산업스파이 현황과 대응방안

Analysis and Countermeasure on Actual Condition of Industrial Espionage

정덕영*, 정병수**
경동대학교 경찰경호학부*, 동국대학교 경찰행정학과**

Duke-Young Jeong(jduke@k1.ac.kr)*, Byoung-Soo Jeong(2079bs@hanmail.net)**

요약

산업스파이는 더 이상 한 기업의 문제가 아닌 국가의 경쟁력이 달린 국가적 차원의 문제로 이에 대한 현재의 실태를 분석하고 대응방안을 모색해야 할 중요한 문제가 되고 있다. 특히, 우리나라에서 매년 증가하고 있는 산업스파이에 의한 산업기밀의 유출은 막대한 국가적 피해를 초래하고 있다. 이 연구에서는 산업스파이에 대한 실태와 문제점을 분석하고 산업스파이에 대하여 효과적으로 대응하기 위한 방안들을 제시할 것이다.

■ 중심어 : | 산업스파이 | 첨단기술활용 | 산업보안 |

Abstract

The industrial espionage issue is not just limited on company competitiveness, but the country competitiveness depends on it too. As the number of espionage cases is increasing year by year, a damage to the country's industries rises accordingly. In this paper, we will analyse a case study of an actual industrial espionage and problems, then search for countermeasures on the issue.

■ keyword : | Industrial Espionage | Pointed Technology Application | Industrial Security |

Ⅰ. 서론

우리는 지금 '정보화 시대', '세계화 시대', '무한경쟁의 시대'에 살아가고 있다. 이러한 시대적 흐름에 우리가 효과적으로 대처하기 위해서는 전문 지식과 기술이 다른 나라 또는 다른 개인이나 집단보다 앞서야 한다. 우리나라는 과거와 달리 단순한 기술수입국에서 벗어나 상당한 정도의 첨단과학 기술을 보유하고 있으며 이를 위하여 많은 투자를 하고 있다.

이렇게 우리나라의 경제규모가 커지고 첨단기술의 보유가 늘어나면서 핵심기술과 산업정보는 국가경쟁력에 있어 매우 중요한 역할을 하고 있다. 따라서 경쟁자나 적으로부터 중요한 기업비밀이나 산업정보 등을 보호하는 것은 현대의 지식정보화 사회에 있어서 매우 중요하다.

산업사회에서의 기술과 정보 등의 유출은 막대한 국가경쟁력의 손실을 유발할 수 있기 때문에 선진국의 경우 이러한 피해에 효과적으로 대처하기 위하여 국가차원에서 법률을 제정하는 등 기업과 국민들에게 이를 적극적으로 홍보하고 있는 실정이다.

또한 냉전의 종식과 함께 세계가 군사정보보다는 경제정보에 더 큰 관심을 가지게 되어 각국의 국가정보기관은 산업정보, 산업스파이 그리고 첩보행위와 같은 경쟁적 정보활동에 참여하고 있다[1].

접수번호 : #071105-003
접수일자 : 2007년 11월 05일
심사완료일 : 2007년 11월 14일
교신저자 : 정덕영, e-mail : jduke@k1.ac.kr

우리나라의 경우, 1998년 2월 KNTC라는 회사의 간부들이 삼성전자, LG반도체의 전·현직 연구원 14명을 꾀어 첨단반도체 기술을 빼내어 대만기업에 유출한 사건이 그 대표적인 사례이다. 이 사건으로 인한 추정피해액이 자그만치 1조2천5백억원에 달할 뿐 아니라, 그 범행대상이 우리나라가 세계적 경쟁력을 갖고 있는 반도체의 제조기술이라는 점 등으로 인하여 사회적으로 큰 반향을 불러일으켰다[2].

이 사건을 계기로 국가와 기업뿐만 아니라 대다수의 국민이 국내의 산업기밀보호에 대해 많은 관심을 가지게 되었으며, 여러 가지 대응방안에 대해서도 다각적으로 연구되고 있다.

그러나 대부분의 산업스파이에 대한 연구가 주로 단속 법규에 관하여 진행되고 있으며, 기업의 영업비밀 보호와 관련된 법적 보호제도 등에 대해서만 연구가 이루어지고 있는 실정이다. 매년 증가하고 있는 산업스파이에 대해 근본적인 원인을 제대로 파악하지 못하면 이에 대한 올바른 대응방안을 제시할 수 없기 때문에 이에 대한 연구가 선행되어야만 효과적인 대응방안을 모색할 수 있을 것이다.

따라서 이 연구에서는 산업스파이에 대한 실태와 문제점을 분석하여 산업스파이에 효과적으로 대응할 수 있는 방안을 제시하고자 하는데 그 목적이 있다.

Ⅱ. 산업스파이의 의의

1. 산업스파이의 개념

산업스파이에 대한 통일된 정의는 아직까지 이루어지지 못했으며, 이를 정의하는 국가, 기관, 학자에 따라 그 의미가 조금씩 다르게 정의되고 있다. 또한 그 용어에 있어서도 다양하게 규정되고 있다.

전통적으로 스파이(espionage)라 함은 스파이들이 적의 군사적 기밀을 획득하는 수단이나 방법을 가리키는 것[3]으로서, 스파이의 기원은 군대에 그 바탕을 두고 있다[4]. 원래 스파이의 어원은 '멀리 본다' 또는 '숨겨져 있는 것을 목격 또는 발견 한다'라는 의미의 고대 프랑스어인 'espier'가 변화한 것으로 알려져 있다[5].

냉전 이후의 경제 전쟁시대에 있어서 산업스파이는 파견 주체가 다르다할지라도 국가안보의 목적보다는 상업적 목적에서 스파이활동이 수행되고 있기 때문에 이 연구에서는 한상훈(2000)의 연구를 토대로 경제스파이와 산업스파이를 동의어적인 관점에서 산업스파이의 개념을 정의하고자 한다.

즉 산업스파이란 파견 주체가 누구인지와는 상관없이 경제적 목적으로 상대국의 기업이나 회사가 소유하고 있는 물품의 제조방법, 판매방법, 기타 산업상, 영업상 유용한 기술이나 경영정보 등 산업체의 업무에 관한 비밀, 줄여서는 영업비밀이나 산업기밀 등을 불법적으로 입수하거나 정탐하는 일체의 행위 또는 이러한 행위를 자행하는 사람으로 정의할 수 있다.

2. 산업스파이의 유형

산업스파이라 하면 종래에는 다른 나라의 스파이 기관들에 의한 비밀정보 취득을 의미하는 경우가 많았다. 당시의 스파이들은 소위 "스파이활동"(Clock and dagger)책략을 사용하여 유괴, 납치, 고문, 살해, 도청 등과 같은 불법적인 행위를 자행하였다.

이러한 전통적인 방법들이 지금도 일부 정보기관들에 의해 여전히 사용되고 있기는 하지만, 이와 같은 "물리적" 정보취득 방법을 사용할 필요성은 근래의 정보통신기술의 발달로 현저히 감소하였다.

오늘날에는 대부분의 비밀 영업정보를 불법적 수단을 사용하지 않고 얼마든지 취득할 수 있기 때문에 "물리적" 정보취득 방법은 감소하고 있는 것이다. 또한, 스파이활동의 주체도 크게 변화하여 최근에는 외국정부나 스파이기관들에 의한 스파이활동은 크게 감소하였으며, 산업스파이의 절대 다수가 서로 경쟁관계에 있는 민간기업체들에 의해 자행되고 있는 추세에 있다[6].

B. Parad(1997)는 산업스파이 기법들을 무려 79종으로 정리하였으며[7], Nodoushani(2002)의 연구에서는 산업스파이의 다양한 형태로서 크게 7가지로 분류[8]하고 있다. Parad의 분류는 산업스파이의 기법들이 서로 유사하거나 중첩되는 경우가 많고, Nodoushani의 분류는 최근에 많이 발생하고 있는 산업스파이의 유형을 소개하고 있지 않기 때문에 아래에서는 비교적 빈번히 발

생하고 중대한 것으로 인식되는 몇 가지를 산업스파이의 유형으로 분류하여 설명하고자 한다.

따라서 이 연구에서는 민수홍·이민식(2006)의 연구를 토대로 하여 산업스파이의 유형을 크게 ① 스카우트(Hiring Away), ② 기업내부자의 매수(Buying up insider of the company), ③ 무단침입(Unlawful Entry), ④ 전통적인 절도(Old-Fashioned Theft), ⑤ 위장침투(Infiltration), ⑥ 컴퓨터접속 또는 해킹(Computer Hook-up), ⑦ 인터넷(Internet), ⑧ 방문(Visiting), ⑨ 전송자료의 가로채기(Interception of Data Transmission), ⑩ 정보브로커(Information Broker), ⑪ 휴대전화 도·감청(Public Airways), ⑫ 자료의 촬영, 녹음, 도청(Photo/Video/Audio Recording, Eavesdropping), ⑬ 항공촬영(Aerial Photography), ⑭ 평가(Evaluation)의 14가지로 분류하고자 한다. 다만, 이러한 방법들은 불법인 경우도 있으나 그렇지 않은 경우도 많다.

3. 산업스파이의 특징

산업스파이는 일반범죄와 구별하여 볼 때 다음과 같은 특징이 있다[9].

첫째, 산업스파이는 각국의 국내법상 허용되지 아니한 방법을 동원하여 정보를 습득한다는 측면에서 볼 때 고의에 의한 범죄행위이다. 반면에 일반범죄는 고의와 과실에 의해서 행하여진다.

둘째, 그 고의도 보복, 원한관계의 청산, 충동으로 자행되는 일반범죄와는 달리 오로지 첨단기술정보를 절취하여 경제적 이익을 달성하기 위한 목적으로 행하여진다.

셋째, 산업스파이의 목적물의 소유주는 국가, 기업 또는 사인이 될 수 있다. 또 그 목적물은 절취된 이후에 경제적 가치로 환산하기 위하여 생산과 판매라는 일련의 과정이 필요하다. 즉 목적물이 생산기술, 생산방법, 설계도 등이므로 금전적으로 환산되기 위해서는 투자·생산이라는 일련의 과정이 필요하다. 반면에 일반범죄는 일반적으로 범죄자들의 목적물의 소유주는 주로 개인과 기업이다. 그 목적물도 금전 또는 금전적 가치가 있는 장물이 대부분이고 투자와 생산이라는 일련의 과정은 필요가 없다.

넷째, 그 목적물의 경제적 가치는 얼마라고 간단히 대답할 수 있는 성질의 것이 아니다. 목적물에 따라서 수 천 억원의 가치로 환산될 수 있고 그 기술의 내용에 따라서 크게 차이가 날 수 있다. 그러나 일반범죄의 목적물은 대부분 쉽게 금전적 가치로 환산할 수 있는 것들이다.

표 1. 일반범죄와 산업스파이와의 비교

구 분	일반범죄	산업스파이
정신적 요소	고의 및 과실	고의
주된 목적	보복, 원한 관계청산, 충동, 경제적 이익	경제적 이익
목적물의 소 유 주	국가, 기업 및 개인이지만 주로 개인과 기업	국가, 기업 및 사인이지만 주로 기업과 국가
목적물의 형 태	금전적으로 쉽게 환산할 수 있는 장물이고 그 장물의 판매가 필요함	생산기술, 생산방법, 설계도가 금전적으로 환산되기 위해서는 투자생산이라는 일련의 과정이 필요함
목적물의 가 치	쉽게 금전적 가치로 환산할 수 있는 것	기술의 내용에 따라서 그 경제적 가치가 현격하게 다름
목적물의 존재형태	주로 유형적 형태로 존재함	유·무형적 형태로 존재함
주 체	누구나 될 수 있음	특정분야의 전문가
방 법	공개 또는 은밀하게 행하여짐	항상 은밀한 방법으로 행하여짐
신 분	일반 사인의 신분	외교관의 신분으로도 가능

다섯째, 목적물이 어떠한 형태로 있느냐라는 측면에서 볼 때 설계도, 컴퓨터에 입력된 프로그램 및 첨단기술을 개발한 사람의 머리에 기억될 수 있다는 점에서 주로 무형적인 형태로 존재한다. 반면에 일반범죄의 대상은 지폐, 지갑, 신용카드 및 타인이 소유 또는 점유하는 재물로서 대부분 유형적인 형태로 존재한다.

여섯째, 산업스파이행위는 첨단산업기술을 개발하였거나 개발할 능력이 있는 사람을 스카우트하는 것도 가능하다는 점에서 특정분야의 전문가이어야 한다. 반면에 일반범죄는 누구나 자행할 수 있는 특징이 있다.

일곱째, 산업스파이는 007과 같이 고도의 훈련을 받은 사람 또는 해당기업 내부에서 근무하는 사람을 매수

해서 행해질 수 있다는 점에서 항상 은밀하게 또는 은밀한 방법으로 행해질 수 있는 특징을 갖고 있다. 반면에 일반범죄는 공개 또는 은밀하게 행하여진다.

여덟째, 신분적인 측면에서 볼 때 산업스파이는 외교관 또는 비밀리에 파견한 국가요원이 행할 수 있다. 반면에 일반범죄는 범죄단체에서 특정한 범죄행위를 자행할 목적으로 다른 나라로 파견한다 하더라도 모두 일반 사인의 신분이다.

Ⅲ. 산업스파이의 실태분석

1. 산업스파이의 발생현황

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.

그러나 최근에는 정밀기계, 자동차, 생명공학 등도 다른 부분에 있어서도 산업스파이들의 주요 표적이 되고 있다. 이러한 국내 첨단기술의 유출이 국가 경쟁력과 직결되는 문제로 대두되면서 국가정보원은 2003년 10월「산업기밀보호센터」를 설립하고 산업스파이 적발 및 기술보호 활동을 수행하고 있다. 국가정보원「산업기밀보호센터」는 2003년 이후 2006년 12월 말까지 총 92건의 국내 산업기술의 해외유출 사건을 적발하여 약 95조 9천억 원 상당의 피해를 예방하였다[10].

국가정보원의 통계에 따르면 [그림 1]에서 보는바와 같이 2003년에 6건에 불과하던 것이, 2004년에는 26건, 2005년에는 29건, 지난해에는 31건이나 발생하여 산업스파이가 점차적으로 증가하고 있음을 알 수 있다.

[그림 1]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.

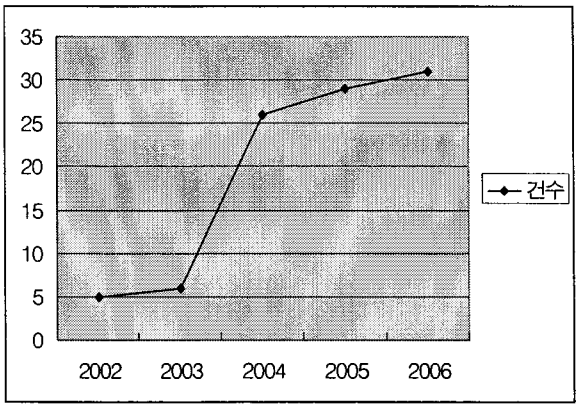


그림 1. 산업스파이 적발 현황

1.1 분야별 기술유출 현황

기술유출 분야는 우리나라가 세계적 경쟁력을 가진 휴대폰·반도체 등 전자·정보통신 분야가 총 92건 중 67건(73%)이나, 최근에는 자동차·조선 등 다른 분야로까지 확대되고 있는 추세로 기술유출이 어느 특정분야에 한정되지 않고 광범위하게 이루어지고 있음을 알 수 있다.

1.2 신분별 기술유출 현황

신분별 기술유출 현황을 살펴보면 주로 전·현직 직원(79건, 86%)에 의한 생계형 기술 유출이 대부분임을 알 수 있다. 기업의 내부자가 정보유출에 깊게 관여하게 되는데 내부자는 보통 목표물인 기술정보를 내장한 저장장치와 이를 입수할 수 있는 인적 네트워크를 소유하고 있으며, 내부통제 및 보안구조의 허점 등에 대해서도 잘 알고 있어 기술유출을 용이하게 할 수 있다고 생각된다.

최근에 사회적 이슈로 떠올랐던 현대·기아차 기술유출 사건과 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·현직 직원

들에 의해 이루어진 것으로 조사결과 나타났다[11].

또한 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.

1.3 유형별 기술유출 현황

유형별 기술유출 현황을 살펴보면 연구원을 매수하여 기술을 유출하는 유형이 71건으로 가장 많았다. 연구원 매수는 대부분 스카우트 형식으로 고액의 돈을 제시하는 등 금전적 유혹에 의한 매수로 이루어지고 있다.

IMF 구조조정을 겪은 연구원들은 신분에 대한 불안감 때문에 고액연봉, 중국 등 해외근무 조건이 제시되면서 거부하기가 어려운 등 금전적 유혹에 취약하다.

다음으로는 공동연구 5건, 위장합작 4건, 불법수출 3건, 해킹 2건 등을 나타내고 있다. 기업차원의 공동연구와 위장합작을 통한 기술유출이 총 9건으로 해외업체들은 국내 핵심연구원에게 접근하여 합작법인 설립 시 경영권을 주겠다고 유혹하거나 경영컨설팅이라는 명분으로 관련기술 절취 후 영업목적으로 절취기술을 재활용하는 사례가 빈번하게 나타나고 있다[12].

1.4 동기별 기술유출 현황

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.

이처럼 산업스파이는 대부분 금전적 이익과 개인적 이익을 위하여 범죄를 저지르고 있음을 알 수 있다. 또한 비리연루와 신분불안이 각각 4건으로 나타났다.

2. 기업의 산업기밀 관리현황

한국산업기술진흥협회는 기업의 산업기밀 관리실태 등을 조사하기 위해 2006년 5월 9일부터 2006년 5월 19일 까지 기업연구소를 보유한 11,325개 회사에서 업종별, 매출액별로 이원 층화추출한 459개 회사를 임의로 선정하였다.

조사방법으로는 팩스, 이메일 및 전화를 통한 설문조사를 실시하였다. 다음은 한국산업기술진흥협회의 조사결과를 토대로 기업의 산업기밀 관리 현황을 살펴보면 다음과 같다[13].

2.1 조직 및 제도

산업기밀 관리에 대한 조직 및 제도를 살펴보면 보안관리 규정은 전체 58.8%로 대체적으로 기업들은 산업보안에 대한 중요성을 인식하고 있음을 알 수 있다. 그러나 보안전담부서의 설치나 정례 보안점검 및 감사는 상대적으로 낮아 기업의 보안관리 감독체계가 대체적으로 부실함을 알 수 있다.

표 2. 기업의 산업보안 관리 조직 및 제도 (단위:%)

구분	항목	전체	대기업	중소기업	벤처기업
조직및제도	보안관리규정 마련	58.8	81.9	47.6	58.5
	보안담당부서 설치	17.9	42.6	13.2	9.7
	보안담당자 지정	49.0	64.9	43.4	46.6
	정례 보안점검, 감사	26.6	56.4	19.6	18.2

기업규모별로 살펴보면 대기업은 산업보안의 중요성에 대한 인식으로 보안관리의 감독체계에 관심을 갖고 대응을 하는 것으로 분석되나, 중소기업이나 벤처기업은 자체 보안인프라가 부족하여 이에 보안담당부서의 설치나 정례 보안점검·감사가 대기업과 비교했을 때 월등히 낮은 수준을 보여 이에 대한 관심과 대책이 요구되고 있다.

2.2 보안감독 체계

기업의 보안감독 체계를 보면 대체적으로 대기업의 경우 보안감독 시스템이 중소기업과 벤처기업에 비해 월등히 높은 것으로 나타나고 있다. 입사 시 비밀엄수 서서약 작성, 퇴사 시 비밀유지 및 경업 금지서약 등 여러 가지 항목들이 중소기업과 벤처기업보다 높은 것으

로 나타나 기업의 산업보안 감독시스템에 많은 관심을 기울이고 있음을 알 수 있다.

그러나 중소기업과 벤처기업의 경우 입사 시 비밀엄수서약서 작성, 방문자 출입통제 등 기본적인 시스템만 실시하고 있어 보안감독 시스템에 대한 중요성과 인식을 제고시킬 필요성이 요구되고 있다.

표 3. 기업의 산업보안 감독체계 (단위:%)

	항 목	전 체	대 기업	중소 기업	벤처 기업
보안 감독 체계	입사구분시 비밀엄수서 서약 작성	58.8	78.7	48.7	59.1
	퇴사시 비밀유지 및 경업금지 서약	48.1	73.4	38.6	44.9
	거래업체 비밀유지계약	26.1	43.5	18.1	27.1
	정례 보안관리 교육	25.1	48.7	17.5	20.9
	연구노트, 일지작성	35.9	42.6	30.7	38.1
	방문자 출입통제	74.5	89.4	69.8	71.6

2.3 기밀관리 시스템

기밀관리 시스템은 산업보안에 있어 주로 기술적 보호장치를 말하는 것으로 기업의 기밀관리 시스템 현황을 살펴보면 다음과 같다. 연구실이나 실험실 등의 카드키 설치, 문서세단기, 패스워드 및 이동식 디스크 관리는 다른 항목들에 비해 어느 정도는 기밀관리 시스템이 구축되어 있다고 볼 수 있다. 이는 다른 기밀관리 시스템에 비해 상대적으로 많은 예산이 소요되지 않아 대기업과 중소·벤처기업이 큰 차이 없이 실행하고 있음을 알 수 있다.

그러나 상대적으로 예산이 많이 투입되는 정보보안 시스템이나 DRM(Digital Rights Management, 디지털 저작관리) 솔루션의 도입, 문서관리 시스템은 대기업과 중소·벤처기업간의 보유격차가 커 이에 대한 대책을 마련할 필요성이 요구된다. 다음은 이러한 시스템의 주요 내용이다.

정보보안 시스템은 주로 Firewall(방화벽), IDS (Intrusion Detection System, 침입 탐지 시스템) 등을 말하는 것으로 방화벽은 내부의 네트워크와 인터넷과 같은 외부의 네트워크 사이에 진입 장벽을 구축하는 네트워크 정책과 이를 지원하는 하드웨어 및 소프트웨어를 포괄하는 컴퓨터 보안 시스템을 말한다. 해킹과 같은 외부의 비정상적이고 불법적인 접근으로부터 내부 네트워크의 정보자산을 보호하고 각종 유해 정보의 유입을 차단하는 것이 목적이다.

또한 침입 탐지 시스템은 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템으로 침입 차단 시스템만으로 내부 사용자의 불법적인 행동(기밀 유출 등)과 외부 해킹에 대처할 수 없으므로 모든 내·외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보 감시가 필요하다.

표 4. 기밀관리 시스템 구축 현황 (단위:%)

	항 목	전 체	대 기업	중소 기업	벤처 기업
기밀관리시스템	카드키 설치 (연구실, 실험실 등)	63.0	79.8	56.6	60.8
	정보보안시스템 구축 (Firewall, IDS 등)	29.4	62.8	22.2	19.3
	문서관리 시스템 (보안등급 부여 등)	27.7	53.2	20.1	22.2
	DRM(디지털저작관리) 솔루션 도입	6.1	21.3	2.1	2.3
	문서세단기	58.8	85.1	51.9	52.3
	패스워드 및 이동식 디스크 관리	63.8	74.5	53.4	69.3

문서관리 시스템은 문서를 보안등급으로 나누어 문서를 관리하는 것을 말한다. 문서정보의 중요도를 표현한 것으로 중요도 단계와 중요도 범주로 나누어 관리하는 것을 특징으로 하는 것을 말한다.

최근에 산업기밀유출에 있어서 그 수법이 다양화되고 전문화되는 시대적 상황에 비추어 볼 때 이와 같은 기술적 보안시스템의 구축은 매우 중요하다. 그러나 재정적 여건이 충분하지 못한 소규모의 중소·벤처기업은 이에 대한 충분한 대책이 이루어지지 못하고 있다.

2.4 연구원 보상시스템

연구개발 성과에 대한 금전보상 시스템을 시행하는 기업을 보면 대기업 46.8%, 중소기업 39.7%, 벤처기업 56.3%로 다른 항목들에 대해 상대적으로 높음을 알 수

때문에 가능할지 모르지만 중소기업이나 벤처기업의 경우에는 규모의 영세성으로 인하여 자체 보안관리 시스템 구축에 있어 많은 어려움이 있다. 이를 위해서 정부가 핵심기술의 보안관리를 위하여 예산을 지원하는 방안도 고려해 볼 수 있을 것이다.

2. 민·관 협력체계의 구축

산업보안에 있어서 정부와 기업이 추구하는 목표는 다르다고 할 수 있다. 즉 정부는 산업보안의 가치를 국가안전보장 또는 국익보호에 두고 있는 반면 기업은 이윤 극대화에 두고 있다. 그러나 양자의 기술적 과정은 "관리"라는 동일한 현상으로 나타나게 된다. 특히 기업의 대형화로 조직의 규모가 확대되면서 업무처리의 분업·전문화가 요구되고 있고 기업의 사회적 책임성이 강조되면서 정부와 기업에는 어떠한 형태로든 협동의 필요성이 높아지고 있다.

산업보안도 예외일 수는 없다. 산업기밀의 유출이 궁극적으로는 국익과 관련된 사항이라는 점을 감안한다면 정부와 기업은 공동대응 방안을 모색하지 않을 수 없다. 이 문제를 효과적으로 해결할 수 있는 방안으로 정부와 기업 간의 협력체를 구성·운영하는 것이다[15].

경찰은 산업기밀 보호활동을 더욱 강화하기 위하여 2004년 3월 경찰청 및 각 지방청 홈페이지에 「산업스파이신고센터」를 개설·운영하는 한편, 각 지방경찰청 별로 산업체·연구소 보안담당자와 경찰관으로 구성되는 '산업보안협의회'를 구성하여 매년 2번(상반기·하반기)의 정례회의를 개최하고 있다[16].

그러나 이러한 '산업보안협의회'는 각 지방청 주관으로 첨단기술 보유업체 및 연구소 등을 자체적으로 선정하여 진행되고 있기 때문에 첨단기술을 보유하고 있으나 선정되지 않은 기업체에 대해서는 민·관의 긴밀한 협력체제를 구축할 수 없다.

따라서 각 지방청이 주관으로 자체적으로 선정하기보다는 신청에 의하여 진행되어야 효과적으로 협력체제가 이루어질 수 있다. 경찰과 정보교류 등 많은 부분에 있어 협력을 원하는 기업체가 있지만, 선정이 안 될 경우에 이러한 협조체제를 구축할 수 없기 때문에 경찰은 효과적인 민·관 협력체계를 구축하기 위하여 적극적으로 홍보를 하는 등의 노력을 하여야 할 것이다.

3. 기술인력에 대한 관리체계의 구축

외국의 많은 산업보안 전문가들은 산업보안에 대한 성공적인 프로그램을 운영하기 위해서는 인적자원관리가 효과적으로 이루어져야 한다고 지적하고 있다. 현직 직원은 기업의 비밀을 가장 많이 알고 있는 최상의 정보원이기 때문에 이에 대한 관리가 효과적으로 이루어져야 한다[17].

전·현직 직원에 의한 산업기밀이 유출되는 것을 예방하기 위해서 기업은 핵심인력에 대한 관리 시스템을 구축하여야 한다. 핵심인력에 대한 비밀유지계약을 체결하여 입사 시 비밀엄수서를 작성과 퇴사 시 비밀유지 및 경업금지 서약 작성 등을 의무화하여 산업스파이에 대응하여야 한다.

산업스파이는 대부분 전·현직 직원이 개인영리를 위하여 발생하는 만큼 기업은 핵심인력에 대하여 기술개발에 전념을 다할 수 있도록 충분한 보상과 대우를 해주어야 할 것이다.

예를 들면 제품개발에 따른 차별화된 보상시스템을 구축하는 것이다. 기술개발, 특허신청, 시제품 출시단계, 양산 등 단계별로 보상을 확대 실시하고, 양산 시점에는 그에 맞는 파격적인 보상을 해주는 것이다[18].

4. 산업보안에 대한 교육과 전문가 양성과정의 운영

산업스파이에 의한 산업기술의 유출은 사후대응보다 사전에 예방하는 것이 피해를 최소화할 수 있다. 따라서 산업스파이를 효과적으로 예방하고 대응하기 위해서는 정부차원에서 기술유출 사례, 대응전략, 산업보안 실무내용, 국내 외 보안관리 우수기업 벤치마킹 등의 정기적·주기적으로 산업보안 교육을 확대 실시하여야 하며, 국가차원에서 산업보안 교육을 통하여 산업스파이에 대해 효과적으로 대응할 수 있는 시스템을 마련하여야 한다.

또한 해외에 진출한 기업에 대한 기술유출 애로사항에 대한 자문활동 및 산업보안 세미나를 개최하는 등의 노력을 하여야 할 것이다. 피해기업이 대기업일 경우,

있다. 하지만 대기업과 중소기업은 전체의 50%도 미치지 못하고 있어 아직까지도 기술개발에 대한 보상을 제대로 시행하고 있지 않음을 알 수 있다.

표 5. 연구원 보상시스템 (단위:%)

항 목	전 체	대 기업	중소 기업	벤처 기업
퇴직 시 별도의 수당지급	5.7	6.4	4.2	6.8
연구개발성과에 대한 금전보상	47.5	46.8	39.7	56.3
퇴직 전 전직 준비기간 부여	11.5	10.6	6.3	17.6
퇴직 후 일정기간 생활보조비 지급	1.5	2.1	-	2.8
분사프로그램 운영	4.6	11.7	2.6	2.8
퇴직 후 계약직(촉탁직) 재임용	4.6	8.5	3.2	4.0

또한 퇴직 시 공로보상이나 퇴직 후 관리는 전체적으로 미흡한 편이어서 연구원의 보상시스템이 전반적으로 실행이 되지 않음을 알 수 있다. 산업스파이는 대부분이 개인의 영리를 추구하거나 금전적 이익을 얻기 위하여 행하여지고 있다. 그러나 현재 대다수의 기업들은 연구 개발자에 대한 충분한 보상시스템을 마련하지 못하고 있어 이에 대한 대책을 마련하여야 산업스파이를 효과적으로 대응할 수 있을 것이다.

2.5 산업기밀관리 애로사항

기업의 산업기밀관리의 주요 애로사항을 살펴보면 핵심인력 유출의 위험성 즉, 연구인력의 전직 및 스카웃 가능성이 28.5%로 가장 높게 나타났으며, 보안인프라 투자의 어려움이 20.5%, 다음으로 임직원의 기밀보호에 대한 관심부족이 16.3%, 법적·제도적 장치의 미흡이 15.8%로 산업기밀관리에 많은 어려움을 느끼고 있다고 조사되었다.

기업규모별로 살펴보면 대기업, 중소기업, 벤처기업 모두 핵심인력의 기술유출 위험성을 가장 큰 애로사항으로 꼽았으며, 대기업의 경우 일반 종업원의 산업기밀보호에 대한 관심부족에 대하여 큰 애로사항을 느낀다고 응답하여 산업보안에 대한 전반적인 인식과 관심이 부족함을 알 수 있다.

반면, 중소기업과 벤처기업은 인력, 장비 등의 보안인프라에 대한 투자곤란을 주요 애로사항으로 응답하였다. 이는 중소기업과 벤처기업 등 규모의 영세성으로 인하여 산업기밀관리에 어려움을 느끼고 있다는 것을 알 수 있다.

표 6. 산업기밀관리의 애로사항 (단위:%)

구 분	대 기업	중소 기업	벤처 기업	합계
핵심인력 유출 위험성	29.3	30.4	25.8	28.4
보안인프라 투자 곤란	18.6	18.0	24.1	20.5
종업원의 기밀보호 관심부족	22.9	16.9	12.0	16.3
법적·제도적 장치 미흡	15.4	16.4	15.3	15.8
보안업무 관련지식 부족	9.5	13.0	16.5	13.6
기술유출 동향정보 부족	4.3	4.5	6.0	5.0
기 타	0.0	0.8	0.3	0.4
합 계	100.0	100.0	100.0	100.0

Ⅳ. 산업스파이 대응방안

1. 산업보안 시스템의 구축

산업스파이로 인하여 산업기밀이 유출되고 나면 범인을 체포하더라도 이미 유출된 산업기밀로 인하여 기업의 피해는 막대할 수 밖에 없다. 즉 산업스파이는 사후대응보다 사전에 예방하는 것이 가장 효과적으로 산업스파이에 대응하는 것이다. 이렇게 산업스파이를 사전에 효과적으로 예방하기 위해서는 다음과 같은 보안관리 감독체계가 구축되어야 할 것이다.

정교하고 고도로 발달된 산업 물품과 관련된 기업은 산업스파이에 대하여 자체적으로 방어시스템을 갖추어야 한다. 기업은 산업스파이에 대응할 수 있는 방어 전략을 수립하여야 한다[14].

기업 내 담당부서를 설치하여 보안담당자를 지정하고, 정기적으로 보안점검 및 감사를 실시하는 등 사전에 산업스파이를 예방할 수 있는 보안관리 감독시스템을 구축하여야 할 것이다.

또한 대기업의 경우에는 자체 보안관리 시스템 구축하는데 있어서 자체적으로 충분한 예산이 뒷받침되기

로폄 등 법률가의 조언으로 민·형사적 구제방안 중 기업에서 편의한 방법을 선택하여 충분한 법률적 조력을 받을 수 있지만, 영세한 중소기업이나 벤처기업의 경우는 구제절차를 잘 모를 뿐만 아니라 비용 면에서 감당하기 어려운 경우가 발생할 수 있다[19].

따라서 정부차원에서 피해기업들에 대한 자문활동을 수행하여 구제절차, 법률가의 조언 등 자문활동을 하여 우리나라 기업이 해외에서 피해를 당하는 일을 예방하여야 할 것이다.

과학기술분야의 급속한 발전과 더불어 기업과 관련된 광범위한 정보보호를 관리하기 위해서는 산업보안의 전문지식과 능력을 갖춘 전문가를 양성하여야 한다. 우리나라의 경우 이러한 시대적 흐름에 부흥하기 위해 산업보안 전문가를 양성하고자 많은 노력을 하고 있지만 선진국에 비해 아직까지 부족한 부분이 많다.

산업보안 전문가를 효과적으로 양성하기 위해서는 대학에 산업보안 전문가 양성과정을 개설하는 방안을 고려해 볼 수 있다. 지금까지 산업보안에 관련된 학문은 매우 다양한 학문분야에 걸쳐서 연계가 되어 있기 때문에 특정한 학문분야로 한정하기에는 어려운 점이 많으나 주로 경찰행정, 경호경비, 정보보호, 산업안전 및 소방 등 관련분야에 학자들의 다양한 연구가 이루어지고 있기 때문에 대학에 산업보안 전문가 양성과정을 개설하는 것이 좋은 방안이 될 수 있다.

또한 정부차원에서 산업보안 전문가 자격증(가칭)을 발급하는 방안이 있다. 산업보안 전문가 자격증은 각종 보안업체뿐만 아니라 일반기업에서의 보안분야 종사자에게 필수적인 조건으로 활용하여 산업스파이에 효과적으로 대응할 수 있도록 하는 것이다.

V. 결론

이 연구에서는 산업스파이에 대한 실태와 문제점을 분석하여 산업스파이에 효과적으로 대응하기 위한 방안들에 대하여 살펴보았다. 이상으로 산업스파이에 대하여 효과적으로 대응하기 위한 방안들을 간략히 정리해보면 다음과 같다.

첫째, 보안관리 감독체계의 구축을 들 수 있다. 산업스파이로 인하여 산업기밀이 유출되고 나면 범인을 체포하더라도 이미 유출된 산업기밀로 인하여 기업의 피해는 막대하기 때문에 산업스파이는 사후대응보다 사전에 예방하는 것이 가장 산업스파이에 효과적으로 대응하는 것이다. 따라서 보안관리의 감독체계의 구축은 무엇보다도 중요하다. 보안관리의 감독체계를 구축하기 위해서는 기업의 보안관리 감독시스템의 구축과 민·관 협력체계의 구축이 효과적으로 이루어져야 할 것이다.

둘째, 산업보안 교육 및 자문활동을 강화를 들 수 있다. 산업보안 교육 및 자문활동을 강화하기 위해서는 정부 및 관련기관은 중소·벤처기업의 보안 취약점 진단 및 보안 마스터플랜 등을 수립하고 지원하여야 한다. 또한 정부차원의 산업보안 교육을 확대하고, 해외에 진출한 기업에 대한 기술유출 애로사항에 대한 자문활동 및 산업보안 세미나를 개최하는 등의 노력과 산업보안 전문가 양성과정을 운영하여야 갈수록 지능화·교묘화 되고 있는 산업스파이에 효과적으로 대응할 수 있을 것이다.

이 밖에도 산업스파이에 대한 법·제도적 장치의 마련이 필요하며 산업보안에 대한 인식도 제고되어야 한다. 산업스파이 문제는 더 이상 기업만의 문제가 아닌 국가차원의 문제이기 때문에 전반적인 사회적 인식의 전환이 필요하다. 이를 위해서는 기업뿐만 아니라 정부는 대대적인 홍보와 관련 교육 등에 관심을 갖고 적극적으로 대처하여야 할 것이다.

참 고 문 헌

[1] 이윤호, *현대사회와 범죄의 이해*, 삼경문화사, 2004.

[2] 한상훈, *산업스파이에 대한 형사법적 대응방안*, 한국형사정책연구원, 2000.

[3] H. Nasheri, *Economic Espionage and Industrial Spying*, Cambridge University Press, 2005.

[4] D. J. Morris, L. P. Ettkin, and M. M. Helms,

"Issues in the illegal transference of US information technologies," Information Management & Computer Security, Vol.88, No.4, p.164, 2000.

[5] 조병인, 정진수, 정완, 탁희성, *사이버범죄에 관한 연구*, 한국형사정책연구원, 2000.

[6] 민수홍, 이민식, "외국의 신종범죄 발생현황과 대책", 치안정책연구소 치안논집, 제22집, p.218, 2006.

[7] P. Boris, "Commercial Espionage: 79 Ways Competitors Can Get Any Business Secrets in Any Country," Global Connection, Inc., pp.9-59, 1997.

[8] O. Nodoushani and P. A. Nodoushani, "Industrial espionage: The dark side of the digital age," *Competitiveness Review*, Vol.12, No.2, p.98, 2002.

[9] 문규석, "국제법상 산업스파이에 관한 연구", 성균관대 비교법연구소, 성균관법학, 제17권, 제3호, pp.413-414, 2005.

[10] 산업기밀보호센터, *첨단기술 유출실태 및 보호활동*, 산업기술의 유출방지 및 보호에 관한 법률에 대한 논의 세미나 자료집, p.8, 2007.

[11] http://news.media.daum.net/politics/administration

[12] 민수홍, 이민식, "외국의 신종범죄 발생현황과 대책", 치안정책연구소 치안논집, 제22집, pp.260-261, 2006.

[13] 노민선, *기업연구소 산업기밀 관리실태 및 개선방안*, 한국산업기술진흥협회, pp.49-59, 2006.

[14] A. C. Samli and L. Jacobs, "Counteracting Global Industrial Espionage: A Damage Control Strategy," Business and Society Review, Vol.108, No.1, p.105, 2003.

[15] 민병설, *산업보안체계의 정립에 관한 연구*, 경희대학교 대학원 박사학위논문, p.161, 2002.

[16] http://www.police.go.kr/pds/whitePaperView.do

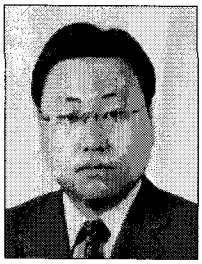
[17] P. C. Wright and G. Roy, "Industrial espionage and competitive intelligence: one you do; one you do not," Journal of Workplace Learning, Vol.11, MCB University Press, p.56, 1999.

[18] 노민선, *기업연구소 산업기밀 관리실태 및 개선방안*, 한국산업기술진흥협회, pp.62-65, 2006.

[19] 남상봉, "산업스파이 수사사례 분석 및 대응방안", 국가정보원, 산업보안 연구논총, 제1호, p.47, 2004.

저 자 소 개

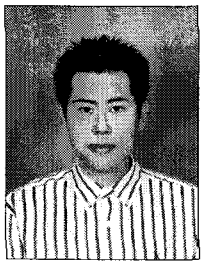
정 덕 영(Duke-Young Jeong) 정회원



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

<관심분야> : 경찰학, 범죄학, 민간경비

정 병 수(Byoung-Soo Jeong) 정회원



- 2005년 3월 : 동국대학교 경찰행정학과(경찰학석사)
- 2007년 9월 ~ 현재 : 동국대학교 경찰행정학과(박사과정)
- 2007년 9월 ~ 현재 : 중부대학교 경찰행정학과 강사

<관심분야> : 경찰학, 범죄학, 산업보안