, 기술적, 관리적 대책이 기본적으로 포함되어 있다. 그럼에도 불구하고 ISMS 등의 인증을 받은 기업의 핵심 기술 유출 사고가 우려되는 것은 기존 인증 체계의 한계를 말해주고 있는 것이다. 실제로 5명 정도의 인증심사원으로 구성되는 심사팀이 ISMS 심사를 진행시 해당 기업의 정보자산은 개인정보 등에 보다 치중해서 심사를 하고 있고, 핵심 기술 보호 등에 대한 전문 인력 배정은 쉽지 않은 것이 현실이다.

6.2.2 핵심 기술 전문 인력 활용 제안 및 기대

핵심기술을 보유한 사업체 등이 ISMS 등과 같은 인증 심사의 최초 또는 사후 심사를 받을시 기존 인증 심사원의 POOL에 핵심 기술과 관련한 심사 인원이 추가되어 심사를 받는다면 기업 또는 행정적인 측면에서도 시간과 예산의 낭비를 막을 수 있을 것으로 예상된다. 핵심기술 관리 체계 인증 등의 활성화를 위한 전문 인력의 확보와 운영 방안을 제안하는 바이다. 다시 말해, 핵심 기술 보호를 위한 핵심 기술 관리 체계의 운영주체는 ISMS 등 인증 심사시 핵심 기술 보호에 대해서 전담할 수 있는 인력을 배정 등을 협의했으면 한다.

아래 〔표 8〕은 산업기술 보호 협회에서 진행하고 있는 인력 양성 프로그램 현황을 정리하였다. 이와는 별도로 핵심 기술 관리 체계 수립을 위하여 KISA의

ISMS 또는 PIMS 인증 심사원과 유사한 전문 인력의 양성과 인재 POOL 확보를 제안하는 바이다.

그러나 기업의 입장에서는 활성화된 기존 ISMS 등에 핵심 기술 보호를 위한 노력까지 수행한다는 것은 적지 않은 부담인 것이 현실이다. 따라서 핵심 기술 관리 체계 인증 등을 부여받은 기업들이 정부차원에서 취득자에게 다양한 취득 혜택을 줄 수 있는 추가적인 연구 방안 등이 필요하다. 예를 들어 정책 및 제도 개선 등을 통해 핵심 기술 유출 방지를 위해서 노력하는 업체에 대해서는 각종 정부 사업시 가산점을 주는 것도 활성화를 할 수 있는 방안을 고려해볼 수 있을 것이다. 이렇게 함으로써 기업 내 핵심 기술 관리 내재화가 이루어질 것으로 기대된다.

〔표 8〕 산업기술보호 협회 진행 인력 양성 프로그램

현황	진행기관
2010년 11월13일 제 1회 산업보안 관리사 1회 시험 (민간) 2012년 9월 현재 제 3회 시험	산업기술 보호협회
산업보안 내부 진단 전문가 양성 교육 과정 진행 (2012년 6월, 9월)	
산업보안 내부 강사 양성 과정 (2012년 5월)	
차세대 CSO 양성과정 (2011년 7월, 2012년 7월)	

VII. 핵심 기술 관리 체계 통제 항목 수립을 위한 기존 ISMS 보완 및 개선 제안

7.1 핵심 기술 보호를 위한 기존 관리 체계 한계

앞에서 잠시 언급한 것처럼 최근 제도적으로 성공했다고 평가되고 있는 정보통신망법의 경우에는 2008년도 6월에 일부 개정되어 2012년 8월 18일까지 보완과 개정이 지속적으로 이루어졌다. 또한 행정기관의 고시 및 해설서 등을 통해 기업들이 어떤 기술적, 관리적 보호조치를 해야 하는지, 각 법률 조항에 대한 실천사항을 보다 쉽게 이해 할수 있도록 명확히 설명하고 있다. 기업들은 관련 법률 준수를 위해 ISMS 등의 인증 제도를 자발적으로 도입 및 운영하고 있고, 금년부터는 대상 기업의 ISMS를 의무화는 등의 노력을 기울이고 있다. 이는 법률 준수를 위한 준거성 측면에서 많은 기여를 하고 있다고 볼 수 있다.

여기서 흥미로운 것은 ISMS는 '개인정보'라는 특정한 자산을 보호하기 위해서 수립된 것이 아니라, 정보보안의 3요소인 기밀성(C), 무결성(I), 가용성(A)를 지킬 수 있도록 구성된 정보보호 관리 체계이다. 따라서 ISMS가 성공적으로 구축된 기업이라면 정보보안의 3요소 중 기밀성이 지켜져야 한다고 말할 수 있다. 다시 말해서 ISMS 등의 구축은 핵심 기술과 관련한 사고도 방지될 수 있는 체계가 함께 구축되어야 한다는 논리가 생성되어야 한다.

그러나 최근 사고가 일어났던 S사 및 L사 등 국내 유수의 대기업들은 ISMS 등 체계가 도입되어 있음에도 불구하고 사고가 발생하였다. 이는 정보자산의 기밀성, 무결성, 가용성의 관리 체계의 수립과 운영을 인증한다는 ISMS(정보보호 관리체계)가 기업의 기밀성, 특히 핵심 기술이라는 특정 자산의 보호를 위한 운영 관리 체계의 검증에 미흡한 부분이 있는 것은 아닌가라는 시사점과 의문점을 함께 던져주고 있다고 볼 수 있다. 다시 말해 ISMS에서 요구하는 정보자산이란 기업의 물리적, 논리적인 자산 등 기업이 보호해야 될 핵심 기술 등도 포함하고 있음에도 불구하고, 정보통신망법 등에서 요구하는 개인정보 등에 치중되어 점검이 이루어진 부분은 기존 정보보호 관리 체계의 미흡한 부분이라고 판단된다.

이에 따라 본 논문에서는 기업의 핵심 기술 관리 체계를 수립하고 이를 검증하기 위해서는 기존의 ISMS 등 검증된 방법론을 대상으로 기존 통제 항목 등의 미흡점을 보완하거나, 핵심 기술에 치중한 새로운 통제 항목 등의 추가 설계를 한다면, 기존 활성화된 제도를 활용할 수 있다는 가정을 하였다. 이를 위해 성공한 인증제도인 ISMS를 기반으로 핵심 기술 관리 체계를 수립하고, 운영할 수 있는 도메인과 통제 항목의 개선의 제안이 필요하다.

7.2 핵심 기술 관리 체계 수립 위한 통제 항목 모델링 방법론

이에 따라 본 논문에서는 기존 ISMS 통제 항목을 응용하여 핵심 기술 관리 체계를 수립할 수 있는 개선 및 보완된 통제 항목 모델링 방안에 대해서 고민해보고자 한다. 기존 ISMS 각 도메인의 통제 항목의 내용을 바탕으로 핵심 기술 유출 방지라는 추가적인 목적을 달성하기 위해서 핵심기술 관리 체계에서 고려되어야 할 가장 중요한 Factor를 본 논문에서는 2가지로 가정하였다. 먼저, 기존 정보보호 관리 체계에서 정의한 정보자산의 3요소 중 기밀성(Confidenti-

ality)을 가중치 factor로 정의하였다. 또한, 핵심 기술이라는 정보자산의 '유출'을 예방하는데 초점을 맞추기 위해서 사전 예방 활동을 또 다른 가중치 factor로 정의하였다.

2가지 가중치 factor를 활용하여 각 통제 항목의 정보자산의 기밀성 및 기밀 유출 등의 사전 예방 활동에 대한 밀접도 분석 후 가중치를 부여하는 과정은 다음과 같다. 첫째, "기밀성" 및 "사전 예방 활동"에 대한 각각의 가중치를 〔표 9〕과 같이 기준을 수립하였다. 둘째, 기존 ISMS 통제 항목 요소를 열거 후 해당 항목에 기밀성 관련 밀접도와 사전예방 활동 밀접도에 따른 가중치를 부여해준다. 셋째, 해당 통제 항목이 핵심 기술 관리 체계의 통제 항목으로 활용될 수 있는가를 판단하기 위해 각 가중치를 합산한다. 넷째, 가중치 합산 값에 따라 통제항목을 핵심기술관리 체계 통제항목으로 '반영'할 것인지, 해당 항목을 '개선'할 것인지 등에 대한 기준을 〔표 10〕과 같이 수립하고, 이용하려고 한다.

〔표 9〕 CTMS 항목 도출을 위한 factor별 밀접도 점수

구분	기밀성관련 밀접도	사전예방활동 밀접도
high	5	5
low	1	1

〔표 10〕 가중치 합산 값에 따른 통제 항목 조치 사항

구분	통제항목 응용 방향	비고
9점~10점	필수항목 '반영' 검토	
6점 ~ 8점	통제 항목 '개선' 또는 '추가' 검토	
5점 이하	통제 항목 '제거' 검토	
0점	통제항목 '제거'	

즉, 각 통제 항목에 2가지 factor에 대한 가중치를 합산한 값에 의거하여, 〔표 10〕과 같이 합산 값이 9점~10점인 통제 항목은 핵심 기술 관리 체계에 필수 통제 항목으로 반영하고, 6점~8점인 합산 값이 부여된 통제 항목은 해당 내용을 핵심 기술 관리 체계의 통제항목으로 '개선' 또는 '추가'하는 것을 검토하는 것으

〔표 11〕 ISMS를 활용한 CTMS 통제 항목 도출

정보보호관리체계(ISMS)_정보보호 대책							CTMS전환통제 중요도지 가중치		
NO.	도메인	No	통제 그룹	No	통제 항목	설명	기밀성관련 밀접도	사전예방활동 밀접도	합계
1	1. 정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	문서화된 정보보호정책은 최고경영자의 승인을 받아야 한다.	5	5	10
1	1. 정보보호 정책	1.1	정책의 승인 및 공표	1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	3	3	6
1	1. 정보보호 정책	1.2	정책의 체계	1.2.1	상위 정책과의 일관성	정보보호정책은 신청기관의 사업목표 및 정보기술정책과 일관성을 유지하여야 한다.	3	3	6
1	1. 정보보호 정책	1.2	정책의 체계	1.2.2	정책 문서의 유형	정보보호정책을 구체적으로 시행하기 위한 정보보호 지침, 절차 및 표준을 수립하여야 한다. 또한 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립할 수 있다.	5	3	8
1	1. 정보보호 정책	1.3	정책의 유지관리	1.3.1	주기적 검토	정기적으로 정보보호정책의 타당성을 검토하여야 하며, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.	3	3	6
2	2. 정보보호 조직	2.1	조직의 체계	2.1.1	조직의 구성	신청기관내정보보호관리활동을 계획, 관리하는 정보보호관리자가있어야하며,필요에따라 정보보호위원회를 구성할 수 있다.	5	3	8
2	2. 정보보호 조직	2.2	책임과 역할	2.2.1	정보보호관리자	최고경영자의지정을받은정보보호관리자는 정보보호정책 수립, 정보보호 위원회의구성및운영,위험분석및관리,보안사고대응및복구등의정보보호에관한업무를총괄관리하여야한다.	5	5	10
2	2. 정보보호 조직	2.2	책임과 역할	2.2.2	정보보호위원회	신청기관전반에걸친중요한정보보호관련심의및승인기능을수행하며필요한자원할당을통해정보보호관리활동이적절히수행될 수 있도록 하여야 한다.	5	5	10
5	5. 정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.2	교육 및 훈련 대상	교육 및 훈련의 대상에는 [illegible]	4	4	8
5	5. 정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.3	교육 및 훈련 내용	교육 및 훈련은 정보보호정책, 정보보호인식, 보안요구사항, 법적인 책임, 보안사고 대응절차, 업무연속성관리 등을 포함하여야 하고, 교육대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.	4	4	8
5	5. 정보보호 교육 및 훈련	5.2	시행 및 평가	5.2	시행 및 평가	교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육 훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.	4	3	7
6	6. 인적보안	6.1	책임할당 및 규정화	6.1.1.	책임할당	정보보호업무를 이행하는 역할과 책임을 문서화하여야 한다. 문서화의 내용에는 정보보호정책을 수립, 구현, 운영하는 일반적인 책임과 특정 정보자산의 보호와 활동에 대한 구체적인 책임을 포함하여야 한다.	5	5	10
6	6. 인적보안	6.1	책임할당 및 규정화	6.1.2	인사규정	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자에 대해서는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지	5	5	10

로 기준을 수립했다. 또한 본 논문에서는 5점 이하는 핵심 기술 관리 체계 통제 항목에 반영하지 않는 것으로 검토하도록 기준을 수립하였다. 0인 합산 값은 반영되지 않도록 통제 항목을 제거하고자 한다. 실제 이를 적용해서 반영한 도출 사례는 아래 〔표 11〕과 같다.

7.3 핵심 기술 관리 체계 통제 항목 모델링 시사점

2가지 factor에 대한 가중치 합산 값을 계산해본 결과 9점~10점에 해당되는 통제항목이 44개, 6점~8점 이하 통제항목은 33개, 5점 이하 통제 항목은 3개, 0점의 가중치가 부여된 통제 항목은 총 37개였다. 흥미로운 사실은 ISMS 통제항목을 2가지 factor를 적용한 가중치 합산 값 중 전체 약 66%에 해당되는 통제 항목이 기밀성 또는 사전 예방 효과와 관련된 통제 항목으로 분석되었고, 약 34%는 핵심기술 관리 체계에 적용하지 않고 제거가 가능할 것으로 예상되었다.

VIII. 법제도 강화 및 처벌 등 개선 제안

8.1 산업 스파이 등 처벌 강화 필요

최근 발생했던 OLED 사건에서 보듯이 사법 관할권이 미치지 못하는 외국법인에 대한 처벌을 어떻게 가져갈 것인가 하는 문제가 꾸준히 제기되고 있다.

특히 해당 사건이 중국 업체 측의 치밀하고 조직적인 계획인데도 불구하고, 현재의 지식 재산권 및 기밀의 유출에 대한 구속 기준이나 선고형량이 재산 범죄에 비해 낮게 적용되어 효율적인 방어가 어려워 보인다. 특히 징역 법정형을 5년 이하(해외 유출의 경우는 10년 이하)로 규정하고 있는데 이는 단순절도죄의 법정형(징역 6년 이하)보다 낮은 수준이다.

미국의 경우 최근 백서를 통해 경제 스파이에 대한 법정 최대형량을 20년 이상으로 높일 것을 연방의회에 권고했으며, 또한 연방의회가 미국 양형위원회(Sentencing Commission)에 경제스파이 및 영업비밀 절도에 대한 범죄 등급을 높이고 피고인의 범죄행위 비중에 따라 형량을 높여 처벌을 강화할 것을 권고한 것은 시사하는 바가 크다. 기술 유출 범죄에 대한 발생 건수는 〔표 12〕와 같이 지속적으로 증가하고 있으나, 기소율은 과거보다 줄거나 별 차이가 없는 것은 우리 사법기관의 소극적인 대응을 말해주고 있다. 이에 따라 보다 적극적인 기술 유출 범죄에 대한 대응이 필요할 것으로 보인다.

8.2 포상금 확대 등 신고 활성화 필요

현재 산업기술의 유출 방지 및 보호에 관한 법률 제21조 (산업기술 보호 포상 및 보호 등)를 보면 '산업기술을 해외로 유출한 사실을 신고한 자' 등에 대해 '예산의 범위 내에서 포상 및 포상금'을 지급하도록 되어 있다. 그러나 1억원 이내에서 지식경제부령으로 정하는 바에 따라 포상금을 지급한다고 명시하고 있다. 미국의 경우 현재 미국 연방수사국(FBI)은 산업스파이 등에 대한 신고 포상금으로 최고 50만 달러를 지급하는 것은 우리에게 시사하는 바가 크다고 하겠다. 기술유출 신고자에 대한 포상금을 확대하고 이를 적극적으로 시행하는 방안도 적극 검토가 필요할 것으로 보인다.

〔표 12〕 1999년~2009년 국내 기술 유출 사범 기소율

연도	인원	불기소율
1999	95	84.21
2000	234	82.48
2001	315	80.32
2002	389	76.86
2003	347	79.54
2004	398	83.17
2005	509	78.19
2006	628	77.55
2007	511	70.45
2008	698	69.91
2009	807	77.96
총합	4931	76.62

8.3 법률의 실천을 위한 자발적 참여 유도 필요

산업기술 유출 방지법에서는 '제14조 (국가핵심기술의 보호조치) 대상기관이 국가핵심기술을 보유·관리하고 있는 경우 그 대상기관의 장은 법 제10조제2항에 따라 다음 각 호의 보호조치를 하여야 한다.'라는 조항이 있다. 이 조항의 수행을 위해 국가핵심기술에 대한 보호 등급의 부여와 보안 관리 규정의 제정, 국가핵심기술 관리책임자와 보호구역의 지정, 국가핵심기술 보호구역의 통신시설과 통신수단에 대한 보안, 국가핵심기술 관련 정보의 처리 과정과 결과에 관한 자료의 보호, 국가핵심기술의 연구개발 인력에 대한 보안교육 실시, 국가핵심기술의 유출 사고에 대한 대응체제 구축 등에 대해서 기술해놓고 있다.

그러나 산업기술 유출 방지법 또한 기술 유출 방지에 대한 기업의 조치에 대해 보다 상세하게 기술한 해설서 등의 출간 등을 통해 기업이 자발적으로 실천할 수 있는 방향으로 제도가 개선되어야 할 것으로 보인다.

또한 핵심 기술 지정 이후 대기업은 물론 중소기업의 경우에는 특히 관리를 해야 되는 비용 부담이 크다. 이를 위해서 기존 정보통신망법 등의 발전과정과 기업 내 제도적인 활성화 도입 등 발전된 법률에 대해 참조한다면 보다 좋은 관리 모델을 수립할 수 있을 것으로 생각된다.

IX. 결론

첫째, 현재 제정된 산업기술 유출 방지 및 보호에 관한 법률은 과거의 많은 취약한 부분을 고려하는데 성공한 것으로 보인다. 그러나 여전히 해외 법인에 대한 사법 관할권 문제 및 처벌 수위 등에 대한 이슈가 존재한다. 이에 대한 행정, 사법기관의 정책 해결에 대한 노력이 필요할 것으로 보인다.

둘째, 현재 제정된 산업기술 유출 방지법은 대상과 처벌 규정을 명문화 하는 데는 의의를 갖지만, 핵심기술이라는 명확한 목표를 대상으로 기업에서 핵심기술의 라이프 사이클과 관련하여 어떤 활동들을 추진해야 하는지에 대한 세부 실천 사항의 개선과 지속적인 발전 과제를 안고 있다. 실제로 산업기술 유출에 대한 가이드 등은 개인정보보호와 관련된 정보통신망법 등 타 법률에서의 실천 조항을 위한 가이드나 지침 등에 비하면 부족한 것이 현실이다. 개인정보 유출 등이 사회적으로 큰 관심을 가지게 되면서 정보통신망법 제정, 개인정보보호법의 제정은 물론 방통위 및 KISA 등을 통해 기술적, 관리적 보호조치 고시 등이 쏟아져 나오고 있는 상황과 대비하면 국내 기술 유출에 관련한 각계 연구의 노력은 제도적으로 미비하다. 정부가 핵심 기술을 지정하는 것은 물론, 사후에 지정한 업체에 대한 제도적 지원 등이 미흡했다는 목소리도 높다. 따라서 기업이 적극적으로 준수해야할 관리 체계 기준 및 가이드라인 등을 지속적으로 발간 및 제정해야 할 것이다.

셋째, 핵심기술 지정 후 기업이 관리할 수 있는 행정적 제도적 부분에 대한 지원도 필요할 것이다. 이에 대한 모델링은 본 논문에서 제안된 핵심 기술 관리 체계 수립을 위하여 기존에 성공된 케이스로 평가받는 기존 정보보호 관리체계(ISMS) 등 에 대한 발전 과정을 참고하면, 유용하게 활용 될 수 있을 것이다. 이를 위해 기업이 지속적으로 실천할 수 있는 관리 체계가 될 수 있도록 행정기관은 물론, 전문가 그룹의 제도적인 고민이 더 필요하다. 이를 위해서는 보다 추가적인 연구가 필요할 것으로 보인다.

넷째, 최근에 발생된 아몰레드 사건을 보았을 때 기업자체에서 인력을 관리하려는 노력이 더욱 절실히 필요하다. 특히 협력 업체 직원이 한국 법인의 직원이었고, 업무의 특성을 이용하여 핵심 기술 유출을 외국 본사로 유출하였다는 점에서 이와 유사한 사례가 향후에도 발생할 수 있을 것이라 예상된다. 따라서 핵심기술을 보유하는 기관에서 내부 인력 또는 협력 업체 인력 채용 시 해당 업체 직원에 대한 신용도 평가, 소속 조직에 대한 사전 평가 등 사전 예방 프로세스를 실제로 운영하는 등 보안 관련 프로세스를 보다 강화할 필요가 있을 것으로 보여진다. 특히, 이 사건에서 협력 업체 직원들이 해당 기술들을 빼내가는 과정을 살펴보면, 실물 회로도를 몰래 촬영하고, USB 등에 담아 유출하였다는 점에서 핵심 기술 유출 기업의 접근 통제와 통제 구역에 대한 관리 강화 등에 대해 구체적인 대책을 시사하고 있다. 즉, DLP 등 기술적인 관점의 핵심 기술 보호에서 벗어나 물리적인 관점의 기초적인 보안에 대해서도 다시 한번 고민할 시점으로 판단된다.

마지막으로 본 논문에서 핵심 기술 관리 체계 수립을 위한 ISMS 등의 통제 항목 개선 및 보완을 위한 모델링 방법론이 더욱 연구되어 활용하기 위해서는 방통위, 지경부 등 각종 중앙 부처 등이 제도의 개선 및 심사기준, 보고라인, 심사인력 구성 등 다양한 형태의 논의가 많은 시간에 이루어져야 할 것으로 보여진다.. 무엇보다 앞서 정보자산의 기밀성을 보장하고 있는 기존 정보보호 관리 체계(ISMS) 등의 통제 항목의 미흡점을 공공적인 차원에서 분석하고, 이를 보완하는 작업이 선행되어야 할 것으로 보인다. 이를 위해 국정원 및 한국 인터넷 진흥원 등의 TFT 구성 등을 제안하는 바이다.

추가적으로 본 논문에서 제안된 가중치 factor 및 보다 추가적으로 고려되어야 할 객관적인 상호 밀접도 등에 대한 부분은 향후 보다 추가적인 논의 및 연구가 필요할 것이다. 또한 ISMS 및 PIMS 등은 KISA 및 방통위가 관리를 하고 있는 것처럼 핵심 기술 관리 체계를 보완하고, 인증 등의 운영을 관리할 수 있는 전담 TF 등의 구성을 제안하는 바이다.

참고문헌

〔1〕 지경부, "국가 핵심 기술 개정 고시," 2012년 1월

〔2〕 산업기밀보호센터 홈페이지 "기술유출 통계," http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00

〔3〕 보안뉴스, "국가핵심기술 보유기관의 보안수준 77.3점," 2012년 2월 11일, http://www.boannews.com/media/view.asp?idx=30011

〔4〕 서울 중앙 지방 검찰청 배포자료, "국가핵심기술인 삼성 및 LG의 아몰레드 핵심기술을 해외유출한 외국 협력기업 수사 결과," 2012년 6월

〔5〕 아이뉴스24, "삼성·LG 아몰레드 기술 해외 유출됐다," 2012년 6월 27일, http://news.inews24.com/php/news_view.php?g_serial=668271&g_menu=020810&rrf=nv

〔6〕 보안뉴스, "M&A에 의한 산업기술 유출, 규제 가능한가," 2009년 12월 11일, http://www.boannews.com/media/view.asp?idx=18871&kind=1

〔7〕 법제처, "산업기술의 유출 방지 및 보호에 관한 법률 공포," 2011년 7월 25일

〔8〕 이한영, 강하연, 여혁종, "미국 엑슨-플로리오법의 특징 및 시사점 - 규제연구 제15권 제2호," pp.125, 2006년

〔9〕 파이낸셜 뉴스, "엑슨-플로리오법이란? (자국 산업 보호가 글로벌 트렌드)," 2008년 9월 30일, http://www.fnnews.com/view?ra=Sent0601m_View&corp=fnnews&arcid=0921286198&cDateYear=2008&cDateMonth=04&cDateDay=15

〔10〕 한국지식재산연구원, "2011 지식재산집행에 관한 미국 지식 재산 집행 조정관 연례보고서," 2012년 3월

〔11〕 reuters.com, "Ex-Ford engineer sentenced for trade secrets theft," Apr. 13, 2011, http://www.reuters.com/article/2011/04/13/us-djc-ford-tradesecrets-idUSTRE73C3FG20110413

〔12〕 한국 산업 기술 협회, "중소 기업 기술 유출 대응 매뉴얼 별책 부록," 2007년 12월

〔13〕 중앙일보, "중국 국가기밀법 개정…인터넷 보안강화," 2009년 4월 2일, http://article.joinsmsn.com/news/article/article.asp?ctg=13&Total_ID=3555108

〈著者紹介〉

신 동 혁 (Dong Hyuk Shin) 학생회원
2005년 2월: 숭실대학교 산업정보시스템공학과 졸업
2009년 9월~2011년 12월: 고려대학교 정보보호대학원 수료
2005년 6월~2008년 6월: LG 그룹 서브원 (LG 유통) 정보전략그룹 근무
2008년 6월~2012년 4월: NHN 정보보호실 과장
2012년 5월~현재: 쿠팡 개인정보팀장
〈관심분야〉 정보보호정책, 개인정보보호, 핵심기술 보호, 정보보호컨설팅, 보안 감사 등

심 미 나 (Mina Shim) 종신회원
1996년 2월: 성신여자대학교 전산학과 졸업
2006년 2월: 고려대학교 정보보호대학원 공학석사
2010년 2월: 고려대학교 정보보호대학원 공학박사
2008년 3월~현재: 고려대학교 정보보호대학원, 세종사이버대/대학원, 서울디지털대 정보보호/개인정보보호정책 강의
2010년 9월~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 정보보호정책, 정보법학, 프라이버시, 개인정보보호, 개인정보영향평가 등

임 종 인 (Jong In Kim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등