2010-09 | 책임연구보고서

산업보안범죄의 제도적 대응방안

A Study on the Institutional Countermeasure against Industrial Security Crime

치안정책연구소
POLICE SCIENCE INSTITUTE

2010-09 | 책임연구보고서

산업보안범죄의 제도적 대응방안

A Study on the Institutional Countermeasure against Industrial Security Crime

치안정책연구소 범죄수사연구실

연구관 정 웅

목차

Ⅰ. 서 론

1. 연구의 목적

우리나라는 1997년 IMF 외환위기를 겪으면서도 21세기에 들어서기까지 지속적인 기술혁신(technological innovation)과 신지식 창출을 통해 자동차와 조선, 정보기술(IT) 등을 주력산업으로 발전시켜왔으며, 최근 2008년 세계적 금융위기의 상황에 직면하여서도 정부에서는 환경과 융합기술을 비롯한 첨단·신기술의 연구개발에 끊임없는 정책지원을 추진하고 있다.[1] 그 결과 우리나라는 산업화 초기에 보여 주었던 노동 생산요소 중심의 양적 경제성장에서 脫殼하여 산업구조의 고도화를 시현하였으며 개방형 시장경제체제 하에 세계적 첨단기술을 다수 보유한 경제 강국으로 성장하였다.

과거 우리나라는 발전도상국가로서 선진기술을 도입하는 위치에 있으면서 선진국으로부터 때로 불법적 기술수집의 의혹을 받았으나, 이제는 오히려 세계 각국으로부터 첨단기술 유출의 주요 대상이 되고 있고 실제 반도체, 조선, 자동차 등 다양한 분야에서 일부 국내 기업들의 핵심기술이 해외에 유출되는 사례가 발생하고 있다. 이는 개별 기업의 손실을 넘어 국내 산업의 경쟁력 약화는 물론 국민경제와 국가안보에도 큰 위협이 되고 있다.

일례로 최근 국정원의 산업스파이 해외 기술유출 자료를 보면, 2004 - 2009년간 국내 첨단기술을 해외로 불법유출하다 적발된 것만 총 203건에

1) 2009년 이명박정부의 녹색성장 국가전략의 10대 정책방향 가운데, 녹색기술개발 및 첨단융합산업 육성이 제시되고 있다. 녹색기술개발과 관련해서는 녹색 R&D 투자의 전략적 확대와 녹색기술의 기술력 제고를 통해 녹색기술 세계시장 점유율을 2009년 2%에서 2020년 10%, 2050년에는 18%로 높일 계획이다. 이를 위한 녹색기술투자비중은 2009년 16%, 2020년 25%, 2050년 30%로 확대시켜 녹색기술개발 체계를 강화할 예정이다. 또한 첨단융합산업 육성에서는 방송통신 융합, IT융합기술, 신소재, 바이오 산업 등 첨단융합으로 신성장동력 영역을 확대할 것을 제시하고, IT융합산업수출액의 경우는 2009년 755억불 규모에서 2020년 1,443억불, 2050년 3,489억불 규모로 증가시킬 계획이다(녹색성장위원회, 녹색성장 국가전략, 2009. 7).

달하는 것으로 나타나고 있다. 특히 연도별로는 2004년 26건에서 2008년 42건, 2009년 43건으로 최근까지 해마다 지속적으로 증가하고 있는 추세에 있다.[2)]

이같은 첨단 산업기술의 불법적 해외유출에 대처하기 위하여 제도적으로는 2004년 부정경쟁방지및영업비밀보호에관한법률(이하 영업비밀보호법)의 대대적인 개정을 통하여 영업비밀보호를 대폭 강화한 바 있으며, 또한 2006년 10월에는 동 법을 보완한 산업기술의유출방지및보호에관한법률(이하 산업기술보호법)을 제정하였다. 즉 기존의 영업비밀보호법이 민간의 기업비밀 누설에만 처벌이 한정되어 있고 각종 법률에 산재해 있는 관련규정으로는 산업기술유출 방지에 큰 효과를 내지 못하였기 때문에 국가안보에 직접적인 영향을 미치는 국가핵심기술의 해외유출을 규제하고, 산업기술의 부정한 유출을 방지하기 위해 산업기술보호법을 제정하게 된 것이다.

또한 경찰에서도 국가적인 산업기술 불법유출 규제정책에 따라 그 유출방지활동을 강화하기 위하여 2004년 3월 사이버 경찰청 및 각 지방경찰청에 산업스파이신고센터를 개설하는 한편, 전국 지방경찰청에 전문수사인력을 편성하고 경찰청 외사수사과에 전담수사대(국제범죄수사대)를 운영하는 등 첨단 산업기술유출 사범의 검거를 위한 수사 활동을 적극 전개하여 왔다.

본 연구는 이처럼 탈냉전 이후 전개되고 있는 경제전쟁과 첨단과학기술 시대에 우리나라의 선진국 안착을 겨냥한 첨단기술 보호와 불법유출 차단의 필요성 문제를 제기하면서, 최근의 산업기술 유출방지 제도 하에 발생해 온 산업보안범죄의 실태를 점검하고 그 제도적인 대응방안을 모색하는 데 그 목적을 두고자 한다.

---

2) 산업기밀보호센터, “기술유출 통계”, http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00(2010. 6. 10 검색).

2. 연구 시각과 글의 순서

본 연구는 산업기술 불법유출이라는 범죄행동(criminal behavior)에 있어서의 합리적 선택(rational choice)을 가정하고, 범죄경제학(economics of crime)과 신제도주의(new institutionalism) 시각에서 산업보안범죄에 대한 제도적 대응방안을 모색해보고자 한다. 범죄경제학과 신제도주의 접근은 모두 인간행동에서 경제적 유인(incentive)에 대한 반응과 합리적 선택이론을 수용하고 있다. 따라서 이러한 접근은 한 개인의 산업기술 유출과정에서 비용-수익(cost-benefit)에 기초한 불법행동 기회(illegal behavior opportunity)의 선택 경향에 대한 분석을 진행하고, 처벌의 가능성 및 엄격성(probability and severity of punishment)을 갖춘 제도설계(institution design)를 통해 산업보안범죄를 억제하는 방안을 구상하는데 유용할 것으로 보인다.[3)]

범죄자들은 여타 일반인들과 같이 합리적으로 자신의 효용을 극대화하고자 행동하는 바, 이러한 범죄자들이 자신의 목적 달성과정에서 합법적 행동(legal behavior)이 아니라 불법적 활동(illegal activities)을 선택하여 효용을 극대화하는 것을 억제하기 위해서는 적절한 경제적 유인체계가 갖추어진 제도가 설계(design)되어야 한다. 경제적 유인체계와 효율성이 함축된 합리적 선택 신제도주의(rational choice new institutionalism) 접근에 의할 때, 한 범죄대응제도의 성과(performance)는 신고전주의적 생산함수 이외에도 거래비용(transaction cost)의 존재가 고려된 법과 조직

3) 현대 범죄경제학의 맹아가 된 Becker의 연구(1968) 이후 그 기본 분석모형은 E[U]=P・U(Y-f) + (1-P)・U(Y)로 나타낼 수 있다. 즉 범죄행동은 기대효용(Expected Utility)이 正(positive)의 값을 가질 때 이루어진다. 이 모형에서 P는 체포되어 유죄판결을 받을(처벌될) 확률, Y는 범죄로부터 얻는 수익, f는 처벌로 부터의 비용이다. 여기서 범죄를 억제하기 위한 관건은 체포될 확률(P)을 높이고, 범죄수익(Y)을 낮추며, 범죄비용(f) 높이는 엄격한 법제 등을 어떻게 마련할 수 있는가에 달려있다. 이러한 기본 모형을 변형하여 Brown과 Reynolds(1973)는 개인의 초기소득상황(individual's initial income position)을 강조한 모형을 내놓았다. 이 모형은 E[U]=P・U(W-f) + (1-P)・U(W+g)로 나타나고, W는 현재(초기)소득, g는 범죄로부터 얻는 이득이다. Brown과 Reynolds의 모형을 따를 때, 범죄는 기대효용이 현재소득보다 클 때 이루어진다(Eide et al., 2006: 3-4).

등 제도의 함수이기도 하며(North, 1990; Williamson, 1985; Eggertsson, 1990), 법제적·조직적 변수의 성공적인 구축과 선택 여부에 따라 범죄 억제의 성과가 크게 달리하게 되는 결과를 가져올 수 있다.

따라서 본 연구의 진행 순서는 먼저 Ⅱ장에서 산업보안의 의의와 불법 유출위험, 산업보안범죄의 개념범주를 살펴보고 Ⅲ장에서 우리나라와 주요국의 산업보안제도의 동향을 개관한 뒤, Ⅳ장에서 산업보안범죄의 실태분석과 제도적 대응방안을 모색을 하는 것으로 구성하고자 한다.

Ⅱ. 산업보안과 불법위험

1. 산업보안의 의의

탈냉전 이후 국제질서는 군사외교 중심에서 WTO로 대변되는 자유무역 경제질서가 힘을 얻고 이와 병행하여 1990년대 이후에는 지역주의(regionalism)에 기초한 FTA가 확산됨으로써, 국제시장의 치열한 경쟁 속에 한 기업의 산업기술이 국가경쟁력을 담보하는 중요한 요소가 되고 있다. 따라서 21세기에는 더욱 산업기술 문제가 단순한 기업의 차원을 넘어서 산업경쟁력과 국가생존이 걸린 문제로 부상할 것임을 시사하며, 바로 여기에서 이러한 산업기술보호 혹은 산업보안의 필요성이 발견된다.[4)]

이 같은 산업보안이라는 용어는 첨단기술 유출방지 목적 하에 국가행정 실무에서 사용되기 시작하였으나 그 개념은 학문적 또는 법적으로 정립된 용어는 아니다. 산업보안을 인원보안, 문서보안, 시설보안 등과 같이 보안관리 대상분류에 의한 행정서비스 성격을 내포하고 있다고 설명하는 견해에서부터(민병설, 2002: 16), 산업보안을 첨단기술뿐만 아니라 산업활동에 유용한 기술상, 경영상의 모든 정보나 인원, 문서, 시설, 자재 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호. 관리하기 위한 대책이나 활동을 의미하는 것으로 보다 폭넓게 정의하기도 한다(국가정보대학원, 2006: 1; 노호래, 2008: 50).

---

4) 산업보안 필요성을 개인과 기업, 국가 등 산업보안에서의 이해당사자 혹은 행위자(player) 별로 분설하면 첫째, 연구자 개인의 산업기술 보호를 위해 필요하다. 첨단산업기술 개발에는 장기간의 투자와 많은 비용이 소요되며, 연구자들의 연구성과가 산업기술로서 가치가 있는 경우에 보호를 해주어야 할 필요성이 있다. 둘째, 국내기업의 경쟁력 유지를 위해 필요하다. 첨단기술이 유출되어 관련 제품이 경쟁기업을 통해 생산된 경우에 국내외 시장에서 국내기업은 그 경쟁력이 약화되는 상황에 처할 수 있기 때문에 산업기술의 보호가 필요하다. 셋째, 국가 경쟁력 확보 측면에서 그 필요성이 있다. 산업기술의 불법유출은 개인과 기업에 그 피해가 머물지 않고 국가안보와 경제력 약화로 귀결됨으로써, 국가의 경쟁력이 훼손될 수 있다.

산업보안을 정의하기 위해서는 보안의 대상과 주체를 명확히 파악해야 한다. 먼저 보안의 주체 측면에서 보면 산업기술을 보유한 대학, 연구소, 기업 등이 있겠으나 그중에서도 기업이 주요한 산업보안활동의 주체가 된다. 아울러 산업보안활동은 한 국가의 산업계 전반에 걸친 보안활동이므로 그 주요 주체는 기업에 국한되지 않고 국가도 산업보안활동의 주체가 된다.

산업보안활동은 기업의 사적 자율성뿐만 아니라 국가안보에 기초한 공공성을 함께 갖고 있는 바, 그런 면에서 산업보안은 순수한 기업이윤추구에서 관점에서의 기업보안과 구별된다.

즉 기업이 주체가 된 '기업보안' 활동은 그 보호대상에 있어서 기업의 존립이나 명예, 영리와 관련 있는 것은 모두 기업보안의 대상이 되지만, 산업보안은 기업뿐만이 아니라 한 국가의 산업계 전반의 취약요소나 발전전략까지도 포함한다. 따라서 기업의 금융비리나 환경관리상의 취약요소는 기업보안의 대상은 될 수 있지만 산업보안의 대상은 되지 않는다고 할 수 있다(노호래, 2008: 50-51).

산업보안의 대상이 되는 '산업기술(industrial technology)'은 사전적인 논의에서 볼 때[5], "기초기술을 제품화·사업화함으로써 상품을 생산하는 산업분야에 응용한 것"으로 정의해 볼 수 있다.

한편 산업보안의 대상인 산업기술은 법률적으로는 관련 법률인 산업기술보호법을 통해 파악할 수 있는데, 여기서 '산업기술'이라 함은 제품 또는 용역의 개발· 생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계 중앙행정기관의 장이 소관분야의 산업경쟁력 제고 등을 위하여 법령이 규정한 바에 따라 지정 또는 고시· 공고하는 기술로서 다음 각 목의 어느 하나에 해당하는 것을 말한다(산업기술보호법 제2

5) Wikipedia, "Industrial technology", Industrial technology is the field concerned with the application of basic engineering principles and technical skills in support of industrial engineers and managers. http://en.wikipedia.org/wiki/Industrial_technology(2010. 6. 20 검색).

조). 동 법률에서 적시하고 있는 산업기술의 구체적 내용으로서 그 각 목은 첫째, 국내에서 개발된 독창적인 기술로서 선진국 수준과 동등 또는 우수하고 산업화가 가능한 기술, 둘째, 기존제품의 원가절감이나 성능 또는 품질을 현저하게 개선시킬 수 있는 기술, 셋째, 기술적· 경제적 파급효과가 커서 국가기술력 향상과 대외경쟁력 강화에 이바지할 수 있는 기술, 넷째, 앞선 첫 번째와 세 번째 내용에 포함되는 산업기술을 응용 또는 활용하는 기술을 말한다.

한편 산업기술의 의미에는 산업기술보호법상의 산업기술 외에 영업비밀보호법상의 “영업활동에 유용한 기술상 또는 경영상의 정보”를 포함할 수 있다(영업비밀보호법 제2조 제2항).

이상의 논의를 기초로 산업보안을 정의하면 산업보안이란 “국가와 기업을 중심으로 산업활동에 유용한 기술과 정보를 기관외부에 유출하지 않도록 보호하는 활동”이라고 할 수 있다.

2. 산업기술의 불법유출 위험

산업기술은 국가와 기업의 보호노력에도 불구하고 항상 불법유출의 위험성이 존재한다. 즉 불법적 행동으로부터의 비용과 처벌가능성을 감안하더라도 체포되지 않았을 경우의 범죄수익이 높은 경우는 전체적으로 기대되는(Expected) 수익 역시 높아지며, 범죄경제학의 견지에서 볼 때 바로 이것이 행위자 개인으로 하여금 합법적 행동보다는 불법적 범죄를 저지르게(선택하게) 되는 동기를 제공하는 것이다. 더욱이 체포의 가능성 측면에서는, 정보통신기술과 장비의 발달에 따라 산업기술정보의 유출, 침해가 용이해짐으로써 불법행동의 기대수익값은 더욱 높아지고 있다. 즉 복사기, 사진기, 녹음기뿐만 아니라 인터넷 등 외부에서의 해킹, 이동통신, E-mail 등으로 실시간 대량유출과 침해가 가능해졌으며, 또한

CD, USB 등을 통해 기술정보를 소프트화 함으로써 그 불법유출이 수월해지고 있는 것이다.

이러한 불법유출은 개별적 우범상황에서 체포가능성 등을 고려한 범죄기대수익이 매우 높다고 주관적으로 판단되면, 기업 내부자뿐만 아니라 그 협력업체, 일반인까지도 누구든지 유출주체가 될 수 있다.

유출주체와 관련하여 산업보안에 있어서 가장 밀접하게 논의되는 것은 산업스파이(industrial spy)이다. 산업스파이는 사전적으로 "이해가 상반하는 국내외 경쟁기업의 최신 산업정보를 입수하거나 교란시키는 공작 등을 전문으로 하는 사람"으로 정의된다.[6] 모든 기업은 시장정보· 상품정보 등 통상적인 정보의 수집활동을 수행하고 있는데, 그 중에서도 가장 중요한 것이 기술개발 등 경쟁회사에 관한 정보인 것이며, 산업스파이는 이러한 경쟁회사의 정보를 합법적 또는 불법적 방법 등 그 수단을 가리지 않고 수집한다.

따라서 산업보안에 있어서 산업스파이에 대한 보안 활동은 산업보안활동의 가장 본질적이고 핵심적인 부분이라고 해도 과언이 아닐 것이다. 그 만큼 최근 산업보안과 관련하여 문제가 되는 것은 스파이에 의한 산업정보 유출행위라고 할 수 있다(노호래, 2008: 52).

역사적으로 볼 때, 과거 미・소 냉전시대 스파이[7]의 주된 임무는 적국의 정치, 군사 정보를 수집하는 것이었다. 그러나 냉전체제가 붕괴된 이후, 이러한 스파이전은 그 의미가 감소되었으며 경제적 패권주의가 등장함에 따라 첨단기술을 개발한 산업체를 상대로 산업기술을 수집・탐지하는 산업스파이의 산업기술 유출위험 문제점이 전면에 대두하게 된 것이다.

오늘날의 산업스파이 활동은 정보수집 과정에서 첨단화된 장비를 활용

6) 두산백과사전, "산업스파이", http://100.naver.com/100.nhn?docid=85367(2010. 6. 30 검색).
7) 스파이의 어원은 '멀리 본다' 또는 '숨겨져 있는 것을 목격 또는 발견한다'는 뜻의 고대 프랑스어인 'espier'에서 유래되었다고 한다(조병인 외, 2000 : 41).

하면서 이른바 냉전시대부터 이어져온 절취·촬영·도청·녹음 등 전형적인 산업스파이 방법들이 더욱 정교해지고 있다. 최근의 산업스파이 행위들을 유형화하면 다음의 6가지로 구분해 볼 수 있다.[8)]

첫째로, 핵심기술인력의 영입에 의한 방법이다. 흔히 스카우트라고 불리며, 타 경쟁사의 영업비밀을 입수하는 가장 간단한 방법으로 경쟁사의 직원을 회사의 임직원으로 고용하여 필요한 정보를 얻는다. 기술인력의 영입은 영업비밀의 취득이라는 이익뿐 아니라 경쟁사의 인력 손실이라는 불이익을 초래한다.

둘째로, 컴퓨터를 통한 해킹 방법이다. 1990년대 중반 이후 인터넷의 급격한 발달로 정보네트워크가 사회의 핵심 기반으로 자리 잡으면서 컴퓨터에 의한 해킹도 주요한 산업기술정보의 유출수단으로 대두되고 있다.

셋째로, 전자신호 도청 방법이다. 전화, 팩스, 위성 등 통신수단에 대한 도청을 통해 중요한 정보를 얻거나 혹은 직접 경쟁사에 영상 및 음성 도청장치를 설치하여 필요한 정보를 얻는 방법도 중요한 기술유출 수단의 하나이며, 정보통신기술의 발달에 수반하여 그 차단 필요성이 더욱 높아지고 있다.

넷째로, 경쟁업체로 잠입하는 방법이다. 경쟁업체의 산업기밀을 얻기 위하여 위장 침투하는 형태로서, 특채 혹은 일반 공채를 통하여 입사한 후 단기 혹은 장기간에 걸쳐 기업의 핵심적인 정보를 입수하는 것이다.

다섯째로, 기업내부자의 매수이다. 스카우트와 더불어 우리나라에서 일어나는 기술유출의 많은 부분을 차지하고 있는 방법이며, 상대 기업의 임직원을 매수하여 필요한 정보를 얻는다.

여섯째로, 제3자를 이용하는 방법이다. 상대 기업에 대한 많은 정보를

8) 산업스파이 행위의 6개 유형분류(경찰청, 산업보안실무, 2007: 23-27) 외에, ① 절취·복사·촬영, ② 전자기기에 의한 도청 및 비밀녹음, ③ 위장침투, ④ 기업내부자의 매수, ⑤ 인력 스카우트, ⑥ 제3자 이용, ⑦ 컴퓨터 이용 등 7가지로 분류 소개한 경우도 있으나(사법연수원, 2004: 95-99), 포괄된 기본 범주내용은 큰 차이가 없다.

갖고 있는 사람, 예를 들어 기업담당 회계사, 컨설턴트, 변호사 등을 통하여 정보를 얻는 수법으로 첨단장비 등이 동원되어야 할 부담이 없다.

3. 산업보안범죄의 개념범주

본 연구에서는 산업보안을 “국가와 기업을 중심으로 산업활동에 유용한 기술과 정보를 기관외부에 유출하지 않도록 보호하는 활동”이라고 정의하고, 범죄경제학의 시각에서 기대수익에 기초한 불법행동의 선택과 불법유출의 위험성을 강조하였으며, 특히 대표적인 유출주체로서 산업스파이와 그 유출활동 및 수법 등을 언급하였다.

위 논의에 기초하여 산업보안범죄를 정의해보면 산업보안범죄란 “산업활동에 유용한 기술과 정보를 불법적으로 기관외부에 유출하는 행동”이라고 할 수 있다. 이러한 산업보안범죄의 개념범주를 현행 실정법규에 따라 설정해볼 경우 관련 법규인 기술유출방지법 및 영업비밀보호법에서 정한 처벌규정의 위반에서 찾아질 수 있다.

먼저 기술유출방지법에서는 산업기술 유출 및 침해행위를 금하고(동법 제14조)에 대한 형사적 규제를 규정하고 있는데 이러한 침해행위가 있을 경우 산업보안범죄에 해당한다. 예를 들면 산업기술을 외국에서 사용하게 하거나, 사용되게 할 목적으로 부정하게 취득, 사용, 공개, 유출하는 등의 행위와 국내에서 사용하거나, 사용되게 할 목적으로 산업기술을 취득, 사용, 공개, 유출 등의 행위를 하는 경우가 산업보안범죄에 포함된다. 이러한 경우 징역형과 벌금형을 병과할 수 있으며, 미수범죄도 처벌된다. 또한 영업비밀보호법과 마찬가지로 침해행위의 예비, 음모죄를 규정하고 있다.

영업비밀보호법에서는 영업비밀의 취득·사용, 누설에 대해 형사처벌을 규정하고 있으며 이러한 위반행위가 있을 경우 산업보안범죄에 해당한다. 즉 부정한 이익을 얻거나 기업에 손해를 입힐 목적으로 그 기업에

유용한 영업비밀을 취득·사용하거나 제3자에게 누설하는 행위, 영업비밀 침해행위에 대한 미수, 예비, 음모행위도 산업보안범죄에 해당한다.

한편 최근 영업비밀 유출자에 대한 처벌을 강화한 영업비밀보호법 개정안[법률 제9895호, 2009.12.30, 일부개정]이 2010년 3월 31일부로 시행되어 산업보안범죄의 범주가 더욱 넓어졌다. 즉 과거 영업비밀보호법이 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알고 제3자에게 누설한 자에 대해서만 가중 처벌한 것에 비해 개정법은 기업의 영업비밀 유출 예방을 위해 외국에서 사용될 것을 알고 취득한 것만으로도 처벌이 가능토록 변경되었기 때문에 산업보안범죄의 대상 범위가 확대되었다.

Ⅲ. 산업보안 제도의 동향

1. 국내 산업보안 제도 현황

우리나라는 1961년 12월 30일 법률 제911호로 제정된 부정경쟁방지법을 1991년 12월 31일 법률 제4478호로 개정하면서 영업비밀 보호제도를 최초로 도입하였다. 이러한 영업비밀 보호제도의 도입은 1986년 우리나라가 미국 정부와 합의한 양해각서(Memorandum of Understanding)에서 영업비밀에 대한 보호제도를 도입하기로 합의한 것에 기원한 것이었다. 이후 1998년 동법률의 법제목을 부정경쟁방지및영업비밀보호에관한법률로 변경하고, 다시 2004년 1월 20일 제7095호로 동 법률을 대폭 개정하면서 영업비밀보호를 강화하였다. 그러나 이 법률은 기술유출 후의 사후적 규제만을 중심으로 규정하고 있다는 점에서 한계가 있었다. 이러한 한계를 보완하기 위하여 2006년 9월 산업기술의유출방지및보호에관한법률이 국회를 통과하여 2007년 4월부터 시행되고 있다. 양 법률의 구체적인 내용을 살펴보면 다음과 같다.

1) 영업비밀보호법

1961년 도입된 부정경쟁방지법에서 틀에 출발한 영업비밀보호법은 이후 12차에 걸친 개정을 거쳐[9] 현재 법률 제9895호로 시행되고 있다.

9) 1961년 부정경쟁방지법[시행1962.1.1] [법률 제911호, 1961.12.30, 제정]부터, 1차개정[시행1987.1.1] [법률 제3897호, 1986.12.31, 전부개정], 2차개정 [시행1992.12.15] [법률 제4478호, 1991.12.31, 일부개정], 3차개정[시행1998.1.1] [법률 제5454호, 1997.12.13, 타법개정], 4차개정[시행1999.1.1] [법률 제5621호, 1998.12.31, 일부개정], 5차개정[시행1999.7.1] [법률 제5814호, 1999.2.5, 타법개정], 6차개정[시행2001.7.1] [법률 제6421호, 2001.2.3, 일부개정], 7차개정[시행2004.7.21] [법률 제7095호, 2004.1.20, 일부개정], 8차개정[시행2005.7.1] [법률 제7289호, 2004.12.31, 타법개정], 9차개정[시행2007.12.21] [법률 제8767호, 2007.12.21, 일부개정], 10차개정[시행2008.12.26] [법률 제9225호, 2008.12.26, 일부개정], 11차개정[시행2009.3.25] [법률 제9537호, 2009.3.25, 일부개정], 12차개정[시행2010.3.31] [법률 제9895호, 2009.12.30, 일부개정]에 이르고 있다. 그러나 1991년 영업비밀 보호제도가 최초로 도입되었던 1991년 부정경쟁방지법부터 기산하면 영업비밀보호법은 사실상 10차에 걸친 개정이 이루어졌다고

영업비밀보호법은 타인의 영업비밀을 침해하는 행위를 방지하여 건전한 거래질서를 유지함을 목적으로 하고 있으며, 여기서 영업비밀이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의해 비밀로 유지된 생산방법・판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다(영업비밀보호법 제2조 제2호).

현행 영업비밀보호법은 2004년 7차 개정 당시 영업비밀보호를 강화하면서 그 틀을 잡았다고 볼 수 있다.

먼저 영업비밀 침해행위주체에 대해 종전 해당 기업의 전・현직 임직원에서 영업비밀을 침해한 자는 누구든지 처벌할 수 있도록 확대하였다. 또 영업비밀 보호대상도 기업에 유용한 기술상의 영업비밀에서, 경영상의 영업비밀까지 그 보호 대상을 확대하였다. 보호 범위를 확대한 것은 기술상의 비밀과 경영상의 비밀의 경계가 점차 모호해지고, 사업기획과 마켓팅전략 등 경영상 영업비밀이 더욱 중요해지는 산업환경변화에 부응한 것이며, 미국, 영국, 독일의 경우에도 이처럼 기술상의 영업비밀뿐만 아니라 경영상의 비밀 침해행위도 처벌하는 추세에 있다(국가정보원, 2004: 4).

그에 따라 누구든지 부정한 이익을 얻거나 기업에 손해를 가할 목적으로 기업에 유용한 영업비밀의 취득, 사용하거나 제3자에게 누설하는 행위를 하는 경우 5년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처하도록 규정하고 있다. 특히 외국으로의 불법유출의 경우 2004년 7차 개정 시에, 외국에서 사용하거나 외국에서 사용될 것임을 알고 제3자에게 누설한 자에게 7년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처하도록 규정

할 수 있다. 법제처 국가법령정보센터, “부정경쟁방지 및 영업비밀보호에 관한 법률 연혁”, http://www.law.go.kr/LSW/lsSc.do?menuId=0&p1=&subMenu=1&searchName=LicLs%2C0&query=%EC%98%81%EC%97%85%EB%B9%84%EB%B0%80%EB%B3%B4%ED%98%B8&x=13&y=18#liBgcolor0(2010. 6. 10 검색).

하였으며, 2009년 12차 개정 때는 그 처벌을 더욱 강화하여, 기업의 영업비밀 해외유출 예방을 위해 외국에서 사용될 것을 알고 취득한 것만으로도 처벌이 가능토록 하였다.

또한 영업비밀 침해범죄에 대해서는 과거 고소가 있어야만 공소를 제기할 수 있으나, 기업 영업비밀이 국가의 경쟁력을 좌우할 주요한 요소를 부각됨에 따라 고소가 없이도 그 침해행위를 수사·처벌할 수 있도록 친고죄를 폐지하였다. 아울러 영업비밀보호법은 영업비밀 침해행위에 대한 미수범을 처벌할 수 있도록 규정하고 있다. 동 규정을 신설하기 이전에는 영업비밀의 누설 바로 전단계에서 검거된 자에 대해서는 동법으로 처벌할 수 없었다.

이밖에 동법률은 영업비밀 침해행위의 예비·음모죄 처벌조항을 두고 있다. 즉, 국내 영업비밀 침해죄를 범할 목적으로 예비 또는 음모한 자에 대해서는 2년 이하의 징역, 1천만원 이하의 벌금에 처하고 있으며, 국외 영업비밀 침해죄를 범할 목적으로 예비 또는 음모한 자는 3년 이하의 징역, 2천만원 이하의 벌금에 처하고 있다. 기타 동법은 양벌규정을 두어 조직이나 기업에 의한 조직형·기업형 영업비빌 침해범도 처벌할 수 있는 근거를 두고 있다. 이상 우리나라 영업비밀보호법의 주요 내용을 정리하면 다음의 <표 1>과 같다.

<표 1> 영업비밀보호법의 주요 내용

구 분	주요 내용
침해주체	누구든지(비신분범)
보호대상	기업에 유용한 영업비밀(기술상 정보 외에 경영정보도 포함)
위법성	부정한 이익을 얻거나, 손해를 가할 목적
침해행위	국내 : 영업비밀을 취득·사용하거나 제3자에게 누설하는 행위 외국 : 외국에서 사용될 것임을 알면서 취득·사용 또는 제3자에게 누설하는 행위
소추요건	피해자의 고소가 없어도 소추가능(비친고죄)
처벌형량	국내 : 5년이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하의 벌금 외국 : 10년이하의 징역 또는 그 재산상 이득액의 2배이상 10배 이하의 벌금
미수・예비/음모	제18조의2(미수), 제18조의3(예비·음모) 규정에 의하여 처벌
양벌규정	침해행위자를 벌하는 외에 그 법인도 처벌.

2) 산업기술보호법

(1) 제정 배경과 의미

최근 우리 기업의 기술이 해외로 유출되는 사례가 급증하고 특히 기업이 아닌 정부출연연구소 또는 대학부설연구소 등에서 개발된 첨단기술이 유출되는 사례도 발생하고 있으나 이러한 기관들은 영업활동을 하는 기업이 아니기 때문에 이러한 개발성과의 불법유출에 대하여 영업비밀보호

법상의 보호규정이 적용되는지 여부에 대하여는 명확하지 못한 면이 있었다. 아울러 국제교역의 증가 속에 국가 안보와 국민경제에 큰 영향을 미칠 수 있는 핵심기술의 해외 이전에 대해 적절히 규제할 필요성이 고조되어 왔다.

이처럼 산업기술의 불법 해외유출이 심각한 수준에 있었으나 기존 영업비밀보호법에 의한 처벌대상이 민간 기업비밀 누설의 경우로 한정되어 있고, 각종 법률에 산재하여 있는 관련 규정으로는 산업기술유출 방지 및 근절에 큰 효과를 내지 못함이 따라 산업기술보호법을 제정하게 되었다.[10]

특히, 미국과 일본의 경우 영업비밀 보호를 강화하기 위한 법률의 제정이나 개정이 주로 사후 대책에 머무르고 있으나 우리나라의 산업기술보호법은 형사처벌에서 한걸음 더 나아가 산업기밀 유출을 사전에 방지하는 정부의 정책과 제도적 장치를 마련한 데에 큰 의의가 있다고 할 수 있다.[11]

(2) 주요 내용

산업기술보호법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써, 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 그 목적으로 하고 있으며, 그 주요 내용은 ① 산업기술의 유출방지 및 보호 정책의 수립·추진에 관한 사항과 이를 위한 심의기관으로서 산업기술보호위원회의 설치에 관한 사항, ② 국가핵심기술의 수출에 대한 정부의 승인에 관한 사항 및 산업기술의 유출 및 침해행위 금지 등 산업기술의 유출방지 및 관리에 관한 사항, ③ 산업기술보

10) 2004년 11월 이광재 의원 등 여야의원 34명이 공동발의했던 산업기술보호법은 2006년 9월 29일 국회 본회의 의결을 거쳐 2006년 10월 27일 공포되었으며 2007년 4월2 8일부터 효력이 발생되었다. 이후 4차에 걸친 개정을 거쳐 현재 법률 제9368호로 시행되고 있다.

11) 양영준, "「산업기술의 유출방지 및 보호에 관한 법률」에 관한 소고", 9-10면, http://service4.nis.go.kr/servlet/board?cmd=bo_view&no_idx=42&cd_code=industrial&curpage=1&menu=ADC00(2010. 5. 1 검색).

호협회 설립 등 산업기술보호의 기반구축 및 산업보안기술의 개발. 지원에 관한 사항, ④ 산업기술분쟁 조정에 관한 사항 및 ⑤ 법률 위반행위에 대한 벌칙 등으로 되어 있다.

① 우선 산업기술보호법은 산업기술의 유출방지 및 보호를 위한 국가, 관련 기관 및 일반 국민의 책무에 대하여 다음과 같이 규정하고 있다. "국가는 산업기술의 유출방지와 보호에 필요한 종합적인 시책을 수립·추진하여야" 하고(제3조 제1항), "국가·기업·연구기관 및 대학 등 산업기술의 개발·보급 및 활용에 관련된 모든 기관은 이 법의 적용에 있어 산업기술의 연구개발자 등 관련 종사자들이 부당한 처우와 선의의 피해를 받지 아니 하도록 하고, 산업기술 및 지식의 확산과 활용이 제약되지 아니하도록 노력하여야" 하며(제3조 제2항), "모든 국민은 산업기술의 유출방지에 대한 관심과 인식을 높이고, 각자의 직업윤리의식을 배양하기 위하여 노력하여야 한다"고(제3조 제3항) 규정하고 있다.

위에서 언급한 국가의 책무를 이행하기 위하여 정부는 산업기술의 유출방지 및 보호에 관한 기본계획, 시행계획 및 보호지침을 제정하여야 한다. 먼저 기본계획에 따라 관계 중앙행정기관의 장은 매년 산업기술의 유출방지 및 보호에 관한 시행계획을 위원회의 심의를 거쳐 수립. 시행하여야 한다(제6조 제1항). 기본계획이 국가 차원의 정책지침이라면 시행계획은 기본계획을 실천하기 위한 각 정부 부서 차원의 구체적 행동지침이라고 할 수 있을 것이다. 또 지식경제부장관은 산업기술의 유출을 방지하고 산업기술을 보호하기 위하여 필요한 방법. 절차 등에 관한 보호지침을 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 제정하고 이를 대상기관이 활용할 수 있도록 하여야 한다(제8조 제1항). 기본계획 및 시행계획이 정부의 시행지침이라면, 보호지침은 국책연구기관 등 산업기술법의 적용대상인 대상기관 등이 산업기술을 보호, 관리하는 지침을 수립함에 있어 참고로 하는 지침이라고 할 수 있다.

이상의 산업기술의 유출방지 및 보호에 관한 기본계획수립 등을 심의

하기 위하여 국무총리 소속하에 산업기술보호위원회를 둔다(제7조).

② 국가핵심기술의 유출 방지 및 보호를 위해 지식경제부장관은 관계 중앙행정기관의 장으로부터 그 소관의 국가핵심기술로 지정되어야 할 대상기술을 통보받아 위원회의 심의를 거쳐 국가핵심기술로 지정할 수 있다(제9조 제1항). 국가핵심기술이란 “국내외 시장에서 차지하는 기술적.경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술”을 말한다(제2조 제2호).

국가핵심기술로 지정되면 그 기술의 해외수출 등이 규제되어 대상기관의 재산권에 중대한 제한을 가할 수 있으므로 그 지정은 법에서 정한 제반 요건을 검토하여 신중하게 이루어져야 할 것이고 특히 시행령의 내용에서 명확한 지정기준이 제시될 필요가 있다.

국가핵심기술을 보유・관리하고 있는 대상기관의 장은 보호구역의 설정・출입허가 또는 출입시 휴대품 검사 등 국가핵심기술의 유출을 방지하기 위한 기반구축에 필요한 조치를 하여야 한다(제10조 제1항). 또 국가로부터 연구개발비를 지원받아 개발한 국가핵심기술을 보유한 대상기관이 해당국가핵심기술을 외국기업 등에 매각 또는 이전 등의 방법으로 수출하고자 하는 경우에는 지식경제부장관의 승인을 얻어야 한다(제11조 제1항).

이밖에 산업기술에 대해서는 절취・기망・협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개하는 행위를 금하고 있다(제14조).

③ 대상기관은 산업기술의 유출방지 및 보호에 관한 시책을 효율적으로 추진하기 위하여 지식경제부장관의 인가를 받아 산업기술보호협회를 설립할 수 있고(제16조), 정부는 산업기술을 보호하기 위하여 산업보안기술의 개발 및 전문인력의 양성에 관한 시책을 수립하여 추진할 수 있다(제20조).

④ 산업기술의 유출에 대한 분쟁을 신속하게 조정하기 위하여 지식경제부장관 소속하에 산업기술분쟁조정위원회를 둔다(제23조).

⑤ 산업기술을 국내에서 사용하거나, 사용되게 할 목적으로 산업기술의 취득, 공개, 사용 등이 행위를 하는 경우에는 5년 이하의 징역 또는 5억원 이하의 벌금에 처한다(제36조 제2항). 특히 외국에서 사용하거나, 사용되게 할 목적으로 부정하게 취득, 공개, 사용하는 등 동법 제14조의 행위를 한 자에게는 10년 이하의 징역 또는 10억원 이하의 벌금으로 가중처벌하고 있다(제36조 제1항). 이 경우, 징역형과 벌금형을 병과할 수 있으며(제36조 제6항), 제14조의 침해행위에 대한 미수범도 처벌된다(제36조 제7항).

또 유출자가 침해행위로 얻은 이득액의 전부를 몰수할 수 있도록 규정하여, 침해자가 불법으로 기술을 획득함으로서 얻은 부당한 이익을 전부 몰수할 수 있도록 하고 있다(제36조 제4항). 이 밖에 동법은 산업기술침해행위에 대한 예비・음모죄를 규정하고 있으며(제37조)[12], 양벌 규정을 두어 침해자 개인뿐만 아니라 조직적인 기업형 산업기술 유출범죄도 처벌할 수 있는 근거를 마련하고 있다(제38조).

(3) 영업비밀보호법과 산업기술보호법의 비교

① 법률 체계상의 비교

영업비밀보호법은 기업의 영업비밀 침해행위에 대하여 형사처벌 등을 규정하고 있기는 하지만 사인(私人)간의 영업비밀 침해행위에 대한 민사적 구제수단을 주로 규정하여 사법적 성격이 강하다고 할 수 있다. 이에 반하여 산업기술보호법은 민사적 구제수단을 규정하지 아니하고 형사처벌만을 규정하면서, 산업기술 유출방지 및 보호 등에 대한 국가정책의

12) 국외 유출의 목적으로 예비 또는 음모한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하여 국내 유출의 2년 이하의 징역 또는 2천만원 이하의 벌금 보다 처벌이 크다.

수립 및 시행, 핵심기술에 대한 정부의 승인, 산업보안기술의 개발에 대한 지원제도 등을 규정함으로써 공법적 성격이 강하다고 할 수 있다.

산업기술의 유출방지 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 산업기술 보호법에 따르도록 되어 있으므로(법 4조), 산업기술의 유출방지 및 보호에 관한 사항에 대하여는 산업기술보호법이 우선적으로 적용되고 영업비밀보호법이 보충적으로 적용된다. 따라서, 산업기술보호법은 영업비밀보호법에 대한 특별법이라고 할 수 있다. 예를 들면, 산업기술보호법의 적용대상이 되는 산업기술을 보유한 기업의 직원이 비밀유지 의무에 위반하여 산업기술을 유출하였으나 산업기술보호법 제14조 2호에서 정한 “절취, 기망, 협박 그 밖의 부정한 방법”을 사용하지 않은 경우에는 산업기술보호법은 적용되지 않을 것이므로 영업비밀보호법은 적용될 수 있다.[13]

② 영업비밀과 산업기술

영업비밀보호법상의 영업비밀은 외국 기업의 영업비밀도 적용대상에 포함되나, 산업기술보호법상의 산업기술은 우리나라에서 독창적으로 개발된 기술만을 적용대상으로 한다고 생각된다.

또 영업비밀보호법은 “생산방법. 판매방법 기타 영업활동”에 유용한 정보로 규정하여 포괄적으로 규정하고 있으나, 산업기술보호법은 “제품이나 용역의 개발・생산・보급 및 사용”에 필요한 정보라고 한정적으로 정의하고 있다. 아울러 영업비밀보호법에서는 생산방법・판매방법 기타 영업활동에 “유용한” 정보일 것을 요건으로 하는 데 반하여 산업기술보호법에서는 개발・생산・보급 및 사용에 “필요한” 정보일 것을 요건으로 하고 있어 산업기술법상의 요건이 좀 더 엄격하다.[14]

---

13) 양영준, 위의 글, 29-30면.
14) 양영준, 위의 글, 30면.

③ 침해행위의 유형

영업비밀보호법에서는 비밀유지의무의 근거를 “계약 등에 의하여”로 규정하여 계약 이외의 사정으로 비밀유지의무가 발생하는 경우도 포함하고 있으나, 산업기술보호법에서는 “계약에 의하여”로 규정하여 계약 이외의 사유로 비밀유지의무가 발생하는 경우를 제외하고 있다.

또한 영업비밀보호법에서는 비밀유지의무에 위반하여 영업비밀을 누설하면 침해행위로 되지만, 산업기술 보호법에서는 “절취・기망・협박 그 밖의 부정한 방법으로 유출하는” 경우에만 침해행위로 된다. 그 밖에 산업기술보호법에는 국가의 승인 없이 국가핵심기술을 수출하거나 지식경제부 장관의 명령을 이행하지 아니하는 행위와 같이 영업비밀보호법에 없는 침해행위의 유형이 추가되어 있다[15].

2. 외국의 산업보안 제도 개관

1) 미국의 산업보안 관련 법령

① 제도의 도입과 전개

미국에서는 전통적으로 영업비밀(Trade Secret)의 침해행위를 불법행위(Tort)의 일종으로 보는 각 주의 판례법에 따라 영업비밀이 보호되었다. 이러한 판례법을 보다 체계화하기 위하여 1939년에 미국법률협회(American Law Institute)가 제정한 불법행위에 관한 리스테이트먼트(Restatement of the Law of Torts)에 영업비밀에 관한 조항이 최초로 도입되었다. 이후 1970년대 말부터 1980년대에 걸쳐 미국의 산업 경쟁력이 약화된 결과 산업경쟁력을 회복하기 위하여 지적재산권을 보호, 강화

15) 양영준, 위의 글, 31면.

하기 위한 소위 Pro-Patent 정책을 실시하였으며, 그 일환으로 1979년에는 미국법률가협회(American Bar Association)가 통일영업비밀법(The Uniform Trade Secrets Act)을 마련하여 각 주에 그 채택을 권고한 결과 대다수의 주가 이를 법률로 제정하여 시행하고 있다.

1988년에는 외국인이 미국의 기업을 실질적으로 지배하게 되는 인수 또는 합병을 함에 있어 그 인수 또는 합병이 미국의 주간 통상(Interstate Commerce)에 종사하는 자를 통제할 수 있는 결과를 야기할 수 있고 미국의 국가안전보장에 영향을 줄 수 있는 경우에는 대통령이 이를 조사하여 필요한 조치를 할 수 있는 것을 내용으로 하는 엑슨 플로리오조항(Exon-Florio Provision, 50 USC Appendix Section 2170)을 제정하였다.

이후 미국은 통일 영업비밀법이 영업비밀 침해행위에 대한 민사적 구제수단만 규정하고 영업비밀 불법취득행위에 대한 형사처벌을 규정하고 있지 않은 것을 보완하기 위하여 영업비밀(Trade Secret)을 불법으로 취득하는 행위, 이른바 산업스파이를 엄하게 처벌하기 위한 경제스파이법을 1996년 제정하였다(18 USC 제90장). 이 법률의 제정 계기가 된 것은 냉전시대가 끝나고 소위 경제전쟁 시대를 맞아 각국 정부가 미국 기업의 영업비밀을 탐지하는 사건이 빈번하게 발생한 데서 찾아 볼 수 있다.[16]

② 주요 내용

미국에서는 영업비밀이 침해된 경우 민사적 구제와 형사적 구제가 모두 가능하도록 되어 있다. 민사적 구제는 통일영업비밀법을 근간으로 각 주에서 제정한 주영업비밀법에 의해, 형사적 구제는 연방경제스파이법에 의해 이루어진다.[17]

16) 양영준, 위의 글, 6-7면.

17) 산업기밀보호센터, "주요국 법령정보(미국)", http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06&menu=ACF00(2010. 6. 16 검색)

통일영업비밀법은 1979년 영업비밀 보호에 관한 각 주의 판례법상 불균형 및 보호수준의 차이를 시정하기 위해 제정되었으며, 2000년 6월 현재 41개 주에서 동법과 동일하거나 유사한 영업비밀법을 채택하여 운영하고 있다. 상기 법을 채택하지 않은 주는 주 법원의 판례법이나 주 형법상 영업비밀 절도죄, 일반 절도죄 등을 통해 영업비밀을 보호한다.

영업비밀침해에 대한 법적 대응 규정을 보면, 영업비밀 유출 피해 시 금지청구권과 손해배상청구권을 인정하고, 특히 징벌적 손해배상(Punitive Damages)을 채택하여 고의 또는 악의에 의한 침해행위는 손해배상의 2배까지 청구가 가능하도록 하고 있다. 단, 별도의 형사적 처벌 조항은 없다.

경제스파이법(Economic Espionage Act of 1996)은 산업스파이 행위를 연방차원의 형사범죄로 규정하고, 연방정부의 수사·정보기관이 해당사건을 직접 수사할 수 있는 근거를 마련하기 위해 제정한 것인 바, 모든 침해 행위자(비목적범)에 대해 고소 없이 형사처벌이 가능(비친고죄)하며, 소송과정상 영업비밀의 기밀성 유지를 위한 법원명령 등이 가능하도록 규정되어 있다.

경제스파이법의 보호대상 범위는 통상정책은 물론 모든 형태의 재무·사업·과학·기술·공학 정보로 폭넓게 규정하고 있으며, 그 요건은 기업에게 경제적 가치가 있고 비밀보호 조치를 받고 있는 것으로 하고 있다.

형사처벌 규정을 보면, 외국정부·기관 등과 연계된 영업비밀의 유출행위에 대해서는 경제스파이죄로 가중처벌하나, 외국이 관여되지 않은 영업비밀 침해행위에 대해서는 영업비밀절도죄를 적용한다.

즉 외국 산업스파이에 대하여는 15년 이하의 징역형, 법인에 대하여는 1000만불 이하의 벌금형에 처하고 국내 산업스파이에 대하여는 10년 이하의 징역형, 법인의 경우에는 500만불 이하의 벌금형에 처하도록 되어 있다. 처벌의 대상이 되는 행위에는 영업비밀을 불법취득하는 행위는 물론 그러한 불법행위가 개입된 사실을 알면서 취득하는 행위도 포함되어

있다.[18] 미국의 영업비밀침해 처벌 규정을 정리하면 다음의 <표 2>와 같다.

<표 2> 미국의 영업비밀침해 처벌 규정

	개인	법인
산업스파이죄(국외)	15년 이하 징역 또는 50만불	1000만불 이하 벌금
영업비밀절도죄(국내)	10년 이하 징역 또는 50만불	500만불 이하 벌금

자료: 산업기밀보호센터, "주요국 법령정보(미국)", http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06&menu=ACF00(2010. 6. 16 검색)

2) 중국의 산업보안 관련 법령

① 제도의 도입과 전개

중국에서의 기술유출에 관한 보호는 우선 中華人民共和國反不正當競爭法(이하 부정경쟁방지법)을 들 수 있다. 중국의 부정경쟁방지법은 공정경쟁과 영업비밀보호 등을 위해 1993년 9월 2일 제정되어 1993년 12월부터 시행되고 있다.[19] 중국의 부정경쟁방지법은 그 제정 목적에서 사회주의 시장경제의 건전한 발전과 공평한 경쟁을 보호, 부정경쟁행위를 제지하고 경영자와 소비자의 합법적 권익을 보호하기 위해 제정되었음을 밝히고(동법 제1조), 동법에 영업비밀의 정의, 침해유형, 민사책임에 대하여 규정하고 있다.

부정경쟁방지법 외에 영업비밀보호를 위한 법제도로는 행정법규로서

18) 양영준, 앞의 글, 7면.

19) 중국의 부정경쟁방지법은 1993년 9월 2일 제8회 전국인민대표대회 제3차회의에서 통과되고 1993년 9월 2일 중화인민공화국 주석령 제10호로 공포되었다. 중국 부정경쟁방지법 전문(한국어번역문)은 다음을 참조, 산업기밀보호센터, "주요국 법령정보(중국)", http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06sub3&menu=ACF04(2010. 6. 16 검색)

영업비밀침해행위에 관한 규정이 있으며, 기타 영업비밀 관련 법률로서 민법통칙, 계약법, 회사법, 노동법 등이 있다.

특히 1995년 11월 23일에는 영업비밀침해금지에 관한 규정을 개정하는 등 영업비밀에 대한 보호를 강화해나가고 있는 추세에 있으며, 또한 노동시장의 유연성 증대로 인해 영업비밀 보호에 대한 요구가 증대되고 'TRIPS 협정' 규정과 보조를 맞추기 위해 1997년 형법을 개정하여 제219조에 '상업비밀에 대한 침해죄'를 새로이 규정하였다.[20]

② 주요 내용

중국의 부정경쟁방지법은 영업비밀에 대해 "공중이 모르고(不爲公衆所知悉), 권리자에게 경제이익을 가져다주며(能爲權利人帶來經濟利益), 실용성을 구비하고(具有實用性), 그 권리자가 비밀조치를 취한(經權利人采取保密措施) 기술정보와 경영정보를 말한다"고 규정하고 있다(동법 제10조).

위 규정에서와 같이 중국의 부정경쟁방지법상 보호대상은 기술상, 경영상의 정보이며, 소추요건은 비친고죄이다. 침해행위는 절도, 기망, 협박 기타 부정한 수단으로 권리자의 영업비밀을 취득하는 행위, 또는 전술한 수단으로써 권리자의 영업비밀을 공개·사용하거나 제3자가 사용하게 하는 행위이다.

영업비밀침해에 대한 법적 대응 규정을 보면, 민사적 구제는 상대방의 영업비밀을 침해한 자에 대해 손해배상책임 및 피침해자가 부정경쟁행위를 조사하기 위해 지불한 비용에 대한 배상책임을 부여하도록 되어 있다(동법 제20조). 행정적 구제를 보면 영업비밀 침해시 감독 조사기관이 위법행위 정지명령을 해야 하고, 사건 정황에 따라 1만-20만위안의 벌금

20) 산업기밀정보센터, "중국의 영업비밀보호제도", http://service4.nis.go.kr/servlet/notice?cmd=notice_view&no_idx=172&nm_code=global&curpage=5&lst_word=&lst_type1=&lst_type2=&lst_from=&lst_to=&listNum=7(2010. 6. 16 검색).

부과하도록 규정하고 있다(동법 제25조).

형사적 구제는 영업비밀 권리자에게 중대한 손실을 초래한 경우, 그 침해자에 대해 3년 이하의 징역이나 구금을 벌금과 병과하거나 혹은 벌금에 처할 수 있도록 규정되어 있다.[21] 침해행위로 인해 특별히 엄중한 결과를 초래한 경우에는 3년 이상 7년 이하의 징역과 벌금을 병과할 수 있다.[22]

3) 일본의 산업보안 관련 법령

① 제도의 도입과 전개

일본은 우리나라 부정경쟁방지법 개정(1991. 12. 31)보다 6개월 앞선 1990년 6월 29일 법률 제66호로 부정경쟁방지법을 개정하여 영업비밀 보호제도를 도입하였다. 일본의 영업비밀보호 관련 부정경쟁방지법은 우리나라와 대체로 유사하나 우리나라의 경우 영업비밀 누설행위에 대한 형사처벌을 규정한 데 반하여 일본의 부정경쟁방지법은 형사처벌을 규정하지 않았던 점에서 큰 차이가 있었다. 그런데 일본이 지난 10년간 산업경쟁력이 약화되고 경기침체를 겪으면서, 그 해결책으로 고이즈미(小泉) 전 총리가 지적재산권을 강조함으로써 소위 지재입국(知財立國)의 슬로건을 내걸고 pro.patent 정책을 적극적으로 추진하게 되었다. 구체적으로는 지적재산권의 보호범위의 확대, 지적재산권의 국제적 보호에 대한 대응으로서 노하우 부정유출 방지의 강화, 영업비밀을 포함한 지적재산권의 분쟁을 신속히 해결하기 위하여 재판외 분쟁처리(ADR) 제도의 추진 등이 포함되어 있었다. 이를 위하여 2002년 2월 25일 내각총리대신 및 관련부서 대신들과 전문가를 포함하는 지적재산전략회의가 설치되었고 지적재산전략회의는 2002년 7월 3일 지적재산 입국을 실현하기 위한 마

21) 산업기밀보호센터, “주요국 법령정보(중국)”
22) 산업기밀정보센터, “중국의 영업비밀보호제도”, 35면.

스터 플랜(Master Plan)인 지적재산전략대강(知的財産戰略大綱)을 작성하여 총리에게 제출하였다.[23]

지적재산전략대강은 창조전략, 보호전략, 활용전략, 인적기반의 충실 등 4가지 주요 내용으로 되어 있다. 보호전략에는 ①신속・정확한 심사의 실현, ②저작권의 적절한 보호의 도모, ③영업비밀의 보호 강화, ④분쟁처리에 관한 기반의 강화, ⑤해외에서의 보호의 강화 등이 포함되어 있다. 그중 영업비밀의 보호강화를 위하여 경제산업성(經濟産業省)이 취하여야 할 구체적인 행동계획으로서 "기업이 영업비밀의 관리강화를 위한 전략적인 프로그램을 책정할 수 있도록, 참고가 되는 지침을 2002년도 중에 작성한다. 더불어, 부정경쟁방지법 개정에 의한 민사・형사 양면에 걸친 영업비밀의 보호 강화에 대하여 인재유동화에 대한 억지효과 등, 이로 인해 생길 수 있는 문제점을 고려하면서, 2003년도 통상국회에 개정법안을 제출한다. 이때, 대학 연구원의 자유에 대하여도 배려한다."는 사항을 정하였다. 위 행동계획에 따라, 경제산업성은 2003년 1월 기업이 영업비밀을 강화하기 위해 참고해야 할 관리수준을 제시한 "영업비밀관리지침"을 공표하였다.[24] 나아가 일본 경제산업성은 2003년 3월 해외에서 활동하는 기업들의 의도하지 않은 기술유출을 방지하기 위하여 기업이 실무적으로 활용할 수 있는 "기술유출방지지침"을 제정하였다.[25]

② 주요 내용

일본은 한국, 미국, 독일 등 외국의 영업비밀보호 강화 추세 속에 첨단기술 유출에 대한 심각성을 보다 깊게 인식하고 2005년 6월 부정경쟁방지법을 개정하여 2005년 11월부터 영업비밀 침해죄 형벌수준을 높이고(5년 이하의 징역 또는 500만엔 이하의 벌금), 영업비밀 국외사용 및 공개

23) 양영준, 앞의 글, 7면.
24) 양영준, 위의 글, 8면.
25) 산업기밀보호센터, "주요국 법령정보(일본)", http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06sub2&menu=ACF03(2010. 6. 16 검색).

행위 처벌, 퇴직자에 의한 영업비밀의 사용·공개행위 처벌, 법인 처벌 등이 가능토록 규정하고 있다. 또 영업비밀의 누설 교사·방조자도 정범으로 처벌토록 하고 있다. 실제 산업스파이 활동을 하다 검거되면 부정경쟁방지법 외에 형법상 절도죄, 사기죄, 횡령죄, 장물죄, 배임죄 등 각종 재산죄와 비밀누설죄, 信書개피죄, 주거침입죄 등으로 처벌이 가능하며, 영업비밀 침해죄는 공소제기에 피해자 등의 고소를 필요로 하는 친고죄로 처벌도 가능하다.[26]

이밖에 일본은 공무원이 외국공관원과 접촉 시 사전승인 및 사후보고하는 시스템을 제도화하고, 경제산업성 등 부처·사안별로 기술유출방지지침 및 지식재산취득관리지침 등을 제정하여 의도하지 않은 기술유출에 대한 방지대책을 강화하고 있으며, 최근에는 '특허'의 경우도 국가안보와 관련된 내용은 공개하지 않는 방안을 추진하고 있다.

이 중에서도 일본 경제산업성이 2003년 3월 제정한 기술유출방지지침은 기술라이선스 및 기술원조와 관련된 기술유출 등 의도하지 않은 기술유출이 발생하는 7가지 주요 유형을 설명하고 선진기업의 대응사례를 통해 기업이 참고할만한 기술유출 방지대책을 제시하고 있다. 방지대책은는 해외 진출 시 기술이전 전략, 사내 조직체제, 사업활동, 사내 교육, 사후관리 등 경영 전반적인 내용으로 구성되어 있다[27] .

4) 독일의 산업보안 관련 법령

독일은 산업스파이에 대하여 직접 규정한 단행법체계 없이 영업비밀의 보호 차원에서 부정경쟁방지법(UWG: Gesetz gegen den unlauteren Wettbewerb)을 통해 규율하고 있는 바, 1909년 제정된 이래 영업비밀보호와 관련하여 지속적으로 처벌의 확대 및 강화의 방향으로 법개정이 이

26) 산업기밀보호센터, "주요국 법령정보(일본)"
27) 일본 경제산업성의 기술유출방지지침 전문(한국어 번역문)은 산업기밀보호센터, "주요국 법령정보(일본)"에서 참조.

루어져왔다.

부정경쟁방지법은 우리나라의 영업비밀보호법과 유사하나, 친고죄를 원칙으로 하고 공공의 이익을 위해 필요하다고 인정되는 경우에만 피해자의 고소 없이 기소 가능하도록 규정되어 있다. 영업비밀 침해 시 3년 이하 징역 또는 벌금 부과가 가능하며 외국으로 유출 시 5년 이하의 징역에 처하도록 규정되어 있다. 독일의 경우 영업비밀 침해에 대한 미수범은 인정되나 예비・음모는 처벌할 수 없다.[28]

한편 독일은 최근 자국기업을 대상으로 한 외국 산업스파이들의 공세가 증대됨에 따라 산업보안 관련 법제를 강화하는 한편으로 헌법보호청을 통해 기업과의 긴밀 협조체제 구축하여 산업보안을 강화하는 대책을 강구하고 있다.[29]

28) 산업기밀보호센터, “주요국 법령정보(독일)”, http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06sub1&menu=ACF02(2010. 6. 16 검색).

29) 독일 기업이 산업스파이로 인해 입는 피해액은 매년 500억 유로로 추산되고 있으며, 그간 주로 대기업이 경제정보 수집 목표가 되어오다 현재는 중소·신규업체까지 확대되고 있다. 특히 자동차·에너지원천재생·화학·통신기술, 광전자공학, 방위기술 및 디지털제어시스템 등 향후 경제적 잠재력이 큰 분야가 목표가 되고, 침해국 중 개도국들은 자체개발·특허 비용을 절약하기 위해 첨단기술 획득에 치중하는 반면, 선진국들은 혁신방안·융합기술 및 시장전략 입수에 주력하고 있다. 외국 산업스파이의 수법을 보면, 독일기업들의 전산망과 컴퓨터시스템들에 대한 해킹수법이 이용되고 있으며, 중국 정보기관의 경우는 여전히 고전적 수법을 구사하여 주로 유학생·연수생·학자 등 신지식의 획득에 열의가 있고 기업 내부 정보에 접근할 수 있는 비전문가들을 활용하여 정보를 수집하고 있다. 산업기밀보호센터, “獨 헌법보호청, 외국 산업스파이 방어대책 강화”, http://service4.nis.go.kr/servlet/notice?cmd=notice_view&no_idx=182&nm_code=global&curpage=4&lst_word=&lst_type1=&lst_type2=&lst_from=&lst_to=&listNum=15(2010. 6. 16 검색).

Ⅳ. 산업보안범죄의 실태와 대응방안

1. 산업기술 유출 유형과 수사사례분석

1) 유출 유형

국가정보원 산업기밀보호센터에 의하면, 지난 2004년부터 2009년까지 국내 첨단기술을 해외로 불법유출하려다 적발된 사건이 총 203건인 것으로 나타나고 있다. 적발된 산업기밀 유출 현황을 연도별로 살펴보면, 그 적발 건수가 2004년 26건에서부터, 2005년 29건, 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건으로 지속적 증가하고 있다<표 3>.

<표 3> 연도별 산업기술 유출 현황

단위: 건수

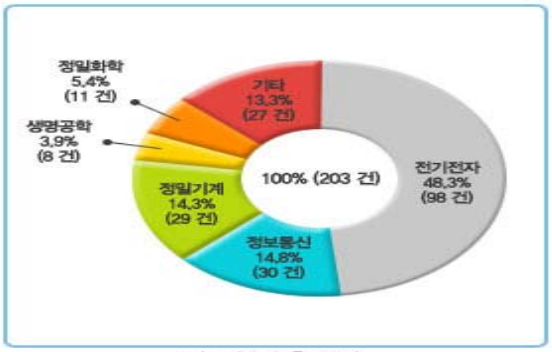
계	2004	2005	2006	2007	2008	2009
203	26	29	31	32	42	42

자료: 산업기밀정보센터, “기술유출 통계” http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00(2010. 6. 16 검색)

2004년 이후 나타난 산업기술유출 현황을 다시 유형별로 살펴보면,

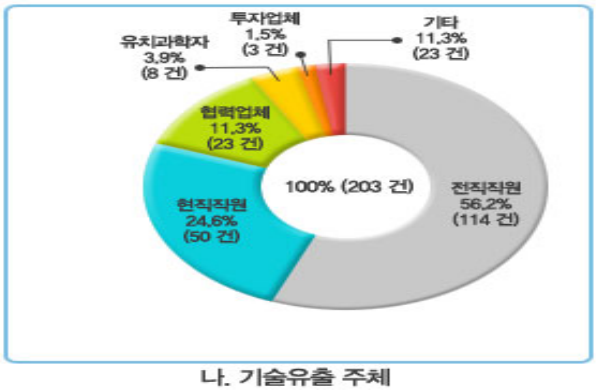
(가) 우선 유출분야에서는, 총 203건 중 전기전자 분야가 가장 많은 98건(48.3%)으로 나타났다. 다음으로 정보통신 30건(14.8%), 정밀기계 29건(14.3%), 정밀화학 11건(5.4%), 생명공학 8건(3.9%), 기타 27건(13.3%)로 나타나고 있다. 전체 유출품목 중에서도 반도체, 휴대폰 등 전기전자와 정보통신 품목이 유출품목의 대종을 차지하고 있으나 최근에는 자동차,

조선을 포함한 기계, 화학 등 거의 전분야로 확대되고 있는 추세이다.



가. 기술유출 분야

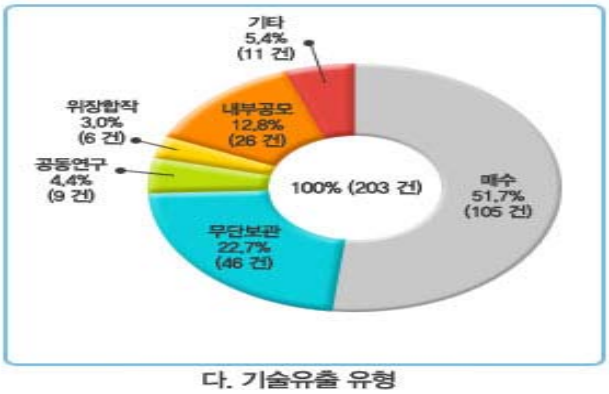
(나) 2004년 이후 나타난 산업기술유출 유형을 그 유출주체별로 살펴보면, 전직 직원 114건(56.2%), 현직 직원 50건(24.6%), 협력업체 23건(11.3%), 유치과학자 8건(3.9%), 투자업체 3건(1.5%)의 순으로 나타나고 있다. 주로 전·현직 직원(164건, 80.8%)에 의한 기술유출이 가장 많은 부분을 차지하고 있으나 최근에는 협력, 용역업체에 의한 기술유출 사례도 점차 증가하고 있음에 주목할 필요가 있다.



나. 기술유출 주체

(다) 산업기술유출 유형을 유출수법별로 살펴보면, 매수 105건(51.7%), 무단보관 46건(22.7%), 내부공모 26건(12.8%), 공동연구 9건(4.4%), 위장합작 6건(3.0%) 등의 순으로 나타나고 있다. 매수의 경우, 연구원 등 개인을 대상으로 금전적 유혹을 유발시키는 매수 형태가 일반적이나, 기업 차원의 공동연구 및 위장합작을 통한 유출 유형도 증가하고 있다.

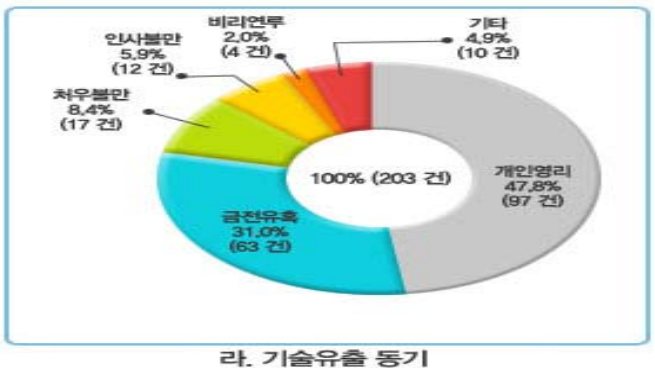
개인 차원을 넘어 기업 차원에서 조직적으로 이루어지는 형태로까지 발전되고 있는 위장합작의 수법은 최근의 M&A를 통한 기술유출 사례에서 확인된다.[30]



다. 기술유출 유형

(라) 산업기술유출 유형을 유출동기별로 살펴보면, 개인영리 97건(47.8%), 금전유혹 63건(31.0%), 처우불만 17건(8.4%), 인사불만 12건(5.9%), 비리연루 4건(2.0%) 등의 순으로 나타나고 있다.

30) 노호래는 산업기밀유출된 사례를 개인형과 M&A형으로 나누고, M&A를 통한 기술유출의 대표적인 사례로『중국 비오이그룹의 LCD관련 하이디스 M&A 사례』(한국경제신문, 2007. 4. 18)와『중국 상하이차그룹의 쌍용차 M&A 사례』(한국경제신문, 2007. 4. 18)를 들고 있다(노호래, 2008: 62-63).



라. 기술유출 동기

2) 검거실적 및 수사사례분석

최근 국내의 각종 첨단산업기술이 경쟁업체 나아가 국외 업체로 유출되고 있는 사례들이 증가하여 이제 산업기술유출이 경쟁기업간의 문제를 넘어 국가차원의 문제로 대두됨에 따라 개별기업 및 민간산업단체 뿐만 아니라 각국의 정보·수사기관 또한 산업기밀 보호활동에 총력을 기울이고 있다. 이에 따라 경찰에서도 산업기술 보호활동을 더욱 강화하기 위하여 2004년 3월 경찰청 및 각 지방청에 산업스파이신고센터를 개설·운영하고 2004년 9월에는 각 지방경찰청 별로 산업체·연구소 보안담당자와 경찰관으로 구성되는 '산업보안협의회'를 구성하여 매년 정례회의를 개최해 왔다. 또한 수사역량 강화를 위하여 전국 지방경찰청에 전문수사인력을 편성하고 경찰청 외사수사과에 전담수사대(국제범죄수사대)를 운영하여 첨단 산업기술유출 관련 수사 활동을 적극 전개하는 한편, 전문교육내실화를 통한 수사요원의 역량 강화 도모, 국정원 등 관계기관과의 정보공유를 활성화, 인터폴·해외 주재관과의 원활한 공조수사체제 구축 등 첨단산업기술 보호 및 국부유출 방지를 위한 적극적인 노력을 기울이고 있다.

경찰의 이러한 산업기술 보호활동 속에서 2004년 15건이던 산업기술 불법유출 검거건수는 2005년 19건으로 늘어났고, 2006년 16건으로 다소 안정 양상을 보이다가 다시 2007년 25건, 2008년 72건으로 크게 증가하고 있는 추세를 보이고 있다. 그에 따라 첨단산업기술 유출로 인한 피해액은 2004년 2004년 1조원에 못 미치던 것이 2008년에는 15조를 상회한 것으로 추산되고 있다<표 4>.

<표 4> 연도별 산업기술 불법유출 검거실적 및 피해추산액

단위: 건, 원

구 분	2004	2005	2006	2007	2008
건수	15	19	16	25	72
피해 추산액	9,435억원	1조 4,949억원	6조 3,509억원	4조 459억원	15조 770억원

자료: 경찰백서, 2008: 313; 2009, 295

2008년도 검거실적을 검거인원 측면에서 살펴보면 해외 불법유출 23명, 국내 불법유출 사범은 132명으로 총 155명으로 나타나고 있다. 특히 국내유출의 경우는 피해추산 100억-1000억 이상이 110명으로 전체 국내유출의 대부분을 차지하고 있으나, 해외유출의 경우에는 전체 23명 중에 1000억 이상 5명, 1조원 이상은 무려 14명으로서 고부가가치의 첨단산업기술이 해외유출을 겨냥한 범죄자들의 유출목표가 되고 있음을 알 수 있다<표 5>.

<표 5> 2008년 산업기술 불법유출사범 검거실적(인원)

단위: 명

구 분	총 계	첨단 산업기술				
		1조이상	1천억이상	500억이상	100억이상	100억미만
해외유출	23	14	5	1	1	2
국내유출	132	10	41	19	50	12

자료: 경찰청 일보, 2009. 2. 23.

이처럼 2008년도에 급증세를 보인 첨단산업기술 불법유출 사건들을 경찰청 본청 및 각 지방청의 대표적인 수사사례(2008. 4 - 2010. 5)들을 중심으로 하여 검거일 순서에 따라 구체적으로 살펴보면 다음과 같다.

● 첨단 산업기술 유출사범 2명 검거(경찰청 일보, 2008. 4. 29)

【개 요】

인천경찰청에서는 휴대폰 키패드, 정밀자동차부품 등 첨단부품 조립용 '지그(Jig)' 제작 영업기밀을 경쟁사에 불법 유출하고, 동종 제품을 생산・판매한 피의자 검거(불구속 2).

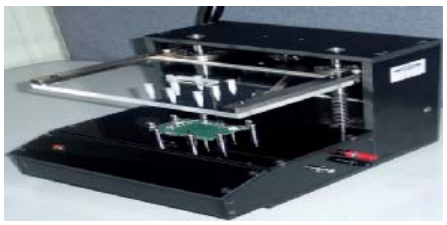
【범죄사실】

- 2007. 10월경 A社 기술영업대리 이○○ 등 2명은 피해사에서 3년간 약 10억원을 투자하여 개발한 휴대폰키패드, 정밀자동차부품 조립용 '지그(Jig)' 제작 핵심 영업기밀을 복사 유출하고,

- 경쟁사인 B社를 설립, 유출한 '지그(Jig)' 제작기술 등을 이용하여 동종의 제품을 생산, 판매한 혐의.

※ 지그(Jig) : 기계가공에서 가공위치를 쉽고 정확하게 정하기 위해 부품을 고정시켜주는 틀

※ 예상 피해액 100억원.



주: 좌측 사진(원제품), 우측 사진(유출제품)

【적용법조】

- 영업비밀보호법 제18조 제2항.
- 형법 제356조(업무상 배임).

● 첨단산업기술 해외유출 피의자 검거 (경찰청 일보, 2008. 5. 8)

【개 요】

경기경찰청에서는 자신이 근무하던 회사에서 개발된 첨단산업기술인 '고화질 HD영상 수신기' 제조 핵심기술을 중국으로 유출 시도한 피의자 11명 검거.

【범죄사실】

- 김○○(42세, 티본社 대표이사) 등 11명 피의자들은 피해회사(홈캐스트社)에 기술개발팀장 등으로 근무한 자들로,
- 2007. 5. 17일경 중국 경쟁업체와 합작社를 설립, 회사가 4년간 약 400억원의 연구비를 들여 개발한 '고화질 HD영상 수신기' 제조 핵심기술을 해외로 유출 시도한 것임.

※ 업계 추정 피해예방액: 향후 5년간 약 1조5천7백억원.

● 첨단산업기술 유출 피의자 검거(경찰청 일보, 2008. 8. 29)

【개 요】

경찰청 국제범죄수사대에서는 자신이 근무하던 회사에서 개발한 첨단산업기술 '덴탈 임플라그라피' 설계도를 미국계 경쟁업체에 유출한 피의자 검거.

【범죄사실】

- 진○○(45세, 구속영장 신청, 피해회사 前 기술연구소장)는 2004. 6. 1 ~ 2006. 4. 30일까지 치과용 의료기기 개발사업체인 ○○社의 기술연구소장으로 근무한 자로,

- 同社가 2003 ~ 2006년까지 약 41억원의 연구비를 들여 개발한 첨단 치과용 의료기기 '덴탈 임플라그라피'의 설계도를 외장하드에 저장하여, 2006. 12. 1일 국내에 있는 미국계 경쟁업체인 ○○社로 이직하면서 유출한 것임.

※ 향후 5년간 피해예상액은 2조 2천억원 상당(피해업체 추산).

※ 덴탈 임플라그라피(Dental Implagraphy)는 치과시술(임플란트 등)을 할 때 필요한 360° 촬영기, 컴퓨터 단층 촬영기, 측면 촬영기를 하나로 통합한 차세대 치과용 의료기기.

【적용법조】

- 영업비밀보호법 제18조 제1항 등

● 첨단 산업기술 유출사범 2명 구속 등 12명 검거 (경찰청 일보, 2008. 6. 23)

【개 요】

경찰청에서는 (주)파카코리아 전·현 임직원들이 공장 자동화 설비에 사용되는 부품의 핵심 설계기술을 취득한 후, (주)슈어텍을 설립하여 동종제품 생산·판매한 피의자 검거 (구속 2, 불구속 10).

【범죄사실】

- 황○○(52세, 前 (주)파카코리아 연구개발실 상무, 現 (주)슈어텍 기술상무) 등 12명 피의자들은 (주)파카코리아에서 8년간 약 135억원 투자·

개발한 공장 자동화설비에 사용되는 부품의 핵심 설계기술 등 영업비밀 부정 취득 후 퇴사하여,

- 경쟁업체 (주)슈어텍 설립 후, 동종제품을 생산하여 약 10-20% 저렴한 가격으로 판매하는 등 재산상 손해를 가한 것임.

※ 예상 피해액 302억원

파카코리아 생산 '공압실린더'	슈어텍 생산 '공압 실린더'
압축된 공기압 에너지를 이용하여 구동하는 기기	

파카코리아 생산 '공기압 청정기기'	슈어텍 생산 '공기압 청정기기'
Filter (여과기) + Regulator (압력 조절기) + Lubricator (윤활유 분사기)	

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제2항
- 업무상 배임 (형법 제356조)
- 2008. 6. 20일 15:00 구속 전 피의자심문 후 영장발부(중앙지법)

- 2008. 6. 26일 서울 중앙지검 송치 예정.

● 경제안보사범 2건 8명 검거 (경찰청 일보, 2008. 6. 30)

【개 요】

대구경찰청에서는 전략물자 불법유출사범 2명 외에 첨단 산업기술 유출사범 6명 검거

【범죄사실】

- 김○○(47세, B社 상무이사) 등 6명은 피해사인 (주)A社 임직원으로 근무하다 '자동차 드럼 브레이크' 생산 설계도면 등 기술정보를 유출하고,

- 동종의 (주)B社를 설립, 유출한 A社의 영업비밀인 '제품 설계도면' 등을 C社에 제공 등의 혐의.

※ 피해예방액 300억.

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제2항.
- 업무상횡령・배임죄.
- 불구속 송치.

● 첨단 산업기술 유출사범 2명 검거(경찰청 일보, 2008. 7. 17)

【개 요】

경기 용인경찰서에서는 국내 최초로 개발한 '2중유리 습기 제거장치' 생산기술을 경쟁업체에 유출하는 등 영업비밀을 불법유출, 사용한 피의자 2명 검거(불구속)

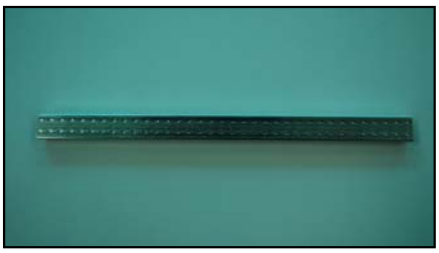
【범죄사실】

- 서○○(57세, (주)B社 대표) 등 피의자 2명은 피해사인 A社로부터 '웰딩스페이스바(2중유리 습기제거 장치)' 생산기계를 주문제작 의뢰받아 생산납품 후, 경쟁업체인 C社 대표와 공모하여,

- A社에서 10년간 40억원을 투자해 연구개발한 영업비밀인 동 제품의 설계도를 불법사용하여, 동일한 생산기계와 '웰딩스페이스바'를 생산・판매한 혐의.

※ 예상 피해액 200억원.

【제품 생산라인】



【웰딩스페이스바】

※ 웰딩스페이스바 : 2중유리 사이에 삽입하는 습기 제거 장치로, 그간 해외시장에서 100% 수입해 사용하던 것을, 피해업체에서 국내 최초로 개발.

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제2항.
- 수원지검 불구속 송치.

● 첨단 산업기술 유출 사범 2명 검거 (경찰청 일보, 2008. 8. 7)

【개 요】

부산경찰청에서는 첨단기술인 전자카메라 주변기기 전자회로도・도면 등 영업비밀을 불법 유출, 동종 제품 생산・판매한 피의자 2명 검거(불

구속).

【범죄사실】

- 2007. 4월경 엄○○(36세, 前(주) A社 해외 영업부장) 등 피의자 2명은 (주)A社에서 7년간 2억 5천만원을 투자하여 연구개발한 전자카메라 주변기기 설계도면 및 해외거래처 명단을 유출하여,

- 동종업체인 (주)B社를 설립, 불법 유출한 전자카메라 설계도・전자회로도 등을 이용, 동종의 제품을 중국 및 국내에서 생산・판매하고,

- (주)A社 소유인 전자카메라 유・무선릴리즈 1셋트 절취 한 혐의.

A社 생산 유・무선'릴리즈

'B社 생산 유・무선'릴리즈'

※ 유・무선'릴리즈' : 카메라 주변기기로 떨림 방지용 셔터기

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제2항.
- 형법 제329조.
- 2008. 8. 6일 부산지검 불구속 송치.

● 첨단 산업기술 해외 유출사범 3명 검거(경찰청 일보, 2008. 8. 25)

【개 요】

서울경찰청에서는 최첨단 홈네트워크 '음성인식시스템' 생산기술을 해

외에 불법 유출, 유사제품을 생산·판매한 피의자 3명 검거(불구속).

【범죄사실】

- 피의자 김○○(41세, (주) T社 기술부장)는 안양시 소재 S전자 기술개발팀장으로 근무하다 2007. 7월 퇴사하면서 자신의 회사에서 3억3천만원 상당을 투자해 독자적으로 기술개발한 홈네트워크 '음성인식 시스템' 기술을 유출하여,
- 경쟁사인 T사에 제공하고, T사 대표 마이클○(47세, 한국계 미국인)와 공모하여 동 기술을 태국의 M사에 다시 유출, OEM방식으로 동종의 '홈네트워크' 기기를 생산, 태국 등에 판매한 혐의.

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제1항, 제2항.
- 형법 제314조(업무방해), 제356조(업무상 배임).
- 서울 남부지검 불구속 송치.

● 첨단 산업기술 해외유출 미수범 5명 검거(경찰청 일보, 2008. 9. 2)

【개 요】

경기경찰청에서는 국내업체에서 세계 최초로 개발한 '원자력 내 방사선 컬러 카메라' 기술과 제작도면 등 영업비밀을 불법취득, 일본 경쟁업체로 불법 유출을 기도한 피의자 5명 검거(불구속).

【범죄사실】

- 피의자 인적사항

① 황○○(39, (주) H社 영업부장) ② 정○○(37, (주) H社 영업차장)

③ 신○○(48, W병원 연구원) ④ 이○○(47, K대학 교수)

⑤ 유○○(48, S기업 대표)

- ①·②의 피의자는 안양시 소재 H사에 영업 부장·차장으로 각 근무하며 회사운영이 어려워지자 2006. 10월 한국○○공사와 합동으로 개발한 '원자력 내 방사선 컬러 카메라'의 제작·영업기술을 유출하고,

- ③~⑤의 피의자들과 공모하여 동종업체를 설립하고, 취득한 자료를 일본의 경쟁업체에 불법 유출하려다 미수에 그친 혐의.

※ 예상 피해액 : 약 400억원.

※ 유출하려한 자료는 2006. 10월 세계 최초로 개발 후 상용화 단계에 있는 기술로, 방사선에 의한 고장이 발생하지 않는 기능을 갖춰 원자력 발전소 방사능 환경감시 및 핵 연료검사 등 다양한 분야에 사용되는 첨단 산업기술.

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제2항
- 수원지검 안산지청 불구속 송치

● 첨단산업기술 유출 피의자 검거(경찰청 일보, 2008. 11. 13)

【개 요】

2008. 11. 12일 경남경찰청에서는 자신이 근무하던 회사의 첨단산업기술인 풍력발전기·항공기 엔진코팅 핵심기술을 유출, 해외에 있는 경쟁업체로 넘기려 한 피의자 검거.

【범죄사실】

- 윤○○(39세, 피해회사 前기술팀장)는 1999 ~ 2008. 10월간 '엔진부품 특수코팅' 제조업체인 (주)A社의 기술팀장으로 근무한 자로서,

- 2008. 8월경 중국(대련) 소재 동종 경쟁업체인 (주)B社에 이직하는 것을 조건으로 (주)A社가 약 10억원의 연구비를 들여 개발한 '엔진부품 특수코팅' 관련 핵심기술을 외장하드에 저장하여 넘기려 한 것임.

※ 유출시 향후 5년간 피해예상액은 약 60억원 상당(업계 추산).

※ 同 기술은 풍력발전기, 전투기, 구축함 등 엔진부품을 특수코팅하여 내열성・내구성을 강화하는 첨단기술임.

〔특수코팅 로봇〕

〔T-50전투기 엔진코팅 장면〕

【적용법조】

- 영업비밀보호법 제18조 제1항, 제2항.

● '첨단핵심 산업기술' 해외 유출사범 검거(경찰청 일보, 2008. 12. 22)

【개 요】

경찰청에서는 S社에서 세계 최초로 개발한 '동시 냉・난방, 급탕 시스템' 핵심기술 등 영업비밀을 중국 경쟁업체인 M社에 불법유출한 피의자 6명 검거.

【범죄사실】

- 2008. 3월경 (주)S社 대표이사 계○○(40세・남)은 同社에서 독자 개발한「케스케이드 열교환기」핵심기술이 수익성이 상당하다는 사실을 인

식하고, 부정한 이득을 취할 목적으로 임원진과 사전협의 없이,

- 중국 M社 한국지사장 등과 공모, 同社에서 영업비밀로 관리하는 핵심기술도면 및 시제품을 해외(중국)에 유출.

※ 케스케이드(cascade)열교환기 : 기존 열교환기는 냉·난방 겸용이 불가능하였으나, 동 제품의 경우 동시 냉·난방 및 급탕 기능이 가능한 첨단 시스템으로서 2007년 국내시장규모가 수조원에 달하며, 중국산 저가 판매 시 국내업체 큰 타격 예상.

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제1항, 제2항.
- 특허법 제225조 등.
- 2008. 12. 22일 기소의견 관할지검(서울중앙지검) 불구속 송치.

● '첨단 섬유소재' 생산기술 해외유출 미수범 검거(경찰청 일보, 2008. 12. 15)

【개 요】

경찰청에서는 국내 P社에서 개발한 'PTMEG(첨단섬유 원료)' 생산기술을 부정취득, 피의자 명의로 특허등록 후, 중국 C社에 기술 유출 시도한 미수범 검거.

【범죄사실】

- 김○○(64세, S社 대표이사, P社 前기술연구소장)는 2000.10월부터 2005.12월까지 P社 기술연구소장으로 재직하다가, 2007.10월부터 현재까지 S社 대표이사로 재직 중인 자로서,
- 2005.12월 P社에서 퇴직하면서 43억원을 투자하여 독자 개발한 영업비밀인 'PTMEG' 제조방법 등 기술자료를 부정취득 후, 피의자 명의로

특허출원・등록(2건)하고,

- 중국 C社로 기술유출을 시도하다 미수에 그침.

※ 기술유출 시 향후 10년간 예상 피해액 약 1조 2천억원 추정.

※ PTMEG : 수영복 등 스포츠의류・속옷 등에 사용되는 고급 신축성 섬유소재로 전량 수입에 의존하였으나, 피해회사에서 1996년 국산화 성공. 기존에는 미국・일본・독일 등 3개국만 생산기술 보유(국내 시장규모 연 3,000억)

【적용법조 및 조치사항】

- 영업비밀보호법 제18조 제1항, 제2항, 제18조의 2.
- 2008. 12. 15일 서울 중앙지검 불구속 송치.

● '휴대폰 카메라' 핵심기술 해외 유출사범 검거(경찰청 일보, 2009. 2. 19)

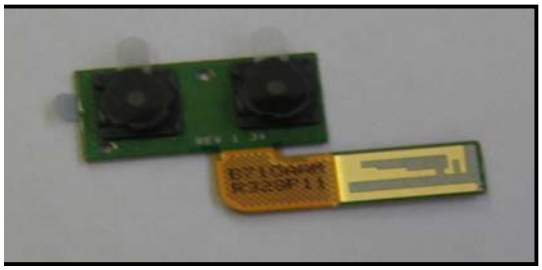
【개 요】

경기경찰청에서는 휴대폰 카메라 핵심기술인 '고화질 입체영상(3D) 카메라′ 설계도 등 영업비밀을 불법취득, 일본 경쟁업체로 유출 기도한 피의자 검거(불구속).

【범죄사실】

- 조○○(48세, 前 (주) A社 소형카메라 개발팀장)는 (주)A社에서 2년간 93억원을 투자, 연구개발한 휴대폰 차세대 핵심기술 '고화질 입체영상 카메라′ 설계도・구성도 등을 외장형 하드에 저장, 퇴사하면서 불법유출,
- 동종업체 설립을 목적으로 경쟁업체인 일본 (주)B社에 핵심서류인 '사업제안서'를 송부하는 등 외에 유출하려다 미수에 그친 혐의.

※ 예상 피해액 : 약 1,000억원.



※ 고화질 입체영상(3D) 카메라: 2대의 카메라를 이용(휴대폰 내부에 장착) 입체영상 구현 및 저장・전송이 가능한 시스템

【적용법조 및 조치사항】

- 영업비밀보호법 제18조의 2(해외유출 미수).
- 수원지검 불구속 송치.

● 유압식 드릴머신 기술유출 피의자 검거(경찰청 일보, 2010. 3. 11)

【개 요】

충북경찰청에서는 2010. 3. 5일 대전 대덕구 소재 ○○기공 연구실에서 압수수색 및 하드디스크 증거분석 등을 통해 기술유출 관련자료 확보 후 피의자 2명 검거(불구속).

【범죄사실】

- 박○○(57세, 남) 등 피의자 2명은 피해회사의 영업이사 및 연구원으로 근무하던 중 유압식 드릴머신 설계도 등을 유출하기로 공모하고,
- 2009. 5월경 퇴직, 설계도면을 경쟁업체로 유출하여 동종제품을 생산・판매한 것임.

※ 향후 5년간 예상피해액 : 약 169억원

● '자동차 알루미늄 휠 열처리 爐 제작' 기술유출 피의자 검거(경찰청 일

보, 2010. 3. 25)

【개 요】

경남경찰청에서는 2010. 3. 22일, 기술유출 피의자 4명 검거(구속 2명).

【범죄사실】

- 김○○(49세, 구속) 등 피의자 4명은 피해회사의 지사장 및 기술 총책임자로 근무하던 중 피해회사가 16억원의 연구비를 투자하여 개발한 '자동차 알루미늄 휠 열처리 爐' 제작 설계도면 등을 유출하기로 공모하여,

- 2009. 6월경 피해회사를 퇴직하며 핵심 설계도면을 유출하여 동종업체를 설립, 제품을 생산·판매하고 중국 경쟁업체에 유출한 것임.

● **산업기술유출 피의자 검거(경찰청 일보, 2010. 4. 2)**

【개 요】

대구 성서경찰서는 2010. 4. 1일 보도블럭 등에 사용하는 벽돌을 생산하는 '블럭성형기계' 설계도면을 유출, 동종업체를 설립하여 제품을 제작·판매하고 중국 관련업체에 판매한 피의자 검거.

【범죄사실】

- 피의자는 김○○(43세)는 피해회사 前 하렉스엔지니어링에 근무하던 중 10억원을 들여 개발한 설계도면을 유출하기로 결심하고,

- 2007. 5월 퇴직하여 동종업체 G정공을 설립, 제품을 제작·판매하고 중국 경쟁업체(H과기)에 유출한 것임.

● **'無毒不燃性 고무바닥재' 기술유출 피의자 검거(경찰청 일보, 2010. 5. 6)**

【개 요】

대구경찰청에서는 피해社 前기술연구소장 기술유출 피의자 3명 검거.

【범죄사실】

- 유○○(49세, 남) 등은 2006. 7월경 피해회사가 정부지원금 등 50억원을 들여 개발한 '무독불연성 고무바닥재' 핵심정보가 담긴 보고서를 동종업체에 유출한 뒤, 입사하여 제품을 제작·판매하려한 것임.

경찰이 검거한 산업기밀 주요 유출사례들을 살펴본 결과, 앞선 유형분석에서 본 바와 같이 분야별로는 정보통신, 섬유소재 품목들도 있으나 전기전자가 대부분을 차지하고 있다. 산업기밀을 유출한 주체와 동기로 보면, 용역업체에 사례도 있지만 대부분 퇴직직원 또는 현직직원들이 개인 영리와 금전 유혹 등 경제적 동기에 의해 이루어졌던 것으로 나타났다.

해외 유출사례의 경우 중국으로의 유출이 가장 많았으며 그밖에 일본, 태국 등으로의 유출도 발생하고 있는 것으로 나타났다.

해외 유출사례에서 특히 주목할 것은 고부가가치의 기술 유출 위험이 높다는 것이다. 앞서 2008년 해외 유출사건 피의자의(23명)의 60% 이상이 피해 추산 1조원 이상에 연루되었던 사실은, '고화질 HD영상 수신기' 제조 핵심기술 중국유출 미수사건**(향후 5년간 업계추정 피해예방액, 약 1조 5천 7백억원)**, 첨단 치과용 의료기기 '덴탈 임플라그라피'의 설계도의 미국계회사 유출사건**(향후 5년간 피해추산액, 2조 2천억원)**, 'PTMEG(첨단섬유 원료)' 생산기술 중국유출 미수사건**(향후 10년간 업계추정 피해예방액, 약 1조 2천억원)** 등에서 뚜렷이 보여준다.

2. 제도적 대응방안

본 연구는 체포되어 유죄판결을 받을 가능성(being caught and convicted) 즉 처벌의 가능성(probability of punishment)을 높이는 한편, 처벌의 엄격성(severity of punishment)에 의해 범죄비용(f)의 증가를 가져오는 제도운용에 의해 산업보안범죄의 억제(deterrence)를 모색해 보고자 한다. 그 대응방향의 주요 내용으로는 제도 설계(institutional design) 단계에서 법규 정비와 산업기술보호기관의 확충, 제도 집행(implementation) 단계에서 정보·신고시스템의 개선, 관계자간 범죄대응 협력체계의 구축, 홍보·교육활동의 강화 등을 제시하고자 한다.[31]

1) 관련법규의 정비

산업보안범죄에 대한 처벌의 엄격성을 높이기 위하여 첫째, 산업기술 유출의 위험(risk) 방지를 위한 국내 법제가 지속적으로 정비되어 갈 필요가 있다. 현재 산업보안 관련법제는 크게 영업비밀보호법과 산업기술보호법이 이원화되어 있어서 두 법률에 형사적 규제의 중복성[32], 형량의 모호성이 존재하는 바[33], 이를 적절하게 보완해야 할 것이다.

---

31) 본 연구는 신제도주의 제도 시각 중에서도 노스(North) 類의 넓은 의미의 제도 개념을 원용하고 있다. 노스의 제도 개념 범주에는 법·규칙과 같은 공식적 제약(formal constraints) 뿐만 아니라 관습이나 행동양식과 같은 비공식적 제약(informal constraints)들이 포괄된다(North, 1990: 4). 그에 따라 본 연구의 제도적 대응방안도 법규 외에 제도 내 행위자로서 조직(기관), 이행당사자간 협력체계 구축 등 넓은 범위에서 접근되었다.

32) 양 법률은 절취, 기망, 협박, 부정한 방법으로 산업기술(영업비밀)을 취득, 사용, 공개하는 행위를 금지하고 있다(영업비밀보호법 제2조 제3호 가목, 산업기술보호법 제14조 제1호). 또한 전득자에 의한 유출확산을 방지하기 위하여 양 법률은 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 당해 산업기술(영업비밀)의 취득 후에 부정 취득한 사실을 알거나 중과실로 알지 못하고 당해 산업기술(영업비밀)을 취득, 사용, 공개하는 행위를 금지하고 있으며(영업비밀보호법 제2조 제3호 나목 및 마목, 산업기술보호법 제14조 제3호), 산업기술(영업비밀)의 취득 후에 부정취득된 사실을 알거나 중과실로 알지 못하고 당해 산업기술(영업비밀)을 사용. 공개하는 행위를 금지 유형에 포함하여 선의로 취득한 자라 하더라도 후에 이를 악의적으로 사용.공개하는 것을 규제하고 있다(영업비밀보호법 제2조 다목 및 바목, 산업기술보호법 제14조 제4호).

33) 현행 영업비밀보호법상의 벌칙규정은 형량의 모호함으로 인하여 오히려 2004년 개정전보다 영업비밀 침해행위에 대한 형사처벌을 더욱 어렵게 했다는 지적이 있다(조용순.홍영서, 2006 : 297-298). 즉, 동법은 재산상 이득액의 2배 이상 10배 이하의 벌금을 규정하고 있는데, 실제 기술유출로 인한

우선 영업비밀보호법과 산업기술보호법의 이원적 체제로 나아가되, 영업비밀보호법은 본래 취지에 맞게 영업비밀 침해행위에 대한 민사적 규제에 관한 사항만을 규정토록 하고, 공공성이 높은 산업기술보호법은 그동안 국내 법제에서 미흡했던 '사전적' 보안체제 확립에 대한 근거 법률적 역할과 함께 기술유출 억제를 위한 강력한 형사적 규제를 담당하도록 양 법률의 역할을 이원화시키는 방안이 바람직할 것이다.

즉 기술유출행위를 국익의 보호차원에서 규제하려는 국제사회의 흐름에 따라 기술유출행위에 대한 형사처벌에 대해서는 산업기술보호법의 규율대상으로 통합하고, 민사적 규제에 대해서는 기존의 영업비밀보호법에서 규율하도록 한다(조용순・홍영서, 2006 : 309-310). 이를 통하여 양법률의 중복적인 부분에서 야기되는 충돌을 방지하고, 각 법률의 목적에 따라 그 기능을 강화함으로써 보다 나은 산업보호 법제를 완성해야 할 것이며, 특히 산업기술보호법 위반 시에 적용될 엄중한 형사처벌 규정을 명백히 해야 할 것이다(노호래, 2008: 67).

2) 산업기술보호기관의 확충

검거(arrest)를 통한 처벌가능성을 높여 산업보안범죄의 확산을 억제하는 차원에서 유관 보호기관의 확충을 고려할 수 있다. 현재 산업보안활동과 관련된 정부의 조직은 국가정보원(산업보안관련 정보수집), 지식경제부(산업보안 관련 정책의 입안과 집행), 경찰과 검찰(산업보안범죄 수사) 등에 분산되어 있다.

산업보안활동의 효율성과 효과성 확보를 위해서 관련된 정부조직을 분산형보다는 통합적 방향으로 정비하는 것이 이상적일 수도 있다. 그러나 산업보안활동 유관 조직을 모두 통합하는 것은 현실적이지도 않고 또한

이득액을 특정할 수 없을 뿐만 아니라, 실제로 영업비밀의 가치가 수천만원에서부터 심지어 수조원에 이른다고 주장하는 경우 사실상 벌금형을 선택할 수 없는 문제점이 있다(노호래, 2008: 58).

과도한 권한집중이라는 점에서 바람직하지 않은 측면도 있다.

따라서 현재와 같이 조직상 독자성을 가지고 움직이되 특히 경찰의 경우 다른 기관보다 범죄위험 일선현장에서의 상시적인 정보, 검거활동이 가능하기 때문에 그 조직을 더욱 확충할 필요가 있다. 이는 베커(Becker)와 에리히(Ehrlich) 등 많은 연구자들의 견해 즉, 검거확율에 대한 범죄자들의 위험인지 제고가 형량 강화에서 오는 고통(suffering)의 크기 혹은 범죄비용(f) 제고 보다 더 효율적인 형사사법 정책수단이라는 분석에서도 그 필요성이 발견된다.

경찰조직에서 산업보안 업무는 경찰청(지방청) 외사국(외사과)에서 관장하고 있으므로 외사부서 내의 산업보안 조직과 기능을 강화해야 할 것이다. 산업보안 전문수사조직의 효과적 운용을 위해서는 수사요원들의 체계적 양성이 필수적이며 여기에는 국내외 산업보안 관련 법제도의 이해, 국제적 첨단산업기술보호 동향 정보수집 및 분석, 수사기법 등에 대한 보다 심화된 전문화교육과정이 마련되어야 할 것이다. 또한 산업보안 전문교육, 정보분석과 자문을 위하여 산업보안 분야에 고도의 기술력과 지식을 가진 전문가 풀을 확보할 필요가 있다.

3) 산업보안 정보 · 신고시스템의 강화

산업기술유출 범죄자로 하여금 처벌가능성 및 범죄비용에 대한 인식을 제고시키고 실제 산업보안범죄 검거율을 높여가기 위해서는 적발과 수사에 필요한 관련 정보를 적실성(relevance), 정확성(accuracy), 적시성(timeliness), 필요성(necessity)을 갖추어 수집(collection), 생산(production), 배포(dissemination) 해낼 수 있는 산업보안정보관리시스템이 구축되어야 한다.

이러한 정보는 산업기술유출 통제에 대한 종합적 · 장기적인 정책수립에 필요한 정보(전략적 성격), 일선 현장에서의 탈법행위 적발에 필요한

정보(전술적 성격), 그리고 위험의 예방과 관리에 활용할 수 있는 정보(방어적 성격)가 전체적으로 망라되어야 할 것이며, 이러한 요구들이 해결될 수 있도록 경찰을 비롯한 각 유관 기관들의 정보시스템 즉, 경찰청의 범죄정보관리시스템(CIMS, Crime Information Management System), 전략물자관리원의 정보시스템인 예스트레이드(yestrade.go.kr), 관세청의 통합정보시스템(CDW, Customs Data Warehouse) 등이 효율적으로 구축되어야 한다.

나아가 정보수집, 조사, 수사 등 각 업무분야에 분산돼 있는 산업보안 기능을 통합해 전략적인 판단에 기초한 미래위험 대비를 추진할 필요가 있는 바, 이를 위해 각 기관들의 정보시스템을 연계하여 종합적인 핵심기술보호정보시스템으로 발전시켜 나가는 것이 바람직하리라고 본다. 아울러 조사기법을 고도화할 필요가 있다. 즉 엄격한 불법유출통제를 위해 거시적 측면에서 종합적 위험관리정보시스템을 마련해 나가는 한편 미시적인 측면에서 연관관계분석(Link Analysis) 등 선진적 조사기법을 개발해 나가는 것이 바람직하다.

산업보안 규정 위반에 대한 단속과정에서 주의해야 할 것은 규정 위반 물품에 대한 과다한 단속이 정상적인 국내외 경제활동・교역활동을 억제하는 결과를 초래하지 않도록 해야 한다는 점이다. 이에 대한 대책의 하나로 위험관리(risk management) 기법을 도입하여 운영하는 방안을 고려할 수 있다. 즉 자체 정보 또는 업무협조를 통한 자료를 기초로 첨단산업기술 품목과 생산업체 등을 고위험(high risk) 및 저위험(low risk) 분야로 구분하고 이중에 특정품목별, 유출주체별, 특정지역별로 우범성이 높은 대상으로 집중 단속하는 것이 바람직하다. 예컨대 경찰의 검거사례에서 본 바와 같이 분야별로는 전기전자・정보통신 분야, 주체면에서는 전・현직 담당직원, 유출국가에서는 중국 등에 관심을 두어야 할 것이다. 특히 해외 유출의 경우는 고부가가치 품목의 기술 유출 위험이 높기 때문에 이에 대한 정보관리・분석이 뒤따라야 할 것이다.

정보시스템 개선과 함께 신고시스템운용이 활성화될 필요가 있다. 현재 국정원에서는 NIS 111콜센터[34] 내에 국제범죄/테러 관련 범죄신고 등과 함께 주요 안보범죄로서 산업스파이 신고가 운영되고 있고 경찰청에서도 2004년 3월부터 사이버경찰청 및 각 지방청 홈페이지에 산업스파이신고센터를 개설·운영해 왔다. 이처럼 경찰과 국정원에서는 각 기관의 홈페이지에 산업스파이신고센터를 개설하여 운영하고 있으나 일반 국민에 숙지되지 못한 면이 있고, 특히 경찰청의 사이버112[35] 내에 운영되는 현재의 산업스파이 신고는 일반인들이 보다 접근하기 편리하도록 개편할 필요가 있다. 향후 경찰청에서는 첨단산업기술 침해의 심각성을 홍보하는 한편 신고에 따른 보상(rewards for reporting) 즉 포상금 지급 등 인센티브를 제도화하여 산업보안범죄 제보가 활성화되도록 산업보안범죄신고센터의 운영 프로세스를 개선해야 할 것이다.

4) 관계자간 범죄대응 협력체계의 구축

산업보안범죄의 처벌가능성과 엄격성을 효율적으로 높이기 위해서는 무엇보다 관계자간 거버넌스(governance) 구축 차원 내지 관민파트너쉽(PPP: Public Private Partnership) 구축 차원에서 주요 이해관계자간의 상호협력의 관행과 행위규범을 축적해나가는 것이 매우 중요하다.

범죄대응에서의 협력관계의 구축을 위해서 첫째로, 우리 정부 내부적으로 먼저 경찰청과 유관부처간 상호협력을 활성화하고 이를 제도화해야 할 필요가 있다. 경찰청은 국정원을 비롯한 관세청, 지식경제부 등과 함께 협력체계를 확대하여 산업보안범죄 대응역량을 강화시켜나가야 할 것이며, 여기에는 구체적으로 정보시스템 연계운용, 홍보활동 공동추진, 상호 인력지원, 상호 전문교육훈련과정 참여, 강사진 지원, 분기별 정보교

34) http://www.nis.go.kr/app/center/prosecute_w?pCode=49(2010. 6. 10 검색).
35) http://cyber112.police.go.kr/main/index.do(2010. 6. 10 검색).

류 정례회의 개최 등이 포함될 수 있다. 정보교류 정례회의에서는 유관기관간 정보연락관제도를 도입해 위험동향 정보를 정기적으로 상호 제공하는 한편, 정례 전략 정보회의를 열어 분야별 현황정보에 대한 체계적인 분석을 통해 각종 위험을 선정, 등급별로 차별화된 대응전략을 도출토록 한다.

유관기관간 협력에서 또하나 중요한 것은 중소기업의 기술유출과 관련한 중소기업청과의 협조이다. 최근 해외 산업기술의 유출분야를 보면 첨단 전자·정보통신 분야에서 자동차·조선을 포함한 기계·화학 등 거의 전 분야로 품목이 확대되고 있고, 특히 대기업에 비해 중소·벤처기업에서의 기술유출 사건이 지속적으로 늘어나고 있는 추세가 발견된다. 따라서 중소기업의 기술유출을 방지하기 위한 임직원의 산업보안 의식제고와 보안시스템 구축 지원확대 등에서 중소기업청과 공조할 필요가 있다.

둘째, 경찰청은 유관기관간 정보교류 및 업무협력을 강화하는 한편으로 첨단산업기술 관련업체로부터 적극적인 참여와 협조관계를 이끌어낼 필요가 있다. 경찰청은 민간부문으로부터 참여와 협력관계를 발전시킴으로써 자율적 법규준수(Informed Compliance) 제고, 정보교류 및 정보수집 범위 확대의 효과를 기할 수 있다.

현행 산업기술보호법에 따르면 산업기술을 보유한 기업・연구기관 등 대상기관은 산업기술의 유출방지 및 보호에 관한 시책을 효율적으로 추진하기 위하여 지식경제부장관의 인가를 받아 산업기술보호협회를 설립할 수 있도록 되어 있다.[36] 또 지방경찰청 및 경찰서 산업보안 담당 외사요원이 참석하고, 산업체의 보안담당자 등이 참석하는 산업보안협의회가 운영되고 있다. 경찰청은 이러한 산업기술보호협회, 산업보안협의회 등을 통해 정보 수집 등 산업기술 유출 예방활동 관련 민간 산업체의 협조를 제도화하는 것이 바람직하다. 이를 위해 경찰에서는 산업보안 수사사례 소개 및 유출차단 방안 정보 등을 업계에 제공하는 한편, 첨단산업

36) 산업기술보호법 제16조.

체 보안담당자의 애로사항과 개선의견을 수용하여 경찰의 산업보안활동에 적극적으로 반영할 필요가 있다.

5) 홍보·교육활동의 강화

산업기술 유출자들이 경제적 이익의 확보를 위해 불법적 행동을 선택하는 데 있어서 고려되는 처벌의 확률(P)은 객관적 확률이 아니라 범죄자가 인식하는 주관적 확률(subjective probability)이다. 따라서 지속적인 산업보안범죄 방지 홍보와 교육을 통해 범죄의 중대성과 차단의지, 엄격한 처벌 사례들을 인식시킴으로써 산업보안범죄를 억제하는 노력이 매우 중요하다. 이런 점에서 경찰청에서 진행한 바 있는 산업보안 관련 홍보 노력들이 더욱 강화될 필요가 있다.[37]

특히 산업보안범죄는 유출자와 피해회사 이외 일반시민의 경우 그 직접적인 피해를 느끼지 않기 때문에 불법 유출이 초래하는 사회적 비용의 문제점에 대한 인식이 높지 못하다. 이러한 산업보안범죄에 대한 낮은 의식과 유출 관련자들의 도덕적 해이는 첨단기술의 해외 유출의 경우 경제안보 차원에서 더욱 심각하다. 따라서 산업보안범죄를 피해자 없는 범죄가 아니라 국가안보와 경제질서를 해할 수 있는 범죄이며 반드시 적발·처벌되는 중대한 범죄라는 사실을 인식시키기 위해서 경찰을 비롯한 정부기관에서는 업계에 대한 홍보활동을 강화하여야 한다. 아울러 기업으로 하여금 연구원 등 내부 직원 등에게 산업기술 유출 방지에 대한 지속적인 교육을 실시토록하고, 이를 통해 산업보안범죄 차단을 위한 노력에 적극 참여하는 업체들에 대해서는 행정적 편의와 보안활동 지원 등이 뒤따르도록 구조화된 범죄대응 유인체계(structured incentive system)를 마련해야 할 것이다.

---

37) 서울경찰청에서는 보안의식 제고와 기술유출 사전 차단의 일환으로 지난 2009. 11. 27 - 12. 26일간 산업기술유출방지를 위한 홍보영상물 CD를 산업체·연구소(70개) 해당업체에 직접 배포하여 社內 세미나 등에 적극 활용토록 한 바 있다(경찰청 일보, 2009. 11. 27).

Ⅴ. 결 론

본 연구는 국제사회의 치열한 경제전쟁과 첨단과학기술 시대에 우리나라의 선진국 안착을 위한 첨단기술 보호와 불법유출 차단의 필요성 문제를 제기하고, 최근의 산업기술 유출방지 제도 하에 발생해 온 산업보안범죄의 실태를 점검하면서, 합리적 선택에 기반한 범죄경제학과 신제도주의 시각에서 산업보안범죄에 대한 제도적 대응방안을 모색해보고자 하였다.

본 연구는 산업보안범죄에서의 처벌가능성을 높이는 한편, 처벌의 엄격성에 의해 범죄비용의 증가를 가져오는 제도운용에 의해 불법기술 유출을 억제하는 방안을 구상하면서 그 대응방향의 주요 내용으로 제도 설계 단계에서 법규 정비와 산업기술보호기관의 확충, 제도 집행 단계에서 정보·신고시스템의 개선, 관계자간 범죄대응 협력체계의 구축, 홍보·교육활동의 강화 등을 제시하였다.

본 연구의 핵심논지는 경제적 이익을 목표로 한 산업보안에서의 탈법위험 최소화를 추구하되, 동시에 억제과정에서 비용이 상대적으로 적게 발생하도록 하는 제도를 고안(design), 운용하자는 것이다. 그에 따라 신제도주의 시각에서 접근된 대응과제들을 제시하였으며 그중에서도 가장 강조된 것은 위험관리(risk management)와 거버넌스(governance)적 기조에서의 제도구상이라고 할 것이다.

즉 탈법위험성이 높은 고부가가치 품목과 유출주체, 유출국가 등에 대해서는 감시를 강화하고 또한 고의적 법규 위반자에 대해서는 무관용(zero tolerance) 원칙에 의해 엄격히 처벌하되, 저위험(low risk) 분야에 대해서는 감시절차를 탄력적으로 운용하고 이중 법규준수업체에 대해서는 다양한 인센티브 제도를 구조화(structured incentive system)하여 차별적으로 대응토록 한 것이다. 산업보안 수요의 증가에 따라 공공기관의

조직 확충이 요구되고 있으나, 거버넌스적 시각 혹은 민간참여에 의한 넓은 의미에서 관민파트너쉽을 통해 산업보안 관련 당사자가 함께 참여하는 상호협력체계를 형성함으로써 조직신설 비용, 대리인 비용의 발생을 억제하는 협력통제제도의 구축을 도모하자는 것이다.

우리 경찰뿐만 아니라 민간부문을 포괄한 산업보안 관련 참여자들은 산업보안 관련제도들을 국내 시장활동과 국제거래의 규제장벽으로 이해하는 수동적 자세에서 벗어나, 효율적 산업기술 유출 통제를 통해 탈법위험 최소화뿐만 아니라 비용 최소화를 함께 달성함으로써, 우리나라를 아시아 경제산업허브와 선진 정상국가로 안착시키도록 하는 능동적 자세를 견지해야 할 것이다.

참고문헌

경찰청 일보, 2008. 4 - 2010, 5.

경찰청, 산업보안실무, 2007.

경찰청, 경찰백서, 2005-2009.

국가정보원, 산업보안 FOCUS, 2004. 7.

국가정보대학원, 산업보안실무, 2006.

노호래, “산업기술 유출범죄에 대한 정책적 대응방안”, 한국공안행정학회보, 제30호, 2008.

녹색성장위원회, 녹색성장 국가전략, 2009. 7.

민병설, 산업보안체계의 정립에 관한 연구, 경희대 박사학위논문, 2002.

법제처 국가법령정보센터, “부정경쟁방지 및 영업비밀보호에 관한 법률 연혁”, http://www.law.go.kr/LSW/lsSc.do?menuId=0&p1=&subMenu=1&searchName=LicLs%2C0&query=%EC%98%81%EC%97%85%EB%B9%84%EB%B0%80%EB%B3%B4%ED%98%B8&x=13&y=18#liBgcolor0(2010. 6. 10 검색).

사법연수원, 신종범죄론, 2004.

산업기밀보호센터, “기술유출 통계”, http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00(2010.6. 10 검색).

산업기밀보호센터, “獨 헌법보호청, 외국 산업스파이 방어대책 강화”, http://service4.nis.go.kr/servlet/notice?cmd=notice_view&no_idx=182&nm_code=global&curpage=4&lst_word=&lst_type1=&lst_type2=&lst_from=&lst_to=&listNum=15(2010. 6. 16 검색).

산업기밀보호센터, “주요국 법령정보”, http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=law_06&menu=ACF00(2010. 6.

16 검색).

산업기밀보호센터, “중국의 영업비밀보호제도”, http://service4.nis.go.kr/servlet/notice?cmd=notice_view&no_idx=172&nm_code=global&curpage=5&lst_word=&lst_type1=&lst_type2=&lst_from=&lst_to=&listNum=7(2010. 6. 16 검색).

양영준, “「산업기술의 유출방지 및 보호에 관한 법률」에 관한 소고”, http://service4.nis.go.kr/servlet/board?cmd=bo_view&no_idx=42&cd_code=industrial&curpage=1&menu=ADC00(2010. 5. 1 검색).

조병인 외, 사이버범죄에 관한 연구, 한국형사정책연구원, 2000.

조용순・홍영서. “산업기술 유출규제에 관한 법적 고찰”, 산업재산권, 21권, 한국산업재산권법학회, 2006.

Eggertsson, T., *Economic Behavior and Institutions*, Cambridge University Press, 1990.

Eide Erling, Paul H. Rubin, and Joanna M. Shepherd, *Economics of Crime*, Hanover: now Publishers Inc., 2006.

North, D. C., *Institution, Institutional Change and Economic Performance*, Cambridge University Press, 1990.

Ostrom, E., “An Agenda for the Study of Institutions”, *Public Choice*, 48, pp. 3-25, 1986.

Wikipedia, “Industrial technology”, http://en.wikipedia.org/wiki/Industrial_technology(2010. 6. 20 검색).

Williamson, Oliver E., *The Economic Institutions of Capitalism*, New York: Free Press, 1985.

Winkler, I., *Corporate Espionage*, Rocklin, CA: Prima Publishing, 1997.

Winter H., The *Economics of Crime: An introduction to rational crime analysis*, New York: Routledge, 2008.

책임연구보고서 2010-09

산업보안범죄의 제도적 대응방안

2010년 9월 30일 발행

발행인 : 이 종 우

발행처 : **치안정책연구소**
경기도 용인시 기흥구 언동1길 29

홈페이지 : www.psi.go.kr

POLICE SCIENCE INSTITUTE