민간조사원(탐정)을 활용한 기업보안활동의 강화방안: 산업 스파이에 대한 대응방안을 중심으로*

A study on The Private Investigator usage for Enterprise Security Activity: Focusing on countermeasure to the Industrial Spy

신 성 균** · 박 상 진***

〈목 차〉

〈요 약〉

1990년대 초 이후 탈냉전 시기에 들어서면서 다양한 안보위험 요소가 등장함에 따라 국가안보의 개념이 전통적인 군사력 위주에서 경제력으로 옮겨 갔다. 국가안보 개념의 변화로 각국은 국가이익 확보를 위하여 외국에 대한 경제정보·산업정보활동에 주력하게 되면서, 이에 대응하기 위한 산업기술보호 활동도 국가안보차원에서 수행하게 되었다.

미국 등 주요 선진국들은「경제스파이처벌법」등을 제정·시행하는 등 자국의 첨단산업 기밀을 보호하기 위하여 강력한 보호 정책을 추진하고 있다.

우리나라는 IT, 조선, 철강, 자동차 등의 분야에서 세계적 수준에 도달하였고 매년 막대한 자금을 첨단기술의 및 개발에 투자하고 있으나 지금까지 체계적인 산업보안활동이 전개되지 못한 실정이다.

하지만 이러한 산업보안은 특성상 공적인 사법기관의 독자적인으로는 수사를 하는데 많은 어려움을 겪는 것이 사실이다.

따라서 민간조사원이 은밀하게 기업사건에 개입하여 증거를 수집하고 정보를 입수하여 위험성을 사전에 확인하고 조치·예방하는 것이 효과적일 것이다. 신속하게 처리해야 하는 범죄를

* 본 연구는 2009 춘계학술대회에서 발표한 논문임.
** 삼성 에스원 상무(제1저자).
*** 백석대학교 법정학부 강사(교신저자).

조사하는데 효과적인 민간조사제도를 국가의 공적인 사법기관이 개입하기 곤란한 산업스파이와 같은 기업범죄 등에 활용함으로서 기업 뿐만 아니라 국가, 나아가 국민의 경제의 손실을 예방할 수 있는 제도가 될 수 있을 것이다.

여기서는 이러한 점을 인식하고 민간조사원(탐정)을 활용한 산업 스파이 대응방안을 제시하고자 한다.

주제어 : 민간조사원, 기업보안, 산업스파이, 경찰

I. 서 론

최근 미래를 주도할 기술 개발에 대한 중요성이 강조되고 있다. 사회가 발달하면서 국가의 부와 미래는 자본과 노동보다 얼마나 혁신적인 기술을 많이 보유하고 있는가에 의해 좌우되기 때문이다. 그동안 우리나라는 조선・자동차・정보기술(IT) 등을 주력산업으로 성장시켰으며 외환위기 이후에도 21세기에 걸맞은 차세대 신 성장동력 육성을 위해 국가 차원의 대형 연구개발(R&D) 사업들을 추진해왔다.

국가안보 개념의 변화로 각국은 국가이익 확보를 위하여 외국에 대한 경제정보・산업정보 활동에 주력하게 되면서, 이에 대응하기 위한 산업기술보호 활동도 국가안보차원에서 수행하게 되었다. 이에 따라 각국은 세계적인 무역자유와 추세와는 상반되게 법적・제도적으로 산업기술보호 체계를 강화하고 있다(이창수, 2008: 4).

미국 등 주요 선진국들은 「경제스파이처벌법」 등을 제정・시행하는 등 자국의 첨단산업 기밀을 보호하기 위하여 강력한 보호 정책을 추진하고 있다. 우리나라에서도 그동안 기술유출보안 관리 및 보안사고 후 대응에 있어서 다소 소극적인 측면이 있었으나, 1998년 '삼성전자 반도체기술의 대만 유출 사건'을 계기로 비교 우위에 있는 각종첨단산업 기술에 대한 보호・관리의 필요성이 제기되었으며, 1998년「부정경쟁 방지 및 영업비밀 보호에 관한 법률」의 제정과, 이후 몇차례의 개정을 통해 산업보안활동에 대해서 국가적인 관심을 넓혀 나가고 있다. 또한 2007년 4월 28일부터 발효된 「산업기술의 유출방지 및 보호에 관한 법률」이 제정되었다. 기존의 「부정경쟁 방지 및 영업비밀 보호에 관한 법률」은 민간의 기업비밀 누설에만 처벌이 한정되어 있고 각종 법률에 산재해 있는 관련규정으로는 산업기술유출방지에 큰 효과를 내지 못하였다. 이에 따라 국가안보에 직접적인 영향을 미치는 국가 핵심기술의 해외유출을 규제하고, 산업기술의 부정한 유출을 방지하기 위해 「산업기술의 유출방지 및 보호에 관한 법률」을 제정하였다.(노호래, 2008: 48 참고). 또한 한편으로는 2007년 10월에 민간 단체인 「한국산업기술보호협회」가 설립되어 민간차원의 산업기술 보호활동이 활성화되는 계기를 맞게 되었다.

특히 우리나라는 IT, 조선, 철강, 자동차 등의 분야에서 세계적 수준에 도달하였고 매년 막대한 자금을 첨단기술의 개발에 투자하고 있으나 지금까지 체계적인 산업보안활동이 전개되지 못한 실정이다. 따라서 국가와 민간기업은 세계적인 경쟁력을 갖춘 우리나라 산업기술의 유출을 방지하고 이를 효과적으로 보호할 필요가 있다(노호래, 2008: 48 참고).

특히 산업기술 유출통로의 한 축으로, 피해를 당하면 기업 뿐만 아니라 국가적으로 막대한

손실을 보게 되는 산업스파이의 경우, 기업이 관심있게 살펴봐야 할 부분이다. 하지만 이러한 산업스파이는 공적인 사법기관이 제대로 수사를 하는 데에 많은 어려움이 있다.

이러한 점을 고려할 때 민간조사원이 은밀하게 기업사건에 개입하여 증거를 수집하고 정보를 입수하여 위험성을 사전에 확인하고 조치・예방하는 것이 효과적일 것이다. 신속하게 처리해야 하는 범죄를 조사하는데 효과적인 민간조사제도를 국가의 공적인 사법기관이 개입하기 곤란한 산업스파이와 같은 기업범죄 등에 활용함으로서 기업 뿐만 아니라 국가, 나아가 국민의 경제의 손실을 예방할 수 있는 제도가 될 수 있을 것이다.

따라서 여기서는 이러한 점을 인식하고 민간조사원(탐정)을 활용한 산업 스파이 대응방안을 제시하고자 한다.

Ⅱ. 이론적 배경

1. 민간조사원(탐정)의 의의

탐정의 사전적인 의미는 "남의 비밀한 일을 은근히 알아내거나. 범죄사건을 추적하여 알아내는 일, 또는 그 일에 종사하는 사람"을 말한다. 영어로 Private Detective 혹은 Private Investigation이라 부르는 탐정이란 수수료를 받고 범죄와 관련된 사항, 신원조회, 증인의 신빙성, 사람의 소재, 재산의 소재 등에 관한 정보를 찾아주는 일 혹은 그러한 일을 하는 사람을 말한다(하정용, 2005:13).

한편 국세청에서 분류한 소득표준율 분류코드(코드번호 749200)에 의하면 탐정이란 "개인 및 재산을 위한 탐지, 감시, 보호 등과 지문채취, 거짓말탐지 및 화재예방 상담, 필체 감정 등의 서비스를 제공하는 업"이라고 정의하고 있다.

미국에서는 "PI"라는 약자의 사립조사관이 사실상 사립탐정을 의미하는 만큼 "Private Investigation"가 점점 일반화 되어가는 추세이다(이동영, 2003: 19).

국내에서는 1999년 공인탐정법안(하순봉의원안)에서 "공인탐정"이라는 용어를 사용하고 있으며, 최근 이상배의원과 최재천의원은 민간조사업법안에서 "민간조사원"이라는 용어를 쓰고 있으며 한국체육대학 김두현 교수와 국제공인탐정연구소 소장 겸 대불대학교 경찰학부 이동영 교수 역시 탐정이라는 용어가 가져다주는 부정적인 이미지와 미국에서 일반화된 "PI"의 해석 그대로 민간조사원의 용어가 적절하다고 주장하고 있다.

이렇게 용어만으로도 많은 견해가 대립하고 있는데 공인탐정법안의 국회 입법과정에서 국민의 의견을 수렴하는 많은 공청회와 학술세미나에서 조차 용어통일이 되지 않고 있는 것은

국민 모두에게 혼선 뿐만 아니라 입법안 자체에도 긍정적인 반응을 얻을 수 없으라는 것이 발제자의 판단이다. 따라서 용어통일이 시급한 시점에서 발제자가 감히 제안하고자 하는 용어로는 기왕이면 국민들에게 용어자체가 친숙해 있고 업무적 관련성을 포괄적으로 부각시키는 명칭이라는 점에서 "공인탐정"이라고 칭하는 것이 탐정제도가 우리사회에 정착하기에 도움이 될 것이라 여겨진다.

2. 산업 스파이의 의의 및 발생원인

1) 산업스파이의 의의

스파이(Spy, Espionage)라 함은 상대방의 허점을 공략하고 보안조치를 무력화시켜 유용한 정보를 획득하는 일련의 과정을 가르킨다(Nasheri, 2005: 13). 원래 스파이의 어원은 '멀리 본다' 또는 '숨겨져 있는 것을 목격 또는 발견한다'라는 의미의 고대 프랑스어 'espier'가 변화한 것으로 알려져 있다(조병인 외, 2000: 41). 현대에 와서 이 개념은 국가간에 외교, 군사에 관한 정보를 한 나라의 정부요원이 비밀리에 정탐, 수집하는 행위를 가르키는 것이었다(사법연수원, 1999: 246). 이러한 스파이는 미국의 CIA와 구 소련의 KGB가 대표적이다. 냉전체제가 붕괴되어 더 이상 미국과 소련, 자본주의와 공산주의의 대결이 무의미하게 되자, 이제는 국제적 경제패권주의에 의하여, 외교, 정치적 정보와 함께 첨단기술을 개발한 산업체를 상대로 산업기밀을 수집, 탐지하는 산업스파이의 문제점이 전면에 대두되게 되었다.

이렇게 경제적 목적으로 산업비밀 등을 비밀리에 입수하기 위하여 상대국의 기업, 회사를 대상으로 스파이활동이 전개될 때, 이를 통상 산업스파이(industrial espionage) 또는 경제스파이(economic espionage)라고 한다.[1)]

경제스파이는 특정 국가의 경제적 경쟁력을 제고하기 위한 목적으로 첩보수집이 행하여지며 국가가 이를 지시, 지원 또는 조정하는 첩보수집활동을 말한다. 반면에 산업스파이는 시장경제에 있어서 경쟁적 우위를 점하기 위하여 행해지는 정보활동에 대해 산업체나 개인기업의 지원 또는 협조로 이루어지는 정보수집활동을 말한다(이윤호, 2004: 303).

이렇게 볼 때, 산업스파이란 상대국 기업, 회사가 소유하고 있는 물품의 제조방법, 판매방

1) 각국이 산업스파이를 활용하는 이유는 다음과 같다. 첫째, 국가 또는 기업이 전략적으로 육성한는고자 하는 특정 분야의 기술을 개발하기 위하여 소요되는 시간과 재정지출을 줄일 수 있다는 점이다. 둘째, 특정 기술을 개발하였다고 하여도 대량생산을 위한 생산기술의 습득이 매우 중요하다는 점이다. 셋째, 국가 경제력의 증진은 군사력의 향상뿐만 아니라 국가안보를 강화하게 한다는 점이다. 넷째, 천문학적인 규모의 국제입찰에서 낙찰을 받아 국제시장에서 성공할 가능성을 증대하기 위함이다. 다섯째, 냉전시대에 활동하던 스파이 활동을 유지하기 위해서 각국이 산업스파이를 활용하고 있다는 것이다(문규석, 2005: 408)

법, 기타 산업상, 영업상 유용한 기술이나 경영정보 등 산업체의 업무에 관한 비밀, 줄여서는 영업비밀을 부정하게 입수하거나 정탐하는 일체의 행위를 말한다고 할 수 있다(사법연수원, 1999: 245).

냉전 당시에는 국방, 외교, 정치상의 비밀이 중요한 스파이행위의 대상이었고, 이에 대하여는 주로 정부간의 스파이전쟁에 의하여 진행되었다. 그러나 냉전 이후 경제적 전쟁시대의 스파이활동은 오히려 경제적, 기술적 정보에 집중되고 있다. 특히, 이러한 기술정보에 대하여는 민간차원, 정부차원을 가리지 않고 거의 모든 역량이 집중되고 있다고 할 수 있다.

2) 산업스파이의 발생원인

이 연구에서는 합리적 선택이론(Rational Choice Theory), 차별적 접촉이론(Differential Association Theory), 중화이론(Neutralization Theory)을 들어 산업스파이의 발생 원인을 설명하고자한다.

(1) 합리적 선택이론(Rational Choice Theory)

합리적 선택이론은 행위가 손해(costs)와 이익(benefits)을 합리적으로 평가한 결과라는 가정을 함으로써 고전학파의 전통을 따르는 이론이다. 이 이론은 일반적으로 사람들이 법위반과 법준수의 양쪽 모두에 대해 이익과 손해를 비교하는 방법에 초점을 두고 있다(장상희 역, 2007: 121).

합리적 선택이론은 범죄자의 합리적이고 환경적응적인 측면을 강조한 이론으로, 기회가 제한되고, 이익이 줄어들며, 손실이 증가할 때 범죄는 감소하게 된다고 한다. 합리적 선택이론에 따르면 주어진 행위(범죄)를 저지를 가능성은 법준수로 인한 손해와 보상에 비해 법위반으로 인한 처벌의 잠재적 고통과 보상이 주는 잠재적 쾌락에 달려 있다고 보았다(장상희 역, 2007: 121).

합리적 선택이론의 가장 정교한 형태는 현대 경제학에 의존하고 있다. 경제학적 접근에 따르면 범죄자들은 근본적으로 보통 사람들과 다르지 않다고 본다. 그들은 자신의 환경에서 주어진 규제 속에서도 개인적 실익을 극대화하고자 한다. 어떤 사람들은 의사나 변호사 혹은 사회과학자가 되는 것과 같은 이유로 범죄자가 된다. 이러한 사람들이 범죄로부터 얻는 '보상(payoff)'은 가능한 다른 대안적 행위로부터 얻는 것보다 훨씬 많기 때문이다(장상희 역, 2007: 121).

산업스파이는 법을 준수할 때의 이익보다 법위반으로 얻을 수 있는 경제적 보상이 크기 때문에 범행을 저지르게 되는 것이다. 산업기술 유출 실태조사에서 산업기술이 유출되는 원인에 '개인적 이익 추구'가 높은 비중을 차지하는 것도 같은 이유이다(국가정보원, 2007a: 10).[2)]

⑵ 차별접촉이론(Differential Association Theory)

서덜랜드의 차별접촉이론은 상호관계와 의사소통을 통한 행위와 태도의 학습을 강조하는 이론으로 인간현상의 두 가지 측면을 설명하고자 했던 이론이다. 이러한 주장은 하류계층범죄자가 법을 준수하는 하류계층의 사람들보다 법을 어기는 하류계층의 사람들과 더 많은 접촉을 한다는 사실처럼 화이트칼라범죄자도 마찬가지일 것이라는 가정에서 시작한다. 그는 여기에서 화이트칼라범죄의 원인은 하류계층범죄의 원인과 아주 다른 점이 있다는 사실을 함축하는 새로운 개념, 즉 차별적 사회조직(differential social organization)을 제시하였다.[3)]

즉, 기업조직은 법규나 규정의 위반의 반범죄적 전통을 지닌 집단이지만, 정부조직은 기업규정의 위반에 강력히 대항하지 못하고 있기 때문에 범죄를 유발하는 차별적 학습과정을 더욱 용이하게 한다는 것이다. 기업의 잠재적 범법자들은 그들의 동료나 상사에 의해서 직·간접적으로 화이트칼라범죄를 범하도록 압력을 받고 있으나, 정부나 일반시민들은 화이트칼라범죄를 강력하게 비난하거나 강력한 법집행을 시행하지 않기 때문에 범죄적 학습과정을 용이하게 한다는 주장이다(국가정보원, 2007a: 114-115).

실제로 기업정보 유출 실태조사에 따르면 산업기밀의 유출보안관리 감독체계의 허술, 법적·제도적 장치의 미흡 등이 큰 원인이 되었음을 알 수 있다(남상봉, 2004b: 52-53).

기업인이나 회사관계자들과의 차별적 접촉을 통한 범죄의 학습과 이러한 범죄를 통제하고자 하는 사회적 노력과 관심의 부족은 산업스파이가 발생하는 중요한 원인이 되고 있다.

⑶ 중화이론(Neutralization Theory)

Sykes와 Matza의 중화이론은 대부분의 비행자와 범죄자들이 관습적인 가치와 태도를 견지하지만 그들은 이들 가치를 중화(합리화, 정당화)시키는 기술을 배워서 비합리적 행위와 관습적 행위 사이를 왔다갔다 표류(drift)한다고 주장한다. Sykes와 Matza는 중화의

---

2) 미국의 「경제스파이법」(The Economic Espionage Act)에서는 해외 유출시 개인에게는 15년 이하의 징역 그리고 50만 달러에 달하는 벌금을 부과하며 법인에게는 1,000만 달러의 벌금을 징수할 정도로 철저하게 경제적 부당이익을 환수하고 있다. 이는 산업기밀침해에 대한 경제적 유인을 철저하게 제거하려는 의도에서 출발한 것으로서 경제적 효율성 면에서 고려해보더라도 단기적인 영업비밀의 침해행위보다 장기적인 연구와 기술개발에 힘쓰는 것이 합리적인 선택이라는 결론을 내릴 수 있게 만들어 준다. 물론 이에 대해 우리나라의 다른 형평성의 문제가 전혀 없는 것은 아니나 산업스파이에 의한 산업기술의 유출은 법·경제학적인 측면세서 보다 높은 형량과 단속 관련 법규의 정비에 의하지 않고서는 해결될 수 없는 문제이다(정보통신부, 2004: 46).

3) 차별적 사회조직이란 우리 사회의 일부는 범죄적 전통을 가지고 일부는 반범죄적 전통을 가지는 등 서로 다른 집단의 사람들로 구성되었다는 사실을 기본으로 하고 있다. 따라서 범죄적 전통을 지닌 집단이 반범죄적 전통을 지닌 집단에 비해 범죄율이 높은데 이것을 차별적 사회조직이라고 한다(이윤호, 2005: 247-248).

기술을 이용하여 자신의 범죄를 합리화, 정당화하여 자신의 범죄행위에 정당성을 강구하게 된다. 다음에서는 Sykes와 Matza의 책임의 부인(Denial of Responsibility), 피해발생의 부인(Denial of Injury), 피해자의 부인(Denial of Victim), 비난자에 대한 비난(Condemnation of Condemners), 충성심의 요구(Appeal to Higher Loyalty) 등 중화의 기술을 살펴보겠다.

① 책임의 부인(Denial of Responsibility)

자신이 저지른 행위는 자신의 의지로는 어쩔 수 없는 강압적인 힘(소질성향・심리적 이상・생리학적 결함)에 의하여 발생된 것이므로 자신에게는 아무런 책임이 없다고 주장하는 것이다.

② 피해발생의 부인(Denial of Injury)

자기 자신의 행위가 위법이긴 하지만 실제로는 아무런 피해가 발생시키지 않았으므로 반도덕적일 수 없다고 주장하는 것이다. 이들은 자신의 범죄로 인한 피해를 부정한다.

③ 피해자의 부인(Denial of Victim)

자신의 행위로 인하여 피해가 발생한 것은 시인하지만 마땅히 제재를 받아야 할 사람에게 행해진 것으로 반도덕적일 수 없다고 주장하는 것이다. 즉, 회사의 연구원이 회사의 영업비밀을 유출했을 경우 회사가 연구원이나 근로자 또는 고객을 착취하기 때문에 손실을 입어도 괜찮으며, 마땅히 응징을 받아야 한다고 합리화시키는 것을 말한다.[4)]

④ 비난자에 대한 비난(Condemnation of Condemners)

알고 보면 자신의 행위를 반도덕적 위법행위로 간주하여 제재를 가하는 검찰, 경찰, 법원 등의 사람들이 더 추악하다고 타락해 있다고 주장하는 것이다. 자신이 연구・개발한 회사의 영업비밀을 유출하는 것보다 이를 처벌하려는 경찰이나 사법기관의 종사자들이 평소 자신보다 더 많은 비리와 범죄를 저지른다고 생각하고 범죄를 합리화・정당화시키는 것을 말한다.

또한 비난자에 대한 비난에 있어 또다른 합리화는 다른 기업이나 회사원들도 다 법을 어기기 때문에 자신들의 행위도 그리 나쁘지 않다고 정당화하는 것을 말한다. 모든 사람이 다 세금을 포탈하고 모든 사람이 다 뇌물을 주고 받기 때문에 안하는 사람들이 바보라고 합리화시켜 자신의 행위를 정당화시키게 된다.

---

4) 산업스파이 혐의와 관련되어 조사를 받은 사람들의 진술의 한 예를 살펴보면 "기업이 기술을 빌미로 개인의 직업선택의 자유를 부당하게 침해하고 있다."라고 기술하고 있다. 이는 기업이 연구원을 부당하게 착취한다고 생각하고 산업스파이 행위를 정당화・합리화시키고 있음을 알 수 있다(이웅혁, 2007: 7).

⑤ 충성심에의 요구(Appeal to Higher Loyalty)

자신의 행위가 옳지 않지만 회사동료나 상관 등의 친밀한 관계에 대한 충성심(의리)에서 범죄를 저질렀으므로 자신의 범죄가 정당화될 수 있다고 주장하는 것이다. 실제로 보고되는 있는 산업스파이 사건을 보면 대학의 선・후배나 회사동료 등 비교적 친근집단에 의해 이루어지고 있다.[5)]http://www.nixe.go.kr 2008년 9월 10

3. 외국의 산업스파이에 대한 민간 대응체계

1) 미국

1955년 민간 보안산업 활성화와 전문성 제고를 위해 설립된 미 산업보안협회(American Society for Industrial Security: ASIS)는 세계최대 민간보안협회로 FBI・법무부 등과 공조하여 산업보안 관련 교육, 인력양성, 정보제공, 정책건의 등의 기능을 수행하고 있으며 기업 정보자산관리과정, 시설보안관리과정 등 교육프로그램을 운영하면서 각종 보안관련 이슈에 대한 해결책을 제시하고, 보안 관련 잡지(시큐리티 매니지먼트 등 3종)를 발간, 회원사에 배표하는 한편 전시회・세미나 등 국제교류활동을 수행하며, CPP(Certified Protection Professional: 공인보안전문가), PSP(Physical Securtiy Professional, 물리보안전문가), PCI(Professional Certified Investigator, 공인조사전문가)등 3종 보안전문 자격증을 발급하고 인터넷 정보자료를 운영하고 있다(국가정보원, 2005a: 3-4).

산업보안협회는 22개국 200여개 지부와 30,000여명의 회원을 보유하고 있으며 본부는 미 버지니아주 알렉산드리아에 소재하고 있다. 산업보안협회는 이사회, 상설위원회, 지역 부회장, 지부회장 등 4개 조직으로, 책임자는 자발적인 봉사자로 협회에서 어떠한 보상도 받지 않는다. 미국의 산업보안협회의 주요활동을 자세히 살펴보면 다음과 같다(국가정보원, 2004b: 17-21).

(1) 교육프로그램

미국 산업보안협회의 교육프로그램에는 워크샵과 연수프로그램이 있다. 워크샵의 주요내용은 출입통제 기초지식과정 워크샵 등 보안활동에 대한 일반적인 관심 사항을 주제로 하여 2~5일간 집중 토론식으로 진행하고 있다. 전문적인 지식을 필요로 하는 신청자에 대하여 통신, 금융신설 등의 특화된 분야에 대한 보안문제 등을 주제로 워크샵을 개최하여 산업보안

5) 최근에 P에 제조공정 기술을 유출하려다 적발된 사례에서도 산업스파이는 대학의 선・후배 사이로 대학 후배가 P에 다면취 기술 매매를 제안하여 대만의 경쟁업체에 기술을 유출시키려다 적발되었다. 국가정보원(http://www.nixe.go.kr 2009년 6월 10일 검색)

에 대한 교육을 하고 있다. 또한 연수프로그램은 경영자 최신정보과정 등 경제환경 변화에 따른 경영상 문제점들에 대한 대처능력 향상을 위한 강좌를 개설하는 한편 보안전문가 자격증 시험대비, 수험생들을 위한 전문 연수프로그램을 개설・운영하고 있다.

⑵ 연례세미나 및 전시회

산업보안협회의 주요행사로 보안분야의 일반적인 사항과 특수분야에 대한 제고를 위해 "연례 보안세미나 및 전시회" 등을 개최하고 있다. 각국의 보안관계자가 참석하여 최신 보안기술・장비・용역 관련정보를 교환하거나 공유하고 있다.

⑶ 정보공유

산업보안협회의 회원들에게 보안 또는 관련분야의 정보 및 자료를 제공하기 위해 「정보자료센터」를 운영하고 있다. 고객들의 정보욕구를 만족시키기 위해 전문가 접촉, 온라인 전산망 정보탐색, 도서관 논문열람 등을 위한 「인터넷 데이터 베이스」를 운영하고 있다.

⑷ 보안전문가 시험 주관 및 자격증 발급

산업보안협회는 복잡한 보안문제에 대한 효과적인 대처를 위해 전문가의 양성에 노력하고 있다. 1977년 연례 세미나에서 보안전문가 자격증의 발급을 결정하여 현재까지 8,000여명에게 자격증을 발급하였다. 보안전문가 자격증은 각종 보안업체뿐만 아니라 일반기업에서도 보안분야 종사자에게 필수적인 조건으로 제시하는 등 자격증 활용이 증가하고 있는 추세이다.

2) 독일

독일의 산업보안 인력은 연방 및 주 산업보안협회, 기업체 보안부서, 민간 보안업체 등에서 주로 근무하고 있는데, 고졸자를 대상으로 한 3년 과정의 직업교육과정을 수료한 인력도 일부 있으나 군, 경찰 등 정보수사기관 퇴직자들이 주축을 이루고 있으며, 최근 민간부문에 보안전문가 수요가 증가하면서 정보수사기관의 인력들이 많이 전직하고 있는 추세이다. 산업보안 전문가는 "상의인증 보안전문가" 제도에 의해 자격을 인정받는데, 기업에서 보안업무에 종사하는 인력 등이 주 산업보안협회가 주관하는 교육을 받고 주 상의가 주관하는 시험에 합격함으로써 자격을 취득하게 되며, 주 산업보안협회의 교육은 총 200시간으로 법률 및 상황대처, 보호기법 등의 내용으로 구성되고 있고, 주 상의가 주관하는 시험의 응시자격은 ① 직업교육과정 수료 후 기업보안관련 부서 2년 이상 근무자, ② 6년간 기업 근무경험이 있고 보안부서 2년 이상 근무자, ③ 기타 특별한 경우 보안관련 능력이나 경험을 제시할 수 있는 자로 한정된다.

3) 일본

일본 기업들에서는 중요기술 보호를 위한 각종 보안제도를 도입하고 있다. 특히 제조업체들의 경우 중국 등 해외 현지공장에서의 핵심기술 유출사고 증가 등을 이유로 자국내 생산공장 설립을 확대하고 있는 실정이다.

LCD 패널을 생산하는 샤프는 첨단 LCD 가공기술의 열람범위를 극소수 임원으로 한정하고, 특허등록도 회피하는 블랙박스 전략을 사용하고 있다. 또한 샤프는 올해 초 1,000억 엔을 투입하여 액정 패널・TV 등 일괄 생산을 위하여 미에・가메야마 공장의 경우 공장전체를 파악할 수 있는 인원을 사장 이하 일부 간부급으로 제한하고 있으며, 공장 종업원에 대해서도 소속외 다른 부서의 출입을 엄격하게 금지하고 카메라폰의 공장 내 반입을 전면 금지하는 등 산업스파이에 대응하고 있다.

캐논의 경우에는 제조용 기계와 공구를 회사 외부에서 구입하지 않고 회사 내에서 직접 제작・사용함으로써 기술관련 정보의 외부유출을 원천차단하고 있다.

한편 니혼게이자이 신문은 주요 제조업체 115개사를 대상으로 자국내 생산공장 건설 계획을 조사한 결과, 향후 3년간 국내생산을 확대할 기업이 대상 업체의 절반에 달하고 있다고 보도하였다. 조사에 참여한 기업들은 중국 등 해외 현지공장에서 경쟁력의 원천인 기술유출 사례가 지속 증가함에 따라 기술유출을 사전 차단하는 동시에, 첨단제품 주개발거점이 일본내에 있으므로 개발・생산・출하과정의 순환이 용이한 일본에서 공장을 운영하는 것이 유리하다면서, 해외 공장에서는 범용제품을 지속 생산하되, 고부가가치 제품의 경우는 다시 자국에서 생산하는 방안을 검토 중이라고 답변하였다. 또한 동 신문은 이러한 국내생산 확대의 원인을 일본이 구조조정 등 힘겨운 과정을 거치면서 "Made in Japan"으로 글로벌 경쟁에서 승리할 수 있다는 자신감을 되찾은 것이라고 설명하였다(민수홍・이민식, 2006: 252).

또한 일본의 기업들은 직원들의 연구 의욕을 높이고 경쟁사로의 기술유출을 막기 위한 수단으로 직무상 발명 보상제도를 도입하여 시행하고 있다. 다음의 〈표 1〉은 일본기업의 직무발명 보사의 주요내용이다(국가정보원, 2004d: 5-6).

〈표 1〉 일본기업의 직무발명 보상 내용

구 분	주요 내용
소니	특허 출원 및 등록 시 최고 100만 엔의 보상금 지급 기술 공헌도를 높게 평가해 6등급으로 나눠 매년 5만~200만 엔을 지급
히타치	특허를 활용한 제품의 매출과 특허권 수입에 대해 상한선 없이 이익금의 일정 비율을 보상금으로 지급
후나이전기	사외로부터 특허 수입이 1,000만 엔 이내일 경우 10%, 1,000만 엔을 넘으면 초과분에 대해 추가로 5% 지급

미쓰비시화학	5년간 영업이익이 60억 엔 이상일 경우 2억 5,000만 엔, 30억~60억 엔 경우 1억 5,000만 엔을 상한으로 보상금 지급
세이코엡슨	특허 출원 및 등록 시 2만 엔을 지급하고, 특허 수입료의 2.5%를 지급
코스모석유	특허 수입이 3년간 5,000억엔 이상일 때 2% 지급

출처: 국가정보원, 2007a: 75.

Ⅲ. 산업스파이의 실태분석 및 대응상의 문제점

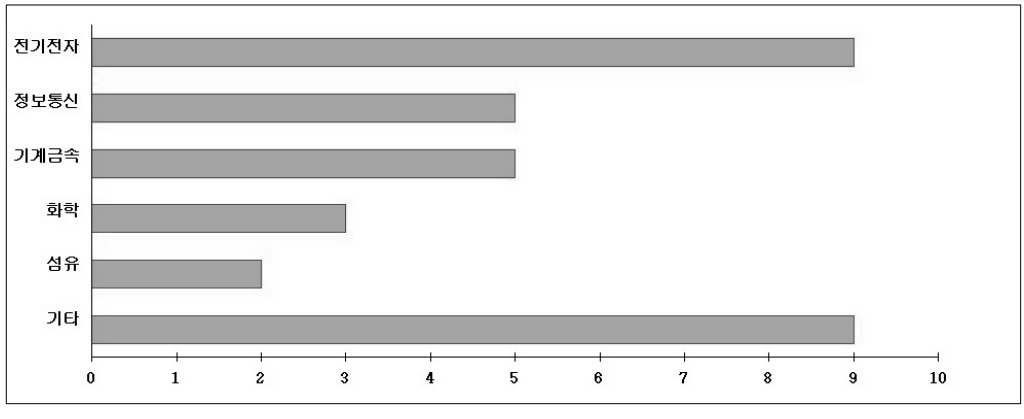
1. 산업스파이의 실태분석

1) 벤처기업과 중소기업의 기술유출 실태

중소기업청과 중소기업진흥공단은 2005년 5월 9일부터 7월 31일까지 국내 이노비즈 및 벤처기업, 그리고 수출중소기업 등 20,000여 업체를 대상으로 설문조사를 실시하였으며, 해외 현지에서 기술유출이나 지식재산권을 침해 받았다고 응답한 40개 업체를 대상으로 유선 및 방문조사를 실시하였다(중소기업청, 2005: 7-16).

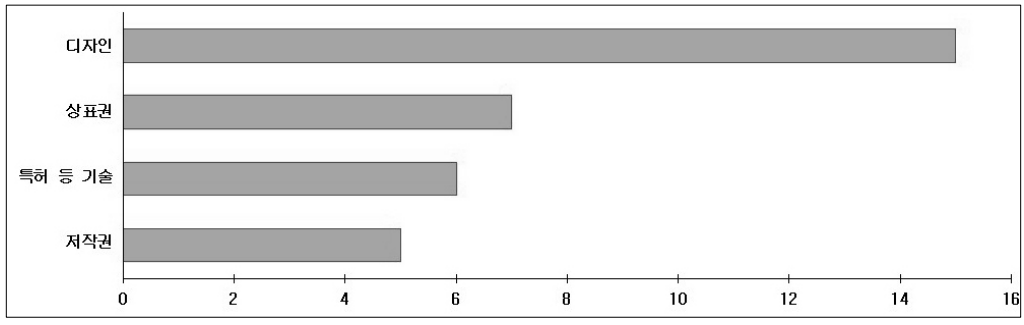
금번 실태조사결과, 특별한 침해사실이 없거나 인터뷰가 어려운 7개사를 제외하고 33개 업체를 대상으로 분석하였으며, 이들 침해업체의 업종별 현황을 살펴보면 전기·전자 및 기타 잡화 업종이 각각 9개사로 가장 많고 그 다음으로 정보통신, 기계·금속, 화학, 섬유 업종의 순으로 조사되었다.

〈그림 1〉 침해업체의 업종별 현황



출처: 중소기업청. 2005: 8. 재구성.

〈그림 2〉 침해유형



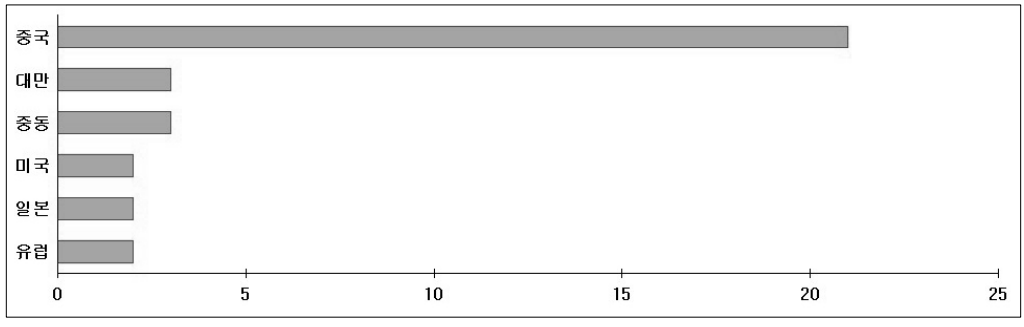
출처: 중소기업청, 2005: 9. 재구성.

또한 지식재산권 관련 전담부서 보유 유무와 관련하여 지식재산권 전담부서를 가지고 있다고 응답한 업체는 전체의 33%(11개사)로, 대다수(67%) 기업에서는 아직 지식재산권 관련 전담부서가 없는 것으로 조사되었다.

침해유형을 살펴보면, 디자인 침해가 전체 46%를 차지, 해외에서 우리기업들이 가장 많은 침해를 당하고 있는 것으로 조사되었으며 다음으로 상표권 침해가 21%, 특허 등 기술침해가 18%, 저작권 침해가 15%로 나타났다.

주요 침해 대상국가로는 중국이 21개사로 가장 많고, 다음으로 대만, 중국, 미국, 일본, 유럽 등의 순으로 나타났다.

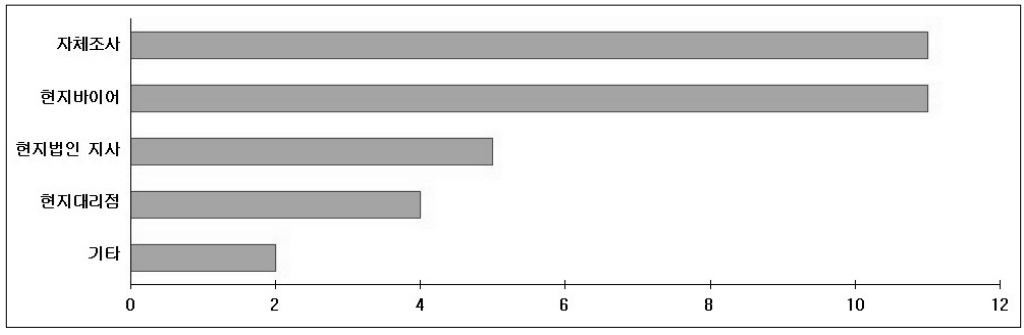
〈그림 3〉 침해 대상국가



출처: 중소기업청, 2005: 10. 재구성.

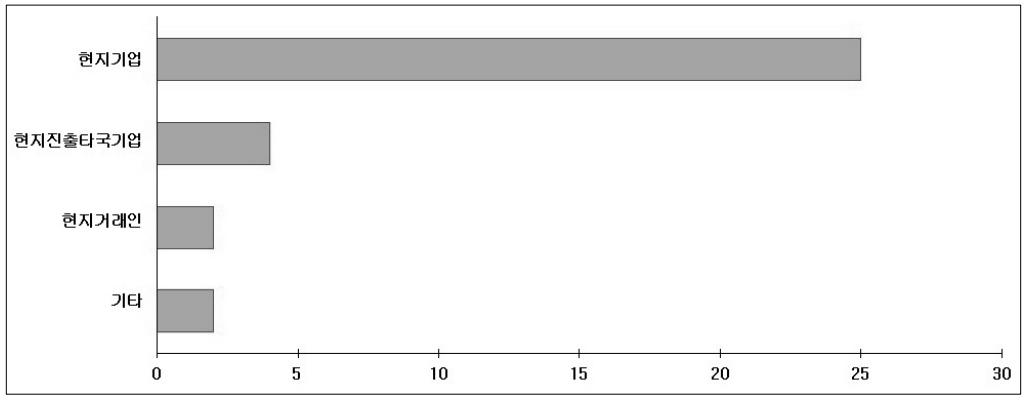
그리고 최초 침해사실을 인지시켜주는 정보제공자는 현지바이어와 자체조사를 통해서 알게 된 경우가 각각 34%를 차지 가장 많았고, 그 다음으로 현지 법인이나 지사를 통해서 발견한 경우가 15%, 현지대리점 12% 순으로 분석되었다

〈그림 4〉 최초 침해사실을 인지시켜 주는 정보제공자



출처: 중소기업청, 2005: 12. 재구성.

〈그림 5〉 주요 침해자 유형



출처: 중소기업청, 2005: 13. 재구성.

주요 침해자는 현지 기업에 의해서가 전체 76%로 가장 많고, 다음으로 현지진출 타국기업이 12%, 현지거래인(바이어 등)이 6%, 기타 6%로 조사되었다.

2) 산업체의 연구원과 임직원의 산업보안 인식 실태

대한상공회의소에서 주관하여 (주)월드리서치에서 2005년 12월부터 2006년 2월까지 전국 500여개 산업체의 연구원과 임직원 1,000명을 대상으로 설문조사를 시행하였다(국가정보원, 2006b: 22-23).

설문조사결과에 따르면 '산업보안의 개념이나 대상' 등 산업보안 기초지식에 관한 이해도는 높았지만 '보안관리 실무요령'이나 '보안사고시 대응방안 및 절차' 등 실무지식에 관한 이

해도는 상대적으로 낮은 것으로 나타났다.

2001년에 '산업보안의 개념이나 대상' 등 기초지식에 관한 인식은 79.3%에서 2005년에는 79.7%로 나타났으며, '보안관리 실무요령'은 2001년에 62.4%에서 2005년에는 64%로 나타나 2001년과 비교해 보았을 때 인식의 많은 변화가 일어나지 않았음을 알 수 있다. 또한 '보안사고시 대응방안 및 절차' 등 실무지식에 관한 이해도는 2001년에 50.2%에서 2005년 57%로 비교적 다른 부분보다 많이 높아지긴 했으나 여전히 상대적으로 낮음을 알 수 있다.

〈표 2〉 산업보안에 대한 인식

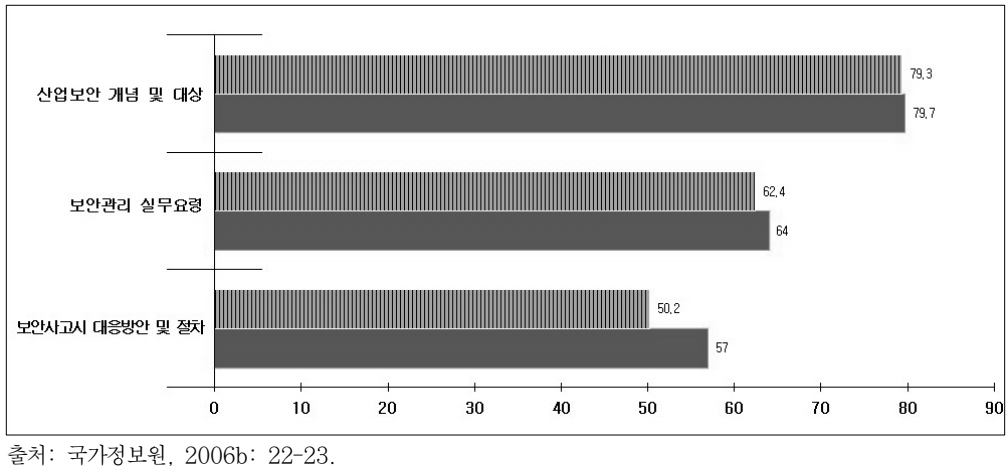
(단위 : %)

구 분	산업보안 개념 및 대상	보안관리 실무요령	보안사고시 대응방안 및 절차
2001	79.3%	62.4%	50.2%
2005	79.7%	64%	57%

출처: 국가정보원, 2006b: 22-23.

〈그림 6〉 산업보안에 대한 인식

(단위 : %)



출처: 국가정보원, 2006b: 22-23.

3) 국내 산업기술의 해외유출 실태

(1) 산업스파이 적발현황

국가경쟁력의 원천은 역사적·시대적 환경에 따라 다르게 변화되어 왔다. 오늘날 정보화·세계화하는 시대적 요구에 가장 부합하는 경쟁력의 원천은 국가의 핵심기술이다. 우리나라의 경우 산업스파이는 IT 산업, 반도체, 정보통신 등 소위 첨단 산업분야에서 주로 발생하고 있다.

국가정보원의 통계에 따르면 〈표 3〉에서 보는 바와 같이 2003년에 6건에 불과하던 것이, 2004년에는 26건, 2005년에는 29건, 2006년에는 31건이나 발생하여 산업스파이가 점차적으로 증가하고 있음을 알 수 있다.

〈표 3〉에서 보면 2003년에 6건에서 2004년에는 26건으로 급격하게 발생건수가 증가한 것은 2003년 10월 국가정보원에 산업기밀보호센터가 신설되어 전문적으로 산업기밀유출에 대한 단속을 실시하였기 때문으로 분석된다. 또한 산업스파이의 주요 표적이 여러 분야에 확대되고 있으며, 그 행위가 은밀하게 이루어지는 특징으로 보아 적발되지 않은 사건을 포함하면 통계에 나온 수치보다 훨씬 더 많을 것으로 생각된다.

〈표 3〉 산업스파이 적발 현황

(단위 : 건수)

구분	2002	2003	2004	2005	2006
발생건수	5	6	26	29	31

출처 : 국가정보원 홈페이지(http://www.nisc.go.kr. 2008년 10월 8일 검색)

(2) 신분별 기술유출 현황

신분별 기술유출 현황을 살펴보면 주로 전·현직 직원(792건, 86%)에 의한 생계형 기술유출이 대부분임을 알 수 있다. 기업의 내부자가 정보유출에 깊게 관여하게 되는데 내부자는 보통 목표물인 기술 정보를 내장한 저장장치와 이를 입수할 수 있는 인적 네트워크를 소유하고 있으며, 내부통제 및 보안구조의 허점 등에 대해서도 잘 알고 있어 기술유출을 용이하게 할 수 있다고 생각된다.

최근에 사회적 이슈로 떠올랐던 현대·기아차 기술유출 사건과 포스데이타의 와이브로 기술유출사건 역시 현직 직원이 핵심기술을 회사 내 컴퓨터에서 빼내 이메일로 퇴직 직원에게 전달하고, 퇴직 직원은 현직 직원의 도움으로 생산현장에 들어가 정보를 입수하는 등 전·현

직 직원들에 의해 이루어진 것으로 조사결과 나타났다(다음뉴스 2007년 5월 20일자 http://news.media.daum.net).

회사에 대한 직원들의 평생직장에 대한 인식이 사라짐으로써 초래되는 애사심의 약화는 인력 유동성을 부추기고 있으며, 전·현직 직원에 대한 관리의 부재는 핵심 기술유출의 최대 통로가 되고 있는 것이다. 그리고 협력·용역업체에 의한 기술유출 사례도 점차 증가하고 있어 이들에 보안관리의 필요성이 증대되고 있다.

〈표 4〉 신분별 기술유출 현황(2003~2007년간)

총 계	전직원	현직원	유치과학자	용업업체	외국유학생	투자업체
107건	65	27	3	8	2	2
100%	61	25	3	7	2	2

출처 : 국가정보원 홈페이지(http://www.nisc.go.kr. 2009년 7월 8일 검색)

⑶ 동기별 기술유출현황

기술유출 동기로는 개인 영리(35건) 및 금전유혹(29건)에 의한 기술유출이 64건으로 약 70%에 달하며, 처우불만(14건)과 인사불만(6건)에 의한 유출이 20건으로 21% 정도를 차지하는 것으로 나타났다. 또한 비리연루와 신분불안이 각각 4건으로 나타났다.

이처럼 산업스파이는 대부분 금전적 이익과 개인적 이익을 위하여 범죄를 저지르고 있음을 알 수 있다.

〈표 5〉 동기별 기술유출 현황(2003~2007년간)

구 분	개인영리	금전유혹	처우불만	인사불만	비리연루	기 타
발생건수 107	45	32	14	7	4	5

출처 : 국가정보원 홈페이지(http://www.nisc.go.kr. 2009년 7월 8일 검색)

4) 산업스파이 검거 사례

오늘날 한 나라의 경제를 좌우할 만큼 천문학적인 경제적 가치를 지닌 것이 기업의 첨단기술이며, 민간기업 차원을 넘어 국가 차원의 기술입수 활동 및 유출방지 활동이 펼쳐지고 있는 것이 현실이다. 특히 우리나라는 IT 및 전자분야에서 세계 최고의 기술을 보유하고 있는 기술 주도국으로서 산업스파이의 주요 목표가 되고 있음에도 불구하고 아직까지 일부 기업들만을

제외하고 대부분 기업들의 산업보안 의식의 수준이 낮고 관련 대책의 수준도 미흡한 실정이다.

지금까지 경찰의 산업기밀유출사범 검거 건수 및 인원은 48건에 148명으로 나타났다. 연도별로 살펴보면, 2003년 6건(6명)이던 것이 2004년 15건(42명), 2005년 18건(70명)으로 각각 늘어났고, 2006년 8월말 기준으로 9건(30명)에 이르고 있다. 2003년부터 2006년까지 경찰의 산업기밀유출사범 검거 건수 및 인원은 〈표 6〉과 같다.

〈표 6〉 경찰의 산업기술유출사범 검거 건수 및 인원(2006/08말 기준)

구 분	검거 건수(건)	검거 인원(명)
2003년	6(국내6)	6
2004년	15(국내13, 해외2)	42
2005년	18(국내14, 해외4)	70
2006년	9(국내5, 해외4)	30
합계	48	148

출처: 경찰청 홈페이지 참고.

또한 경찰청의 자료에 따르면, 2004년 4월부터 2006년 9월까지 경찰의 해외 산업기밀유출사범의 검거 건수(인원)는 총 10건(45명)에 이른다.

경찰이 검거한 해외 산업기밀 유출 사례는 먼저 분야별로는 전기전자, 정보통신, 정밀기계, 생명공학, 정밀화학 등으로 나누어 볼 수 있으며, 산업기밀을 유출한 사람의 신분에 따라서는 퇴직직원, 현직직원, 용역업체, 유치과학자 등으로 나눌 수 있다. 유출국가로는 중국이 가장 많고, 일본, 대만의 순으로 발생건수가 많다(노호래, 2008: 64-65).

〈표 7〉 경찰의 해외 간업기밀유출사범 검거 현황(2006/09말 현재)

일시	유출사례	검거인원(명)	사법처리 결과(명)	피해예방 추정(원)	유출국가
2004년 4월	반도체 테스트 장비유출	3	구속1 불구속2	1,900억	일본
2004년 8월	인터넷 게임 프로그램 솔루션 유출기도	2	구속2	8억	중국
2005년 2월	냉각탑 제작도면 유출	2	불구속2	2억	중국
2005년 4월	모조보석 자동연마시스템 무단 제작 및 판매	9	구속2 불구속7	1,598억	중국
2005년 8월	IT프로그램의 소스코드 등 유출	10	불구속10	2,700억	중국
2005년 9월	메일시스템 기술 유출기도	5	불구속5	100억	중국

2006년 3월	첨단기술이 저정된 하드디스크 절취 후 취업시도	1	구속1	2조4,000억	중국
2006년 3월	차량용 비디오시스템 설계도면 유출	4	불구속4	600억	중국
2006년 5월	선박분석 최적화 시스템의 핵심기술 유출	3	불구속3	9,377억	중국
2006년 9월	자동차 금형 설계프로그램 기술 유출	6	구속2 불구속4	3,000억	일본 대만

출처: 경찰청 홈페이지 참고.

2. 산업스파이 대응상의 문제점

1) 사법기관의 산업스파이 대응상의 한계

산업스파이의 특성상 그리고 기업의 생리상 사법기관의 수사관으로만은 산업스파이를 예방하는 데에는 한계가 있다.

수사관의 전문지식이 부족하고 수사관련 국가기관이 일원화되어 있지 못하여 전담 기구상의 문제가 있으며 외국인과 공모시 유출기술 회수 및 처벌이 곤란한 문제점이 있다(사법연수원, 2004: 130-132).

급속한 과학기술의 발전으로 인하여 사업스파이 사범의 수사를 위해서는 무엇보다도 과학기술 및 산업전반에 관한 전문지식이 필요한다. 고소인이 제기하는 영업비밀이나 산업기술이 형법, 부정경쟁방지법, 산업기술유출방지법상 해당 기업의 특유한 생산기술에 관한 영업기밀인지, 나아가 해당 정보가 산업기술 일반의 수준에 비추어 비공개성 및 독자적인 경제적 가치성이 있는지는 이에 관한 전문지식이 결여된 상태에서는 판단이 불가능하다. 그리고 실무상 수사대상이 된 산업기술(영업비밀)이 대부분 첨단기술분야인 바, 피의자는 유출한 자료가 업계에 공지되었거나 별거 아니라는 식으로 축소하는 경우가 많은데, 이에 대해 중립적으로 진술해 줄 참고인이 없는 경우가 대부분이다. 결국 이에 대해 진술해 줄 참고인은 피의자의 회사 동료일 수 밖에 없어서, 적극적인 진술을 회피하는 경우가 대부분이고, 이러한 태도는 공판단계에서 피의자에 대한 온정적 판결을 이끌어내는데 한몫하고 있다. 또한 해외기술유출사범의 경우 외국인이나 해외거주 교민 등과 공모하여 기술을 유출하는 양상을 보이고 있는 바, 해외로 유출될 경우 그 회수가 어려워 피해기업에 돌이킬 수 없는 손해를 입힐 우려가 있고, 해외에 거주하는 공모자에 대해 범죄인 인도협약이 맺어져 있는 국가라 하더라도 검거 및 수사가 지연되거나 어렵고 이런 협약이 없는 국가에 대하여는 아예 검거를 할 수 없어, 죄질이 무거운 해외공범은 방치되고 있는 실정이다(노호래, 2008: 65-66).

2) 산업스파이에 대한 인식 및 교육 부족

산업기술이 최초의 개발 기업이 아닌 경쟁업체에서 상품화되면 최초의 개발업체는 금전적으로 막대한 손실을 초래할 뿐만 아니라 국가 경쟁력에도 큰 손실을 초래할 수 있기 때문에 산업스파이는 심각한 범죄행위라는 인식을 제고시킬 필요가 있다.[6] 하지만 실제적으로 활용할 수 있다고 믿을 수 있는 법・제도적으로 공인된 지침에 이르지는 못하고 있는 실정이다.

산업스파이의 문제를 해결하기 위해서는 무엇보다도 산업스파이에 대한 심각성과 사회적 문제로서의 중요성에 사회적 인식의 변화가 이루어져야 할 것이다. 즉, 산업스파이는 단순히 기업차원에서의 문제나 개인의 문제가 아닌 사회적 차원의 문제라는 인식의 전환이 필요하다.

또한, 기업의 산업보안에 대한 인식제고 및 기술유출시 적절한 대응을 지원하기 위해서는 정부 및 관련기관은 산업보안 지원프로그램을 확대・운영하여야 한다. 미국의 경우 범정부적인 "국가 산업보안 프로그램(National Industrial Security Program)"을 운영하여 핵심기술 유출방지를 위한 총체적인 대책을 수립・시행하고 있다. 이러한 점을 감안할 때, 정부주도의 산업보안 프로그램의 운영이 기술유출방지를 위한 보다 실질적인 차원에서 실시될 필요가 있다(정보통신부, 2004: 59).

우리나라는 기술유출방지를 위한 실질적인 차원의 산업보안 프로그램이 없다보니 산업보안 교육 및 자문활동이 미비할 수밖에 없다. 대기업의 경우 산업보안에 대한 중요성을 인식하고 이를 직원들에게 주지시키기 위해 산업보안 교육 및 관련 시스템의 정비 등을 통한 노력을 하고 있지만, 중소기업은 경영상의 영세성으로 인하여 CEO 자체도 산업보안에 대하여 무지하고 산업보안 교육 등 여러가지 보안 시스템을 갖추지 못하는 경우가 많다.

최근의 산업스파이 사건을 보면 대기업에서의 산업기술유출 뿐만 아니라 중소기업, 벤처기업에서의 산업기술유출이 빈번하게 일어나는 추세이다. 따라서 정부차원에서 산업보안에 대한 중요성을 기업들에게 주지시킬 필요성이 있으며, 산업스파이의 대응 및 산업보안 관리실무요령 등에 대한 사항들에 대해 자문활동을 펼치는 등 실질적인 차원의 산업보안 프로그램을 마련할 필요가 있다.

3) 보안관리 감독체계의 부실

우리나라의 경우 산업스파이가 해마다 늘어나고 있는 중요한 이유 중 하나는 보안관리 감독체계가 부실하기 때문이다. 보안관리 감독체계가 부실하다보니 산업스파이가 범행을 저지

---

6) 경찰청의 경우 이러한 산업보안의 중요성과 인식을 제고시키기 위하여 "첨단산업 기술유출 방지활동(2003)"이라는 책을 발간하였다. 이 책은 첨단기술과 보안이라는 맥락 속에서 산업보호활동의 대상, 침해자, 유형을 개괄하고 산업기술 유출사례를 보여주면서 기업 차원에서의 산업비밀 보안관리 요령과 산업스파이에 대한 형사법적 대응방안 등을 제시하고 있다.

르기 쉬운 사회적 환경을 제공하고 있다.

산업스파이는 주로 전・현직 직원에 의한 생계형 기술유출이 대부분이다. 산업스파이의 효과적 대응을 위해서는 이러한 기업 내 핵심 기술인력에 대한 관리・감독할 수 있는 관리체계가 요구되고 있다.

그러나 우리나라의 경우 대부분의 기업들은 핵심인력을 관리・감독할 수 있는 관리시스템이 부족하다. 독일의 경우에는 기업들이 산업기밀 보호의 주체로서 자체 보안부서 및 전담직원을 두고 핵심인력에 대해 관리・감독을 수행하고 있으며, 기술보호・안전 등 기업 보안활동을 수행하고 있다.

또한 산업스파이 대응과 관련하여 기관들과 기업들 간의 협력체계가 미흡하여 보안관리에 대한 감독이 제도로 이루어지지 않고 있는 실정이다. 이는 기관들과 기업 간의 연계가 체계적이지 못하기 때문에 효과적으로 산업스파이에 대응할 수 없는 것이다. 향후 기술보호・안전 등 기업 보안활동을 수행하면서 산업보안협회를 매개로 정부기관과 정보교류 등 긴밀한 민・관협력체계 구축이 필요하다(정병수, 2007: 69-70).

Ⅳ. 민간조사원(탐정)을 활용한 산업스파이 대응방안

현대사회에서는 공권력이 모든 범죄 및 기타 안전에 위협되는 것에 대하여 개입하는 것이 사실상 불가능한 상황에 이르렀다. 이와 함께 민간경비 산업의 영역확대와 시큐리티 환경의 변화는 국민으로 하여금 기존의 시큐리티 서비스의 수요증가 뿐 아니라 새로운 분야의 서비스를 기대하고 있으며 이미 선진국에서는 민간조사제도가 사회시장에서 하나의 직업으로 분류되어 영업을 하고 있다. 특히 OECD가입 후 민간조사제도도 외국에 개방되었으나 한국에서는 아직 탐정이나 민간조사라는 용어를 사용하는 것은 금지되고 있다.

산업스파이의 경우 범죄의 특성상 사법기관이 개입하기가 곤란한 부분이 상당이 많이 존재하고 있다.

따라서 앞서 문제점에서 고찰해 본 내용을 토대로 그에 대한 대응방안으로서 민간조사원(탐정)을 활용한 산업스파이에 대한 대응으로. 여기에서 제시된 대응방안은 민간조사원(탐정)이 우리나라에 도입된 후에 민간조사원(탐정)을 활용한 산업스파이 대응방안을 제시하였다.

다음에서는 민간조사원의 기업내 산업스파이 대응방안과 기업내에서 산업스파이 예방업무를 담당하는 민간조사원(탐정)의 산업보안 의식 및 교육의 강화 그리고 민간조사원(탐정)이 직무에 처함에 있어서의 감독상의 방안을 제시하였다.

1. 민간조사원(탐정)을 통한 기업내 산업스파이 대응

현행수사는 공적인 기관인 검・경・군・국정원 등에서 담당하고 있다. 기존의 법체계에서의 수사는 오로지 공적인 기관만 하도록 하고 있으며, 타 민간인이 할 수는 없었다. 공권력에 의한 수사는 강제성과 신속성 등을 달성할 수 있는 장점을 가지나 문제는 경미한 범죄나 장기화된 범죄 특히, 기업에서의 산업스파이에 대하여는 적절한 대처할 수 없는 한계를 가지고 있다(나영민・김원중, 2006: 33).

사건수사가 종결될 때까지 사건관계인들이 느끼는 심리적・경제적 부담을 고려할 때 고소・고발・진정사건이 우리사회에 미치는 영향은 매우 크다고 할 수 있다. 연간 100만건 이상에 달하는 고소・고발・진정사건은 5,000여명에 불과한 수사관에 의해 주로 처리되어 왔으며 그 결과 수사관은 평균 40건 이상을 보유한 상태에서 연간 적정처리건수의 2배에 달하는 1인당 200여건을 수사하게 됨으로써 사건수사지연, 다른 경찰서로의 이송 남발, 부실한 수사, 민원인의 불만과 고통 증폭 등 악순환이 거듭되고 있다(경찰청 홈페이지 참고).

이러한 한계성을 극복할 수 있는 제도가 민간조사제도이다. 민간조사제도는 수사・사법기관이 담당할 수 없는 분야에 의뢰인의 의뢰를 받고 조사를 통하여 형사소송이나 민사소송상 증거자료 등을 확보하여 정부 기관의 업무를 신속하고 원활하게 진행할 수 있게 할 뿐만 아니라 업무의 경감효과도 가질 수 있다. 따라서 민간조사제도는 공적수사기관에 대한 보조기관으로 활용하여 공적 수사기관의 업무 한계성을 보완할 수 있는 역할을 수행 할 수 있다.

뿐만 아니라 기업에서 관심있게 살펴봐야 할 부분은 기업 내 부정비리 조사와 기업의 정보를 유출하고자 하는 산업스파이를 들 수 있는데, 이러한 부정비리조사는 기업의 경영활동의 전반에 걸쳐 발생하고 있는 비리 및 부정에 관한 전문적인 컨설팅으로 건전하고 투명한 기업문화의 정착에 걸림돌로 작용하는 부정과 비리를 사전에 예방하고 방지할 수 있도록 기업의 내부 통제시스템에 대한 진단 및 컨설팅의 수행 및 기업 임직원의 부정비리에 대한 전문적인 조사업무를 위임받아 수행하는 것을 의미한다.

첨단 산업에 의해 그 기술은 회사뿐만 아니라 나아가 국가에도 중요한 기반이 되고 있다. 첨단 기술을 보호하기 위하여 정부는 모든 수사기관의 정보와 수사력을 총동원하여 오고 있다. 이는 전 세계적인 추세로 주로 국제분야에 있는 자국의 기술력이 타국으로 유출되는 막는 것을 각 정보기관에서 중요 업무로 담당하고 있다. 세계는 정보전쟁이라고 표현하고 있듯이 정보는 국가사회를 지지하는 중요한 내용으로 이를 지키기 위한 피나는 노력을 경주하고 있다. 우리나라 역시 앞서 살펴보았듯이 그 피해건수와 피해금액이 날로 증가하고 있다.

공적기관이 공식적으로 정보 유출되고 있는지 아니면 의심이 가는지에 대하여 수사를 하는 것은 제도상의 한계점을 가지고 있다. 따라서 민간조사원이 은밀하게 기업사건에 개입하

여 증거를 수집하고 정보를 입수하여 위험성을 사전에 확인하고 조치하여 예방하는 것이 효과적일 것이다.

신속하게 처리해야 하는 범죄를 조사하는데 효과적인 민간조사제도를 국가의 공적 기관이 개입하기 곤란한 기업범죄 등에 활용함으로써 국가와 국민경제의 손실을 예방할 수 있는 장점이 있으므로 기업범죄에 적극 활용할 수 있는 제도가 마련되어야 한다(정연민, 2007: 73-74 참고).

2. 산업보안에 대한 인식 강화

민간조사원(탐정)이 기업에서의 산업스파이를 예방함에 있어서 업무에 대한 중요성을 인식하게 함으로서 업무의 책임감과 사명감을 고취시켜야 하며, 나아가 정기적인 민간조사원(탐정)의 교육이 이루어 져야 한다.

1) 산업기밀 유출로 인한 피해의 심각성 홍보

산업스파이는 항상 은밀하고 비밀스럽게 이루어지기 때문에 주위에서 쉽게 인식할 수 없으며, 단속 또한 매우 어려운 실정이다. 그러므로 산업스파이에 대한 교육과 홍보는 산업스파이의 예방에 있어서 중요한 부분을 차지한다고 볼 수 있다.

특히, 대중매체의 홍보나 기업에서의 산업기밀 유출로 인한 피해의 심각성의 홍보, 세미나 혹은 상담을 통하여 홍보를 하는 것은 기업에서의 임직원뿐만 아니라 일반 국민에게도 정보나 교육을 제공함으로써 산업스파이 예방에 효과적인 성과를 얻을 수 있을 것이다.

또한 산업기밀 유출로 인한 피해의 심각성을 효과적으로 홍보하기 위해서는 전국에 산업보안 관련 시설에 홍보 포스터를 부착하고 대중매체 등을 이용하여 산업스파이에 대한 피해의 심각성, 산업보안의 중요성 등을 지속적인 홍보가 요구된다.

부정경쟁방지법과 산업기술유출방지법을 국민, 정부, 공공기관, 기업체 등을 대상으로 지속적이고 체계적인 교육과 산업스파이 대응과 관련된 법률의 홍보가 필요하다.[7]

2) 산업보안에 대한 인식의 고양

산업스파이에 대한 효과적인 대응을 위해서는 전반적인 사회적 인식의 전환이 필요하다. 더 이상 산업스파이 문제는 기업 내에서의 문제가 아닌 국가 차원의 문제로서의 인식전환이 필요하다.

---

7) 예를 들면, 최근 시행된 「산업기술유출방지법」 내용은 무엇인지, 기존의 「부정경쟁방지법」과의 차이점은 무엇인지, 과거와 비교했을 때 개정된 사항은 무엇인지 등의 내용을 지속적으로 홍보하는 것이다. 산업보안에 대한 중요성을 인식시킬 수 있으며, 산업기술이 유출되는 것을 효과적으로 예방할 수 있기 때문에 지속적인 홍보는 산업스파이를 효과적으로 대응하는데 있어서 매우 중요하다고 볼 수 있다.

산업스파이를 효과적으로 대응하기 위해서는 무엇보다도 산업 기밀유출에 대한 피해의 심각성과 사회문제로의 중요성에 대한 사회적 인식의 변화가 이루어져야 할 것이다. 즉, 산업스파이에 의한 산업기밀의 유출은 단순히 개인이나 피해 기업만의 문제가 아닌 국가적 문제라는 인식의 전환이 필요하다.

2. 산업보안 활동의 전문성 강화

1) 산업보안에 대한 교육 실시

모든 범죄가 그러하듯, 산업스파이에 의한 산업기술의 유출은 사후대응보다 사전에 예방하는 것이 피해를 최소화할 수 있다. 따라서 산업스파이를 효과적으로 예방하고 대응하기 위해서는 정부차원에서 기술유출 사례, 대응전략, 산업보안 실무내용, 국내외 보안관리 우수기업 벤치마킹 등의 정기적·주기적으로 산업보안 교육을 확대 실시하여야 한다.

산업스파이에 효과적으로 대응하기 위해서는 법집행, 방첩활동, 네트워크 보안, 데이터 잠금장치 등의 노력뿐만 아니라 직원들에 대한 윤리교육이 이루어져야 한다(Omid Nodoushani·Patricia A. Nodoushani, 2002: 96).

하지만 중소기업, 벤처기업 등 영세한 기업의 경우는 산업보안 교육이 제대로 이루어지지 않기 때문에 산업기술 유출에 의한 피해의 심각성이나 산업스파이 대응전략 증이 제대로 이루어지지 않고 있는 것이다.

또한, 해외에 진출한 기업에 대한 기술유출 애로사항에 대한 자문활동 및 산업보안 세미나를 개최하는 등의 노력을 하여야 할 것이다. 피해기업이 대기업일 경우, 로펌 등 법률가의 조언으로 민·형사적 구제방안 중 기업에서 편리한 방법을 선택하여 충분한 법률적 조력을 받을 수 있지만, 영세한 중소기업이나 벤처기업의 경우는 구제절차를 잘 모를 뿐만 아니라 비용면에서 감당하기 어려운 경우가 발생할 수 있다(남상봉, 2004: 47).

따라서 국가차원에서 산업보안 교육을 통하여 산업스파이에 대해 효과적으로 대응할 수 있는 시스템을 마련해야 한다. 정부차원에서 피해기업들에 대한 자문활동을 수행하여 구제절차, 법률가의 조언 등 자문활동을 하여 우리나라 기업이 해외에서 피해를 당하는 일을 예방하여야 할 것이다.

그리고 산업보안에 대해 효율적으로 교육을 시행하기 위해서는 정부차원에서 산업보안 세미나를 정기적으로 개최할 필요가 있다. 산업보안세미나의 정기적인 개최로 인하여 산업보안에 대한 심층적인 학술적 연구가 이루어질 수 있으며, 효율적인 대응방안 등 현실에 맞는 여러 가지 연구가 이루어질 수 있기 때문이다.

2) 산업기술보호 관련 자격제도 도입

오늘날 산업보안은 기업의 내부문제를 넘어서 국가차원의 문제로 인식되고 있으며, 산업기술의 유출로 인한 피해는 막대하다. 따라서 이에 적극 대처하기 위하여산기법이 제정되었는데, 이 법에서는 산업보안에 가장 효율적이라고 볼 수 있는 기업 등의 자율성에 바탕을 둔 보안체계의 마련에는 미흡한 것이 사실이다. 즉 이 법 에서는 산업보안을 위한 "산업보안체계의 인증"과 "산업보안 자격제도"가 누락 되어 있다. 여기서 도입하고자 하는 산업보안 자격제도는 기업 등에 도입을 강제하도록 하는 것이 아니고 산업보안 전문인력의 양성과 기업 등의 자율적인 판단에 따라 이를 활용할 수 있도록 하는 제도적 기반의 조성에 있다. 즉 산업보안 자격제도는 산업보안에 관련한 산업현장의 실무교육(예컨대, 수사, 증거수집, 위기대처등)에 중점을 두어야 한다.

따라서 산업보안 자격제도를 도입하는 경우 어떠한 형태의 자격제도로 운영할 것인가가 문제되는데, 최근 산업기술의 유출사건에서 볼 수 있듯이 산업보안은 국가안보나 국민경제에 중대한 영향을 미칠 수 있다. 따라서 산업보안 자격제도는 기업 등의 수요에 부합하는 정도의 수준에서 관련 전문인력을 공급할 수 있는 형태의 자격, 즉 국가자격제도로 도입되어야 한다. 산업보안 자격제도를 국가자격으로 도입하고자 한다면, 산기법을 개정해야 하고 관련된 입법사항을 법률, 시행령 및 시행규칙에 반영하여야 한다. 예컨대, 산업기술보안 자격의 도입근거, 산업기술보안 자격제도의 운영 및 자격기준, 산업보안자격 취득자의 의무 및 해택 등에 관하여 입법화하여야 한다(현대호, 2008: 261).

3. 보안관리 감독체계의 구축

민간조사원(탐정)이 기업의 산업스파이를 예방하는 업무를 담당하게 되면, 기업에서의 상당한 권한뿐만 아니라 기업의 기밀을 쉽게 접촉할 있는 기회를 가지게 되므로 적절한 감독이 필요하다.

산업스파이로 인한 피해는 산업의 기밀이 유출된 후에는 범인이 체포 된다 하더라도 그로 인한 피해는 막대할 수 밖 에 없다. 즉, 산업스파이는 사후대응보다 사전예방이 훨씬 효과적이라고 할 수 있다.

따라서 기업은 생존과 관련된 문제라는 인식을 갖고 기업내의 자체 보안 시스템을 구축하여야 한다. 기업의 산업기밀, 현황을 보더라도 기업내의 자체 보안시스템이 많은 부분 부족하다는 것을 알 수 있다. 기업은 산업기밀을 보호하기 위하여 보안 담당부서를 설치하여 산업스파이에 대응하여야 한다.

기업내 담당 부서를 설치하여 보안담당자를 지정하고, 정기적으로 보안 점검 및 감사를

실시하는 등 사전에 산업스파이를 예방할 수 있는 보안관리 감독시스템을 구축하여야 할 것이다.

지금까지 기업이 자체 보안 시스템 구축을 위해 많은 투자를 하지 않았던 것은 보안 업무의 특성상 당장 성과로 나타나지 않기 때문이다. 그러나 산업스파이에 대한 피해가 한번 발생하고 나면 되돌릴 수 없는 막대한 피해를 가져오기 때문에 산업보안에 대한 투자를 아끼지 말아야 한다.

또한, 대기업의 경우에는 자체 보안관리 시스템을 구축하는데 있어서 자체적으로 충분한 예산이 뒷받침되기 때문에 가능할지 모르지만 중소기업이나 벤처기업의 경우에는 규모의 영세성으로 인하여 자체 보안관리 시스템 구축에 있어 많은 어려움이 있다. 이를 위해서는 중소기업은 외부에 보안관리를 위탁하는 형태로 관리하는 방안도 고려해 볼수 있을 것이다.

V. 결 론

치열한 국제 경제환경 속에서 기업들은 첨단기술 확보에 심혈을 기울이고 있고 이러한 첨단기술력의 확보는 국가경쟁력을 결정하는 중요한 변수이다.

우리나라는 IT, 조선, 철강, 자동차 등의 분야에서 세계적 수준에 도달하였고 매년 막대한 자금을 첨단기술의 및 개발에 투자하고 있으나 지금까지 체계적인 산업보안활동이 전개되지 못한 실정이다.

특히 피해를 당하면 기업뿐만 아니라 국가적으로 막대한 손실을 보게 되는 산업스파이는 기업과 관련하여 관심있게 살펴봐야 할 부분이다.

하지만 산업 스파이는 공적인 사법기관이 공식적으로 정보가 유출되고 있는지 아니면 의심이 가는지에 대하여 수사를 하는 것은 제도상의 한계점이 있다. 예컨대, 공적인 사법기관이 수사에 착수할 경우에 그 가해자들은 이미 정보를 입수하여 은폐할 것이며, 또한 공적인 사법기관 구체적인 사건이 발생할 경우에 개입할 수 있는 한계점 등에 의해 수사가 제대로 이루어지기 어려울 것이다(나영민 외, 2006: 33).

무엇보다 중요한 것은 산업기술보호에 대한 기업들의 적극적인 의식변화와 자발적인 참여다. 산업기술보호 환경의 변화를 조기에 인식하는 것은 그만큼 우리가 준비하고 대응해야 할 시간을 벌어준다는 의미에서 매우 중요하다. 우리 기업들이 이러한 움직임을 보다 일찍 감지한다면 기술유출을 사전에 방지하고 미래에 발생될 수도 있는 피해를 최소화할 수 있는 방법을 강구할 수 있게 될 것이다.

이러한 점을 고려할 때 민간조사원이 은밀하게 기업사건에 개입하여 증거를 수집하고 정

보를 입수하여 위험성을 사전에 확인하고 조치하여 예방하는 것이 효과적일 것이다. 신속하게 처리해야 하는 범죄를 조사하는데 효과적인 민간조사제도를 국가의 공적인 사법기관이 개입하기 곤란한 산업스파이와 같은 기업범죄 등에 활용함으로서 기업 뿐 아니라 국가, 나아가 국민의 경제의 손실을 예방할 수 있는 제도가 도입되어야 할 것이다.

따라서 기업내에서의 부정비리조사와 산업스파이의 예방을 위하여 민간조사원(탐정)이 사법기관의 한계를 보완할 수 있는 역할을 하는 것이 바람직하다고 판단되며, 이러한 민간조사원(탐정)에 대해서는 업무 특성상 기업내에서의 권한과 함께 쉽게 기업기밀에 접근할 수 있는 점 등을 감안할 때 정기적이고 체계적인 교육으로 업무에 대한 중요성을 인식 시키는 한편, 적절한 관리감독 체계가 필요하다고 할 수 있겠다.

참 고 문 헌

1. 국내문헌

〈단행본〉

경찰청(2006),「경찰백서」

경찰청(2007),「경찰백서」

경찰청(2008),「경찰백서」

과학기술부(2003),「과학기술정보 보호체제 강화방안 연구」.

국가정보원(2004a),「산업보안 focus」.

_____(2004b),「산업스파이 사건 재조명」

_____(2004c),「산업스파이 식별요령」

_____(2004d),「첨단 산업기술 보호동향 제2호」

_____(2005a),「첨단 산업기술 보호동향 제3호」.

_____(2005b),「첨단 산업기술 보호동향 제4호」.

_____(2006a),「첨단 산업기술 보호동향 제5호」.

_____(2006b),「첨단 산업기술 보호동향 제6호」.

_____(2007a),「첨단 산업기술 보호동향 제7호」.

_____(2007b),「첨단 산업기술 보호동향 제8호」.

_____(2008),「첨단 산업기술 보호동향 제9호」.

_____(2009),「첨단 산업기술 보호동향 제10호」.

사법연수원(1999),「신종범죄론」.

이동영(2003),「21세기 공인탐정이 뛴다」, 서울 : 굿인포메인션.

이윤효(2004),「범죄학개론」, 서울 : 박영사.

정보통신부(2004),「IT기술 해외유출 방지방안에 관한 연구」, 서울 : 정보통신부.

중소기업청(2004),「중소기업 기술유출 사례와 대응전략」.

_____(2005).「기업비밀이 샌다: 기술유출 가이드북」, 대전 : 중소기업청·중소기업공단.

특허청(2004),「영업비밀보호 가이드북」

하정용(2005),「탐정학의 이해」, 서울 : 청목출판사.

〈논문〉

나영민(2005), "탐정제의 도입방안에 관한 연구",「학위논문」, 한국체육대학교 대학원.

남상봉(2004a), "산업스파이 수사사례 분석 및 대응방안", 국가정보원,「산업보안 연구논총」, 1: 55-78.

_____(2004b), "산업기밀 유출 사건과 법적 대응방안",「월간 시큐리티 월드」, 2004 한국 산업보안세미나자료집.

노호래(2008), "산업기술 유출범죄에 대한 정책적 대응방안",「공안행정학화보」, 제30호: 47-77
문규석(2005), "국제법상 산업스파이에 관한 연구", 성균관대학교 비교법연구소, 성균관법학, 17(3): 405-433.
민수홍·이민식(2006), "외국의 신종범죄 발생현황과 대책", 치안정책연구소,「치안논집」제22집.
이웅혁(2007), "산업스파이범죄 예방을 위한 거짓말탐지기의 활용: 그 필연성에 대한 논거를 중심으로", 국회의원 정두언 정책토론회 세미나자료집.
송봉규(2006), "민간조사원 도입에 관한 연구",「학위논문」, 동국대학교 대학원.
정병수(2007), "산업스파이의 실태분석 및 대응방안에 관한 연구",「학위논문」, 동국대학교 대학원.
정연민(2005), "민간경비시장의 환경변화에 따른 민간조사업의 전망과 도입방안",「학위논문」, 용인대학교 대학원.
황정익(2005), "공인조사(공인탐점)제도의 도입에 관한 연구", 치안정책연구소,「연구보고서」, 2005-1.
현대호(2008), "산업보안 자격제도의 도입방안",「산업보안 연구논총」

2. 외국문헌

Abagnale, Frank.(2004). *The Real Guide to Identity Theft*. Real U Guides.
Arata, Michael J.(2004). *Preventing Identity Theft for Dummies*. Wiley Publishing, Inc.
Beccaria, Cesare.(1963). *On Crimes and Punishments*. Indianapolis: Bobbs-Merrill.
Morris, Daniel J., Etkin, Lawrence P, and Helms, Marilyn M.(2000). "Issues in the illegal transference of U.S. information technologies", *Information Management & Computer Security*, 88(4): 164-173.
Nasheri, Hedieh.(2005). *Economic espionage and Industrial spying*, United Kingdom: Cambridge University Press.
Samli, A. Coskun and Jacobs, Laurence.(2003). "Counteracting Global Industrial Espionage: A Damage Control Strategy", *Business and Society Review*, 108(1): 95-113.
Schmalleger, Frank.(2006). *Criminology Today: An Integrative Introduction, New Jersey*: Upper Saddle River, New Jersey: Prentice Hall.
Stuart, F. H., Allison, Amie M. Schuck and Kim Michelle Lersch.(2005). "Exploring the Crime of Identhity Theft: Prevalence, clearance rates, and victim/offender characteristics". *Journal of Criminal Justice,* 33: 19-29.
Sullivan, Bob.(2004). *Your Evil Twin: Behind the Identity Theft Epidemic*. New Jersey: John Wiley & Sons, Incorporated.

Abstract

A study on The Private Investigator usage for Enterprise Security Activity:
Focusing on countermeasure to the Industrial Spy

Sin, Sung-Gyun · Park, Sang-Jin

National security of post cold-war since 1990′s shift that conception of the national security transfer traditional military strength to economic strength. Accordingly, the national interest about how to protect the of the high-technology industry enterprises has become contentious social issue.

The U.S. and advanced countries promote the policy to protect The United State′s Economic Espionage Act(EEA).

The Korea reaching to high level a field at IT, Shipbuilding, Steel, Automobile Industry and huge capital investment to high-technology & development. But, systematic industry security activity not an unfold.

So private investigator collect the evidence and information of business case for prevent danger is efficient. The private investigator system, deal with the matter efficiently, will good system to prevent economic loss of business, state and nation through make a good use in business crime that machinery of law difficult to intervene.

This article countermeasure about industry spy through make a good use of private investigator.

Key Word : Private Investigator, Enterprise Security, Industrial Spy, police

논문투고일 2009.07.31, 심사일 2009.08.10, 게재확정일 2009.09.01