

## 외국인 산업스파이에 의한 산업기술유출 대응방안에 관한 연구 - 단기 출입국자를 중심으로 -

A Study on Countermeasures of the Industrial Technology Leakage Crimes  
by Foreigner's Immigration Control  
- Focused on Short-term Entry and Exit Passenger -

주 성 빈(Joo, Sung-Bhin)\* · 최 응 렬(Choi, Eung-Ryul)\*\*

### ABSTRACT

The South Korea put a lot of hard effort to secure Core Technology. Consequently, as of March 2012, South Korea designated and maintained the national core technology of electrical and electronic 8 technology, automobile manufacturing 8 technology, shipbuilding 6 technology, steel 7 technology, nuclear energy 4 technology, information and communication 17 technology, space engineering 5 technology and biotechnology 3 technology.

But, as the number of technology leakage crimes cases is increasing year by year, a damage to the country's industries rises accordingly.

Main agents of industrial technology leakage is commonly recognized by former employee, current employee today. But industrial technology leakage by foreigner nonimmigrant will increase day by day.

In this paper, we will analyse a case study of an actual technology leakage crimes and problems, then search for countermeasures on the issue.

First, immigration control system must maintain consistency: law and institutional devices of immigration control system for technology leakage crimes are demanded. Second, the fingerprint recognition system also had to be fortified to prevent industrial technology leakage by foreigner nonimmigrant. The third, we builds integrated personal information sharing system.

It is no use to capture the espionage, after the industrial technology leakage. Because it would cause irreparable damage to the South Korea or company. So prevention is more effective than after the fact countermove.

Therefore, the government, companies and citizen all should cooperate for the construction of security administration and supervision.

It is very important that establishment of the immigration control system and integrated personal information sharing system.

Key Words: Foreigner, Industrial Technology Leakage, Industrial Espionage, Nonimmigrant, APIS(Advance Passenger Information System)

\* 동국대학교 일반대학원 경찰행정학과 박사과정(제1저자)

\*\* 동국대학교-서울 경찰행정학과 교수(교신저자)

## I. 서론

국가간 치열한 경제전쟁 속에서 기술개발과 더불어 산업기술의 보호가 국가 산업경쟁력 강화를 위한 중요한 요소로 대두되고 있다. 왜냐하면 산업기술 유출문제는 피해규모에 따라서 단순히 기업에 국한되는 문제가 아니라 국가 경쟁력 저하에 결정적인 영향을 미칠 수 있기 때문이다.

현재 산업기술의 유출 목적, 수단, 대상은 과거와는 달리 다양한 형태로 등장하고 있음을 국가공공기관, 각종 언론매체 등을 통해서 쉽게 접할 수 있다. 변화된 양상에 대해서 구체적으로 살펴보면, 유출 목적은 상대국 동향 파악 등 군사전략적 목적에서 기술 및 기술정보 선점을 통한 경쟁력 우위 확보로 변화하였고, 유출 수단은 문서 등과 같은 단편적 수단에서 대용량의 소형 이동식 기기와 통신기술 등을 통한 최첨단 기법으로 발전하였으며, 유출 대상은 시설·장비·제품 등에 대한 정보에서 산업인력 정보와 기술 자체 확보를 위한 정보수집으로 이동하고 있다(산업통상자원부, 2007: 3).<sup>1)</sup>

이렇게 산업기술의 유출형태가 다양해질수록 산업스파이가 범행을 계획하는 주 대상은 경공업부터 정보산업까지 거의 모든 산업분야를 망라하게 되고, 실제로 최근에는 항공, 통신, 컴퓨터 소프트웨어, 바이오, 제약, 에너지 등의 새로운 분야가 주요 표적이 되고 있다(<http://article.joinsmsn.com/>, 검색일: 2013. 4. 3).

산업기밀 유출의 주체는 외부 인력이나 업체보다는 주로 전·현직 직원에 의한 유출이 대부분이다. 국가정보원 산업기밀보호센터의 2005년~2011년 산업스파이 적발건수를 분석해 보면, 전체 기술유출의 79%가 전·현직직원으로 밝혀져 그 심각성의 정도를 가늠해 볼 수 있다(<http://service4.nis.go.kr/> 2013. 4. 5). 이처럼 지금까지 산업기밀을 보유한 분야에서 내부 출신이 유출주체로 가장 많은 비율을 차지하고 있는 이유는 누구보다 산업기밀에의 접근이 용이하고, 조직 내부적으로도 감시·감독이 상대적으로 허술했기 때문이라 여겨진다.

하지만 오늘날의 많은 국가와 기업들은 상호간에 인적·물적 교류가 빈번하게 이루

1)

구분	과거	현재
유출 목적	냉전 시대 ① 개인·기업의 발전보다는 국가경제 발전이 중요 ② 군사적 목적으로 상대국 동향 파악 정보수집	탈냉전 시대 ① 기업간 기술정보 선점을 통한 경쟁력 우위 확보 ② 합법적 방법을 동원한 첨단 산업기술 확보
	아날로그 시대 ① 저장매체의 미발달로 유출이 용이하지 못함 ② 문서, 노하우의 전수 등과 같은 제한적 유출 수단	디지털 시대 ① 대용량 소형 이동식 저장기기 등 발달로 정보유출 용이 ② 무제한 전송이 가능한 정보 통신기술
유출 수단	기술추격 시대	기술혁신 시대
	시설·장비·제품에 대한 정보	기술인력 정보나 산업기술 자체를 전문적으로 수집·유출

어지고 있어 과거보다는 점차 외부 인력에 의한 기밀유출이 심화될 것으로 판단된다. 그 중에서도 최근 연구원, 산업연수생 등 외국인이 한국 기업에 취업하고 있는 추세가 급증함에 따라 이들로 인한 기술 유출 사례가 다수 나타나고 있다.<sup>2)</sup> 비록 기술 유출의 전체 비율에 비추본다면 외국인에 의한 유출 정도가 미약하다고 여겨질 수도 있지만, 그 피해는 전·현직 직원에 의한 기밀유출 못지않을 것으로 예상된다. 왜냐하면 산업기술의 유출 목적을 가지고 입국하는 범죄자들은 국내 입국 전부터 우리나라에서 범행할 계획을 치밀하게 준비하였을 것이고, 또한 우리나라에서 체포되었을 경우 예상되는 처벌과 형량, 산업기술의 보호를 관장하는 관련기관의 활동 등을 모두 고려한 후 범행을 진행하는 등 심각성이 크기 때문이다(이창한, 2010: 281).

미국 국토안보부(DHS: Department of Homeland Security)는 2011년 비(非)이민자 입국허가 연례보고서(Nonimmigrant Admissions to the United States)에서 2011년 한 해 우리나라의 단기비자에 해당하는 비이민 입국허가 총 신고건수는 159,000,000건이었으며, 이중 출입국 신고서(Form I-94, 이하 I-94) 기준 비이민 입국허가는 33%인 53,082,286건으로 집계됐다. 출입국 신고서(I-94) 기준, 전체 입국허가 수는 2009년과 2010년에 각각 36,231,554건과 46,471,516건을 기록한 것에 이어 가파른 증가세를 보였다.

<표 1>과 같이 미국의 비이민자<sup>3)</sup> 입국허가 현황을 국적별로 살펴보면, 멕시코가 1,705만 2,559명(32.1%)으로 가장 많았다. 영국이 4,547,728명(8.6%)으로 2위, 일본이 3,777,643명(7.1%)으로 3위, 독일이 2,182,441명(4.1%)으로 4위였다. 뒤이어 캐나다

2) 국내 A전자 연구소에서 근무하던 중국인 연구원 C모씨는 A전자의 가전제품 소음방지 기술 및 경영전략 등 핵심 영업기밀 자료를 출력, 디지털카메라로 촬영한 뒤 노트북에 담아 중국 최대 가전업체인 H사로 전직시 해당 자료의 유출을 기도하다 적발된 사건이다. 이 사건은 외국인 연구원에 의한 산업기술 유출의 대표적인 사건으로 기술유출을 사전에 차단하여 국내 핵심 기밀 자료가 중국으로 유출·활용되었을 경우 발생할 기술격차 단축 등 막대한 피해를 사전 예방하였다(산업기밀보호센터, <http://service4.nis.go.kr/>, 검색일: 2013. 4. 10). 미국산업기밀보호협회(ASIA)에 따르면 미국이 연간 산업스파이로 입는 손실은 2002년 590억 달러에서 2012년은 2,500억 달러 이상으로 추산하고 있다. 지난 몇 년간 미국의 듀폰, 모토로라, GM, 마이크로소프트 등의 다국적 업체가 암호장비, 모바일폰 부품, F-35전투기 장비 등의 기술을 유출당했다. 한국도 예외는 아니다. 한국은 휴대전화와 반도체, 조선 등 최첨단 기술을 보유한 국가로 산업스파이의 핵심 타깃 중 하나다. 2012년 6월 삼성과 LG는 2조원 이상을 투자해서 개발한 55인치 TV용 능동형 유기발광 다이오드(AMOLED: Active Matrix Organic Light-Emitting Diode) 기술을 산업스파이에게 털렸다. 장비검사업체인 이스라엘 업체 오보텍의 직원이 디스플레이 패널의 장비검사를 하는 척하며 회로도를 몰래 찍어 유출한 것이다. 이들은 빼돌린 기밀자료를 경쟁업체인 중국과 대만 회사로 넘겼다. 아몰레드 기술은 국가핵심산업 기술로 지정돼 향후 5년간 30조원 이상의 수익을 올릴 것으로 기대하고 있었다(중앙일보, <http://article.joinsmsn.com/>, 검색일: 2013. 4. 12).

3) 미국의 비이민자 비자의 주요 유형은 다음과 같다.

A1: 중앙정부 고위직 또는 미국 주재 공관 파견 외교관과 그의 배우자 또는 자녀, A2: 대한민국 정부를 위해 공무원로 가는 정부공무원과 그의 배우자 또는 자녀, B1: 단기 상용 방문, B2: 단기 관광, F1: 정규교육 혹은 언어연수를 위한 유학, F2: F1 소지자의 배우자 또는 자녀, H1B: 전문직 직원(간호사 제외), H1C: 간호사, J1: 문화 교류방문자, M1: 직업교육 유학, M2: M1 소지자의 직계가족 등.

(1,868,179명, 3.5%), 프랑스(1,845,227명, 3.5%), 브라질(1,539,015명, 2.9%)이 5~7위에 올랐다.

한국은 1,460,972명(2.8%)으로 8위였다. 한국인 입국허가 인원은 2009년에 906,006명(전체의 2.5%), 2010년 1,332,387명(2.9%)으로 빠르게 늘어나는 추세를 보였다. 2011년 수치는 2010년 대비 9.65%, 2009년 대비 61.25% 증가한 것이다. 9위는 1,364,078명(2.6%)인 중국, 10위는 1,246,091명(2.3%)인 호주였다. 이를 분석해 보면, 상위 비율을 차지하는 10개 나라가 전체 출입국 신고서 기준 입국허가의 69%를 차지했음을 알 수 있다.

<표 1> 미국의 국가별 비이민자 입국 허가 현황(2009-2011)

(단위: 명, %)

국가	2011		2010		2009	
	인원	비율	인원	비율	인원	비율
전체	53,082,286	100.0	46,471,516	100.0	36,231,554	100.0
멕시코	17,052,559	32.1	12,917,788	27.8	6,601,059	18.2
영국	4,547,728	8.6	4,539,433	9.8	4,713,284	13.0
일본	3,777,643	7.1	3,831,174	8.2	3,368,590	9.3
독일	2,182,441	4.1	2,076,216	4.5	2,023,971	5.6
캐나다	1,868,179	3.5	1,428,940	3.1	1,683,372	4.6
프랑스	1,845,227	3.5	1,696,770	3.7	1,683,372	4.6
브라질	1,539,015	2.9	1,233,457	2.7	959,448	2.6
한국	1,460,972	2.8	1,332,387	2.9	906,006	2.5
중국	1,364,078	2.6	1,038,279	2.2	729,931	2.0
호주	1,246,091	2.3	1,037,683	2.2	834,000	2.3
기타	15,698,851	29.6	14,773,452	31.8	13,825,663	38.2
미상	499,502	0.9	565,937	1.2	294,588	0.8

※ 출입국 신고서 기준

자료: U.S. Department of Homeland Security, 2012: 5.

국토안보부가 이러한 비이민자에 대한 관심을 높이고 있는 이유는 미국의 첨단기술의 주요 유출 주체들이 이들이라고 판단하고 있기 때문이다. 즉, 2005년 외국인의 경제 정보수집 및 산업스파이에 관한 연례보고서(Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2005)에 의하면, 미국 경제가 개방되고 세계화가 가속화되면서 개인단위의 기술유출자들에게 유리한 환경으로 변화하고 있다고 밝히고 있다.<sup>4)</sup> 왜냐하면 이들이 미국을 단기간에 방문하고 자국으로 돌아갈 수 있는 수단(nonimmigrant visas)을 활용하여 신속하게 산업기술을 유출해 나가기 때문에

4) 출입국 신고서 기준 입국허가의 약 87%는 사업이나 관광 목적의 단기체류 목적이었다. 구체적으로 살펴보면, 관광목적은 약 76%, 비즈니스 목적은 약 11%를 차지하고 있다. 그리고 약 6.4%는 단기근로나 연수, 주재원과 미국 현지의 가족 방문이었으며, 약 3.4%는 유학생들이었다(U.S. Department of Homeland Security, 2012: 4).

적발과 검거에도 상당한 어려움이 있기 때문이다. 이와 관련된 첨단기술의 주요 유출 주체는 외국인 사업가, 과학자, 기술자, 학생 그리고 학자들이 있다(National Counterintelligence Center, 2006: 2).

이 연구는 위에서 살펴본 것과 같이 단기 출입국하는 외국인에 의한 산업기술유출의 위험성에 대한 인식을 바탕으로 국내의 효과적인 대응방안을 수립하기 위한 목적의 연구이다. 여기서 ‘단기’의 범위는 「출입국관리법」 제31조(외국인 등록)<sup>5)</sup>와 관련하여 체류기간에 따른 외국인 등록을 90일 기준으로 규정하고 있어 90일 이하로 정하고자 한다.

## II. 이론적 배경

### 1. 실태분석

우리나라의 2011년 총 출입국자는 2010년도 42,988,101명보다 2,434,809명(5.7%) 증가한 45,422,910명으로 2010년, 2011년 2년 연속으로 4천만 명을 돌파하였다. 출입국자의 증가는 내국인의 경우 전년 대비 1.9% 증가에 그친 반면 외국인의 경우에는 계속된 유럽발 경제위기 및 일본 대지진 등에도 불구하고 전년 대비 11.2% 증가를 기록하였는데, 이는 친절하고 신속한 출입국심사 서비스 제공과 비자 발급절차 간소화 조치로 중국, 일본 등 외국인 관광객의 증가에 기인한 것으로 평가되고 있다(법무부 출입국·외국인정책본부, 2012: 2).

입국허가 등급		2011	2010	2009
비자 유형	목적	비율	비율	비율
전체		100.0	100.0	100.0
B2 / WT 비자 등	관광	76.4	75.6	76.7
B1 / WB 비자 등	사업	10.8	11.2	12.1
F1, F2 / M1, M2 비자 등	유학	3.4	3.4	2.6
H 비자 등	단기근로 등	6.4	6.1	4.7
기타		3.0	3.7	3.9

#### 5) 「출입국관리법」 제31조 (외국인등록)

- ① 외국인이 입국한 날부터 90일을 초과하여 대한민국에 체류하려면 대통령령으로 정하는 바에 따라 입국한 날부터 90일 이내에 그의 체류지를 관할하는 사무소장이나 출장소장에게 외국인등록을 하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 외국인의 경우에는 그러하지 아니하다.

1. 주한외국공관(대사관과 영사관을 포함한다)과 국제기구의 직원 및 그의 가족
2. 대한민국정부와의 협정에 따라 외교관 또는 영사와 유사한 특권 및 면제를 누리는 사람과 그의 가족
3. 대한민국정부가 초청한 사람 등으로서 법무부령으로 정하는 사람

## 1) 출입국 현황

### (1) 연도별 출입국자 증감 추이

최근 연도별 내·외국인 출입국 현황을 <표 2>에서 살펴보면, 매년 지속적으로 증가하던 출입국자가 2008년 금융 위기 여파와 이후 국내 경기침체 및 신종플루 발생 등에 따라 대폭 감소되어 외국인 출입국자의 증가에도 불구하고 2009년까지 전체 출입국자가 감소되고 있다.

그러나 2010년부터 국내 경기회복 및 친절·신속한 출입국심사 서비스와 비자 발급절차 간소화 등 외국인 관광객 유치를 적극 지원하여 내·외국인 출입국자 수가 대폭 증가하였으며, 2011년까지 지속적으로 이어져 오고 있는 추세이다.

<표 2> 연도별 내·외국인 출입국 현황

(단위: 천명)

	2004년	2005년	2006년	2007년	2008년	2009년	2010년	2011년
총계	29,609	32,638	35,851	39,833	38,203	35,206	42,988	45,422
내국인	18,177	20,638	13,538	27,174	24,677	19,586	25,585	26,064
외국인	11,432	11,999	12,312	12,659	13,526	15,619	17,402	19,358
출국자	14,820	16,363	17,905	19,854	19,017	17,590	21,442	22,611
입국자	14,788	16,274	17,945	19,979	19,186	17,616	21,545	22,811

자료: 경찰청, 2012: 254; 법무부 출입국·외국인정책본부, 2012: 4.

특히, 외국인 입국자는 <표 3>과 같이 5년 연속하여 계속 증가하고 있으며, 2011년도는 9,765,902명으로 사상 최고를 기록하고 있다. 이는 한류 열풍과 함께 중국·동남아시아 국가 국민에 대한 비자 발급절차 간소화 조치에 힘입어 일본, 중국, 홍콩, 인도네시아, 말레이시아, 태국 등 아시아권 관광객의 대폭 증가에 기인한 것으로 보인다.

체류자격별 외국인 입국자는 관광통과(B-2) 50.9%(4,969,884명), 단기종합(C-3) 13.6%(1,324,640명), 선원 및 승무원 11.3%(1,099,399명), 사증면제(B-1) 9.3%(909,930명) 순이다. 외국인 입국자 중 전년대비 높은 증가율을 보인 체류자격 유형은 재외동포(F-4) 47.3%(61,070명), 영주(F-5) 41.5%, 단기종합(C-3) 38.1%의 순이었다.

<표 3> 외국인 입국자 체류자격별 현황

(단위: 명, %)

체류자격	2010년 입국자수	2011년		
		입국자수	구성비	전년대비
총계	8,766,915	9,765,902	100	111.4
관광통과(B-2)	4,601,828	4,969,884	50.9	108.0
단기종합(C-3)	959,374	1,324,640	13.6	138.1
선원 및 승무원	992,270	1,099,399	11.3	110.8
사증면제(B-1)	803,617	909,930	9.3	113.2
방문취업(H-2)	310,230	295,464	3.0	95.2

자료: 법무부 출입국·외국인정책본부, 2012: 15.

주: 상위 다섯 유형(전체의 88.1% 구성)의 체류자격 외에도 외교(A-1), 공무(A-2), 협정(A-3), 단기상용(C-2), 단기취업(C-4), 유학(D-2), 일반연구(D-4), 주재(D-7), 기업투자(D-8), 무역경영(D-9), 교수(E-1), 회화지도(E-2), 연구(E-3), 예술홍행(E-6), 특정활동(E-7), 비전문취업(E-9), 선원취업(E-10), 방문동거(F-1), 거주(F-2), 동반(F-3), 재외동포(F-4), 영주(F-5), 방문취업(H-2), 기타 유형이 있다.

## (2) 국적별 외국인 입국자 현황

<표 4>에서 2011년도 외국인 입국자를 국적별로 살펴보면 일본인 37.7%(3,270,290명), 중국인 23.6%(2,045,380명), 미국인 8.0%(694,990명), 타이완인 5.3%(457,680명), 홍콩인 3.1%(272,600명) 순이다. 2010년 대비 입국자 증가율이 높은 국가는 인도네시아 38.6%(23,759명), 말레이시아 38.2%, 홍콩 23.3%, 타이 19.8% 순인 반면, 독일 1.5%, 뉴질랜드 1.1% 각각 감소하고 있다.

<표 4> 국적별 외국인 입국자 현황

(단위: 명, %)

국적	입국자수	구성비	전년대비	국적	입국자수	구성비	전년대비
총계	8,666,503	100	111.5				
아시아주	7,145,097	82.4	113.5	아메리카주	842,110	9.7	100.6
일본	3,270,290	37.7	108.9	미국	694,990	8.0	100.2
중국	2,045,380	23.6	118.7	유럽주	502,205	5.8	105.7
타이완	457,680	5.3	104.5	오세아니아주	145,433	1.7	106.4
홍콩	272,600	3.1	123.3	아프리카주	30,506	0.4	107.7
				기타	1,152	0.0	112.1

※ 승무원 제외

자료: 법무부 출입국·외국인정책본부, 2012: 15.

## (3) 출국 외국인 체류기간별 현황

2011년도 외국인 출국자는 8,550,194명으로 체류기간에 따라 살펴보면 5일 이하가

72.8%(6,225,938명), 6일~10일 이하가 7.9%(672,821명)를 차지하고 있다. 결국, 외국인의 91.5%는 3개월 미만 단기 체류 후 출국하는 것을 알 수 있다. 자세한 사항을 살펴보면 <표 5>와 같다.

<표 5> 출국 외국인 체류기간별 현황

(단위: 명, %)

구분	2010년 출국자수	2011년		
		출국자수	구성비	전년대비
총계	7,669,426	8,550,194	100	111.5
5일 이하	5,626,012	6,225,938	72.8	110.7
10일 이하	565,300	672,821	7.9	119.0
20일 이하	322,468	343,972	4.0	106.7
6개월 이하	704,797	815,623	9.5	-
1년 이하	186,657	226,179	2.6	121.2
1년 초과	264,192	265,661	3.1	100.6

※ 승무원 제외

자료: 법무부 출입국·외국인정책본부, 2012: 19.

## 2) 국가 기업간 기술유출 현황

### (1) 국내 발생 산업스파이 사건 현황

<표 6>과 같이 2011년 총 84건의 산업기술유출사건을 적발하여 311명을 검거하였으며, 특히 중소기업 기술보호 활동에 집중한 결과 전체사건의 89.3%인 75건의 중소기업 기술유출 피해사건을 해결하였다.

<표 6> 연도별 산업스파이 검거실적 현황

(단위: 건, 명)

구분	계	2007년	2008년	2009년	2010년	2011년
검거건수	267	25	72	46	40	84
검거인원	954	80	245	164	154	311
국외유출	71	1	15	16	9	24
국내유출	206	18	57	30	41	60

자료: 사이버경찰청, 2012: 261; <http://service4.nis.go.kr/> (검색일: 2013. 4. 20).

### (2) 국가별 기술유출 현황

한편, 전체 유출사건의 28.6%(24건)가 해외 유출사건으로 파악되었으며, <표 7>과 같이 유출지역은 중국 이외 미국·독일·영국·대만·일본 등으로 다양화되고 있다. 유출유형을 살펴보면, 내부자의 이직 및 창업 등에 의한 피해가 전체 82%로 인적 보안관리의



중요성을 시사하고 있다.

<표 7> 국가별 주요 기술유출 현황(2003-2012년)

(단위: 명)

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	계
중국	0	0	0	1	1	1	0	2	3	1	9
일본	1	0	0	0	0	1	0	0	0	0	2
대만	0	0	0	0	0	1	0	0	0	0	1
호주	0	0	0	0	0	1	0	0	0	0	1
러시아	0	0	0	0	0	0	1	0	0	0	1
카자흐스탄	0	0	0	1	0	0	0	0	0	0	1
미상	1	7	3	0	3	0	0	1	0	0	15
계	2	7	3	2	4	4	1	3	3	1	30

자료: <http://service4.nis.go.kr/> 내용 재구성 (검색일: 2013. 4. 20).

### 3. 선행연구 검토

기술유출과 관련된 주된 연구주제는 크게 산업기술 유출방지를 위한 법·제도 개선, 기술유출 방지를 위한 보안시스템 구축방안, 산업기술 유출방지를 위한 인력 관리에 관한 연구, 중소기업 기술유출 방지를 위한 대응방안, 내부정보 유출방지의 관리적 대책 방안 등으로 나누어볼 수 있다.

국내 연구 중 대표적 연구들을 살펴보면 다음과 같다.

먼저, 최응렬 외 (2012)는 전문가들을 대상으로 산업기술 유출경로에 대해 조사하였다. 그 결과 내부 구성원들의 유출 방법은 휴대폰, 이동식 저장매체, 이메일 등으로 나타났다. 외부에서는 재고용, 기업간 M&A, 해킹 등이라고 밝히고 있다. 이희선(2012)은 기술유출범죄에 대하여 이론적으로 고찰해 보고 우리나라의 기술유출범죄의 실태와 문제점을 분석하여 기술유출범죄에 효과적으로 대응하기 위해 기술유출범죄에 대한 법·제도적 장치의 마련, 산업보안에 대한 인식의 제고, 보안관리 감독체계의 구축을 제시하고 있다. 김성준·김우현·이영석(2011)은 국가핵심기술의 유출이 우려되는 외국인 투자가 증가하고 있지만 규제를 다루는 법들은 미비함에 문제인식을 가지고 해외기업이 국가핵심기술을 보유한 국내기업을 대상으로 기술유출을 목적으로 한 적대적 M&A를 통해 인수하거나 합작투자로 핵심기술을 유출하는 경우에 이를 효과적으로 규율할 수 있는 방안을 모색하였다. 김순석·신제철(2010)은 산업기술 유출방지를 위한 핵심인력 관리방안에 관한 연구를 통하여 핵심인력 유출을 방지하기 위한 대책을 마련하였다. 구체적인 대책으로는 핵심인재에 대한 차별화된 처우와 보장, 감독을 실시해야 하며, 핵심인력이 다시 돌아올 경우 인사상 불이익이 가해지지 않는 방안 등을 제시하고 있다. 김민배·김경준(2007)은 핵심 산업기술의 유출에 의한 국가산업의 붕괴를 방지하고, 국민의 생존권 확보를 위해서는 산업기술 유출과 관련된 법적 장치와 그 대책 마련이

시급하다는 문제 인식을 가지고 연구를 진행하였다. 그 결과 국가핵심기술 등의 해외유출이나 산업기술의 부정확한 유출의 방지가 필요함을 제시하고, 이를 통해 핵심 산업기술의 유출방지를 위한 제도적 차원의 지원과 법적 미비점을 개선할 필요성이 있다고 언급하고 있다.

위에서 살펴본 바와 같이 산업기술 유출에 관한 다양한 연구 주제 중 인적 구성원에 의한 기술 유출에 관한 연구는 다수 이루어졌지만 외부적 요인, 특히 외국인 출입국자에 의한 산업기술 유출 대응방안을 점검하는 연구는 미미한 실정이다.

### III. 외국인 출입국자에 의한 산업기술유출 대응방안의 문제점

#### 1. 출입국시스템 운영의 비일관적 행태

우리나라의 출입국자 중 국민과 외국인의 구성비는 2011년 기준 국민 57.4%, 외국인 42.6%이며, 2010년 대비 출입국자는 국민은 28.7% 감소한 반면, 외국인은 거의 비슷한 수준을 유지하고 있는 것으로 나타났다(법무부 출입국·외국인정책본부, 2012: 4-5). 교통수단의 발달과 국가별로 다양한 방문목적 발생 그리고 글로벌 시대를 맞이하여 다른 국가들과의 민족적, 종교적, 문화적 인식차이를 넘나들고 있기에 앞으로 외국인의 출입국자는 더욱 증가할 것으로 예상된다.

최근 각국에서는 외국인에 의해 자국에서 발생가능한 테러 및 주요 범죄를 사전에 차단하기 위하여 공·항만 검색을 강화하고, 엄격한 검색 절차를 받도록 했으며, 출입국하는 항공기의 탑승자와 수하물 보안검색 및 기내 행동규정을 크게 강화하고 있는 추세이다. 이와 관련하여 전 세계적으로 신속하게 위험물품을 탐지할 수 있는 전신검색기를 도입하여 운영 중이고, 한국도 인천공항, 김포공항 등 주요 국제공항에서도 최신 항공보안 검색장비를 설치·운영하고 있다(권정훈, 2011: 220-221).

하지만 산업기술 유출과 관련해서는 물적 도구의 검색하는 시스템만으로는 사전에 예방하기는 상당히 어렵다. 그 이유는 산업기술을 유출하기 위한 실질적인 도구나 기기는 누구나 휴대하기 편리한 소형물품일 가능성이 높기 때문이다. 따라서 국내에서는 신분제타를 통한 불법 입국 기도자, 국익 침해자의 입국을 차단하고, 범법외국인을 추적·조사할 수 있는 외국인 신원관리시스템의 필요성이 제기되었고, 2010년 8월 15일부터 외국인 지문제공을 의무화하는 내용으로 「출입국관리법」을 개정·시행하고 있다.<sup>6)</sup>

외국인 지문제공 시스템은 3단계로 진행되었으며 2012년 1월 1일부터 3단계(전면 시행)가 시행 중이다. 이는 우리나라에 입국하는 17세 이상의 모든 외국인은 우리 당국

6) 미국은 2004년부터, 일본은 2007년부터 각각 입국하는 외국인을 상대로 지문확인제도를 시행하고 있으며, 영국과 프랑스·독일 등 EU 국가는 비자 발급이나 외국인등록 시 지문 및 얼굴 정보를 확인하고 있음(법무부, 2011: 1-2).

에 지문과 얼굴정보를 제공해야 하는 것을 골자로 하는 것으로 이 때 얼굴사진 촬영도 함께 이뤄진다.<sup>7)</sup> 다만, 17세 미만자, 외교관이나 중앙행정기관의 장이 면제를 요청한 사람 등은 제외된다.<sup>8)</sup> 지문확인 대상은 국제테러범과 인적사항이 유사하거나 인터폴 등에 분실 신고된 여권을 소지한 자, 여행경로가 특이하거나 출발 당일 현금으로 편도 항공권만 구매한 자, 위·변조 여권이나 위명여권 소지 등 신분세탁이 의심되는 자, 국적국의 언어를 구사하지 못하거나 국적국 사정에 어두운 자, 입국심사관의 질문에 불응하거나 거동이 수상한 자 등이다(법무부, 2011: 1-3).

하지만 출입국시스템 운영의 비일관적 행태에 대해서는 우려가 되는 것이 사실이다. 즉, 출입국시스템의 선진화와 불법입국 방지 및 외국인 신원관리 강화를 위하여 상기 규정과 같이 외국인 신원정보 확보의 필요성에는 공감을 하지만, 외국인 입국시 지문날인제도가 법·제도적 일관성을 갖고 운영될 것인지에 대한 의문이 그것이다.

실제로 법무부가 밝힌 2010년 입법취지는 불법입국의 외국인 신원관리시스템 구축을 통한 범질서 확립이지만, 「출입국관리법」이 2003년 12월 31일에 일부개정되기 전까지 이미 시행되고 있던 외국인 입국 시 지문날인제도를 외국인들에 대한 인권침해 우려로 인하여 폐지되었던 사례가 있다.

## 2. 외국인 지문인식시스템 활용의 한계

지문인식시스템이 도입된다고 해서 외국인 출입국자에 의한 기술유출 차단 가능성을 다음과 같은 이유로 전적으로 신뢰할 수는 없다.

첫째, 지문의 위조 가능성이 존재한다. 실제로 2010년에 지문인식시스템을 먼저 도입한 일본에서 실리콘 인조지문 등으로 검색대를 빠져나간 사례가 발생하였다.<sup>9)</sup>

둘째, 지문인식기술의 오차율이 문제될 수 있다. 대부분의 국가에서 채택하고 있는

7) 1단계로 2010년 9월부터 입국하는 외국인 중 신분세탁자, 국제테러분자 등으로 의심되는 외국인에 대해 선별적으로 우선 시행하였고, 2단계로 2011년 7월부터는 90일 초과 장기체류외국인(등록외국인)을 대상으로 지문 및 얼굴정보를 제공받고 있으며, 3단계는 시행(전면 시행)에 대비하여 2011년 12월부터 인천공항, 김포·김해공항 등 전국 주요 공항만 사무소의 입국심사대 구조개선 및 우수한 성능을 가진 최첨단 지문인식기 360대를 설치하여 시범 운영하였다.

8) 「출입국관리법」 제12조의2 (입국 시 지문 및 얼굴에 관한 정보의 제공 등)

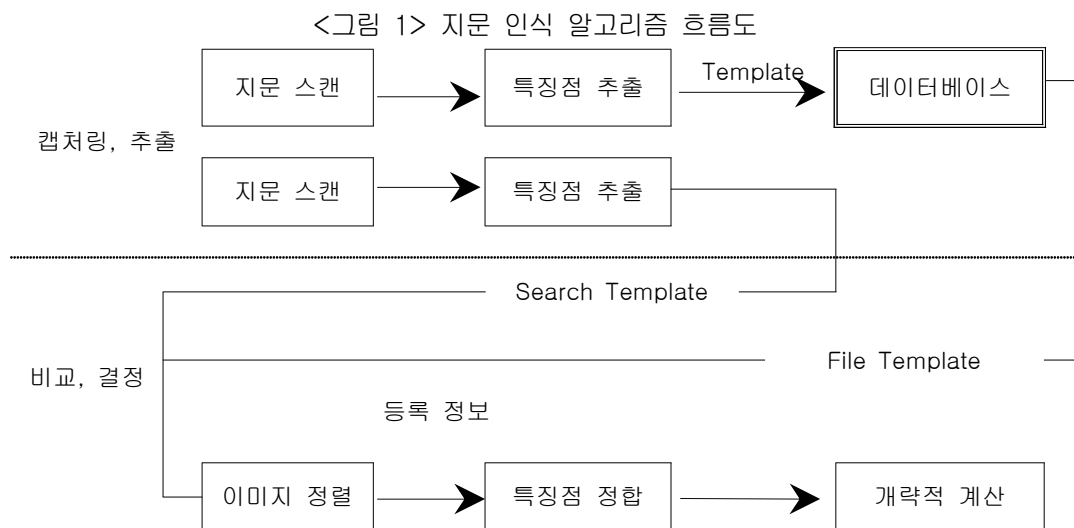
① 입국하려는 외국인은 제12조에 따라 입국심사를 받을 때 법무부령으로 정하는 방법으로 지문 및 얼굴에 관한 정보를 제공하고 본인임을 확인하는 절차에 응하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 사람은 그러하지 아니하다.

1. 17세 미만인 사람
2. 외국정부 또는 국제기구의 업무를 수행하기 위하여 입국하는 사람과 그 동반 가족
3. 외국과의 우호 및 문화교류 증진, 경제활동 촉진 또는 대한민국의 이익 등을 고려하여 지문 및 얼굴에 관한 정보의 제공을 면제하는 것이 필요하다고 대통령령으로 정하는 사람

9) 2010년 5월 6일 서울지방경찰청 국제범죄수사대에 붙잡힌 위조기술자 최모(43)씨는 1,200만~1,500만원씩 받고 타인의 지문이 새겨진 실리콘 지문을 제작해서 2007년 지문인식을 도입한 일본 입국심사를 통과할 수 있도록 해준 사례가 있다( <http://news.hankooki.com/>, 검색일: 2013. 4. 10).

두 손가락 지문확인방식의 오차율은 1% 내외로 알려져 있다. 한해 수 천만명 이상이 출입국하는 우리나라의 실태에 비춰보면 적은 수치만은 아님을 알 수 있다. 실제로 몇 년 전 미국에선 테러범의 지문을 추적한 결과 테러범이 아닌 미 해병의 지문과 동일하다는 잘못된 결과가 나온 사건도 있었다.

이처럼 지문인식이 틀릴 수 있는 이유는 <그림 1>과 같이 지문의 동일성을 판단하는 방식 때문이다. 한 손가락의 지문에는 사람마다 다른 특징점(Minutia)이 50~100개 존재한다. 그 중 특징점이 12개 이상 같으면 동일인이라고 보통 판단한다. 이를 디지털로 변환해 판독할 경우 개략적인 계산(Probability Calculation) 결과를 도출하게 되는데 이 때 미세한 차이를 분간하기 힘들어지는 문제가 발생하기도 한다(반성범 외, 2001: 47-54; <http://news.hankooki.com>, 검색일: 2013. 4. 10).



자료: 반성범 외, 2010: 49.

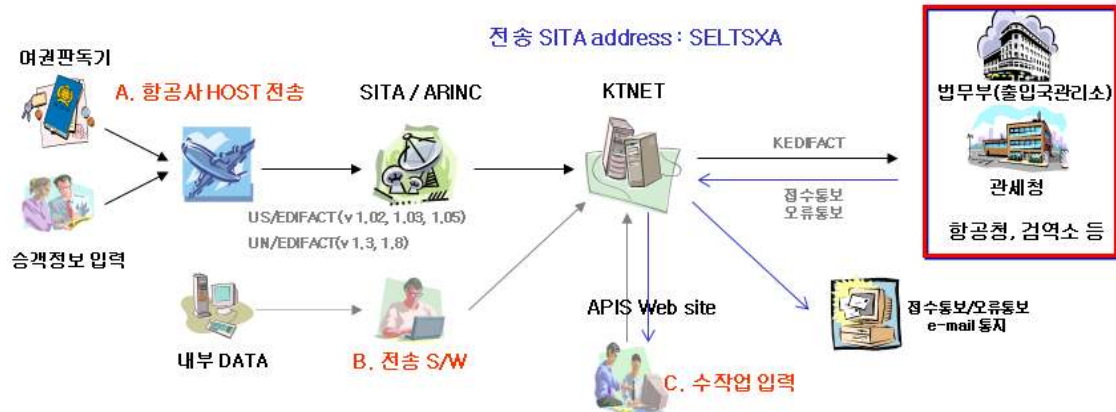
### 3. APIS 정보 활용상의 문제점

전 세계적으로 초국가적 범죄의 위험성이 증대됨에 따라 정보기술의 업그레이드, 국경관리기관간 상호협력 강화, 각국 세관당국과 타 국경관리기관간 국제협력 강화, 국경관리기관과 항공사간 협력 강화 등 안전한 국경관리를 위한 다각적인 노력들을 펼쳐왔다.

이러한 환경적·시대적 요구에 따라 국경관리 임무를 수행하고 있는 세관 등 국경관리당국은 인력에 의한 고위험 우범자 색출에 한계가 있다는 점에 인식을 같이하고 과학적 시스템에 의한 정보분석을 통해 사회안전을 위협하는 우범자를 정확히 선별해내기 위한 방안을 고민하게 되었다. 그 방안의 일환으로 우리나라는 2001년 3월 인천국제공항 개항에 맞추어 사전 승객정보 분석시스템(APIS: Advance Passenger

Information System)을 최초로 도입하게 되었고, 이후 <그림 2>와 같이 관세청과 법무부의 전산시스템이 연계·구축되어 설치·운영되고 있다.

<그림 2> APIS 체계도



자료: 한국무역정보통신, 2005: 5.

문제는 기타 주요 기관과의 정보 연계문제이다. 현재 법무부(출입국관리사무소)에서는 항공사로부터 제공받은 사전승객정보분석시스템(APIS) 정보를 분석 탑승객 가운데 수배, 테러혐의 등 사유로 입국시 통보 요청된 자 등을 색출한 후 특정해서 당해 탑승 항공기가 국내공항에 도착하기 전에 경찰청, 국가정보원 등 유관기관에 통보해 주고 있다.

하지만 이러한 정보를 통보해 주는 것이 재량사항일 뿐 의무사항은 아니라는 점이 가장 큰 문제이다. 이러한 통보문제가 특히 수배 등의 사유로 입국시 통보 요청된 피의자의 신병을 확보하는데 있어 매우 중요한 사항인데도 단지 재량에 의해 통보 여부를 결정하도록 하는 것은 수사의 비효율성 문제는 물론 경우에 따라서는 타 기관 불신의 문제로 비화될 수도 있다.

#### IV. 외국인 출입국자에 의한 산업기술유출 방지를 위한 효과적인 대응방안

##### 1. 출입국시스템 운영의 일관성 유지

실제로 법무부가 밝힌 2010년 입법취지는 불법입국의 외국인 신원관리시스템 구축을 통한 법질서 확립이지만, 「출입국관리법」이 2003년 12월 31일에 일부개정되기 전까지 이미 시행되고 있던 외국인 입국 시 지문날인제도를 외국인들에 대한 인권침해 우려로 인하여 폐지되었던 사례가 있다.

이러한 우려는 「출입국관리법」의 제정 및 개정과정을 살펴보면 더욱 명확해진다. 즉, 1963년에 「출입국관리법」이 제정된 이래, 산업발전과 국제화 추세에 따라 출입국자가 급증하고, 외국인 불법취업자가 계속 증가되고 있는 등 체류외국인의 활동이 복잡·다양화되고 있는 현실을 반영하기 위하여 제38조(지문찍기) 조항을 신설하는 등 기존 규정상의 미비점을 보완하려는 의도로 1992년 12월 8일에 전문개정이 이루어졌다.

이후 2003년 12월 31일에 일부개정 시 체류외국인의 편의를 증진하고 국가 이미지를 제고하기 위하여 1년 이상 체류하는 20세 이상의 외국인으로서 외국인등록을 하는 자에 대한 지문찍기를 폐지하였고, 2010년 개정·시행에 이르고 있다.

하지만 오늘날 국내외의 주요 정책을 살펴보면, 국가이미지 제고도 중요하지만 국가안보를 최우선시하고 있음을 알 수 있다. 따라서 이에 관하여 명확하게 입장을 견지하여 현재 시행되는 제도가 일관성있게 추진되어 외국인 출입국자에 의한 산업기술 유출 방지에 있어서도 효과적으로 대응해야 할 것이다.

## 2. 지문인식시스템의 보완

지문인식시스템의 몇 가지 한계점을 보완하기 위해서는 생체인식과 관련된 보완 시스템에 대한 검토가 요구된다.

현재 전 세계적으로 생체인식 기술을 활용한 대표적인 기술 분야는 <표 8>과 같이 단연 지문인식 방법이 가장 보편적이나, 얼굴인식과 홍채인식 등 다양한 방법과 분야에서 첨단기술들이 개발되고 있다. 현재 출입국 보안·검색과 관련되어 활용되고 있는 기술들은 지문, 얼굴 인식이 활용되고 있으나 산업스파이, 테러리스트와 같이 국가안보를 위협하는 의심 외국인들은 더욱 정확도가 높은 홍채, 목소리, 서명 등과 같은 차별적인 기술분야를 활용할 필요가 있다.

<표 8> 기술분야별 시장점유율 현황

(단위: %)

기술분야	AFIS (Live-Scan)	지문	얼굴	미들 웨어	손	홍채	목소리	서명	정맥	기타
2004년	-	48.0	12.0	12.0	11.0	9.0	6.0	2.0	-	-
2009년	38.3	28.4	11.4	8.0	1.8	5.1	3.0	-	2.4	1.6

자료: Holmes & Walmsley, 2005: 29; <https://ibgweb.com/> (검색일: 2013. 4. 15).

또한 향후에는 단편적인 기술분야의 접근보다는 지문인식과 얼굴인식, 화자인식과 얼굴인식과 지문인식, 홍채인식과 얼굴인식 등과 같이 각각의 독립적인 생체인식 기술을 융합해서 사용하는 다중 생체 인식시스템이 활용되어야 할 것이다. 물론 현재로 지문인식과 얼굴인식과 같은 방법들은 병행해서 활용되고 있지만, 방법들간 장단점이 존재하므로 외국에서 출입국한 산업스파이를 검거하기 위해 적합한 생체인식 기술 조합

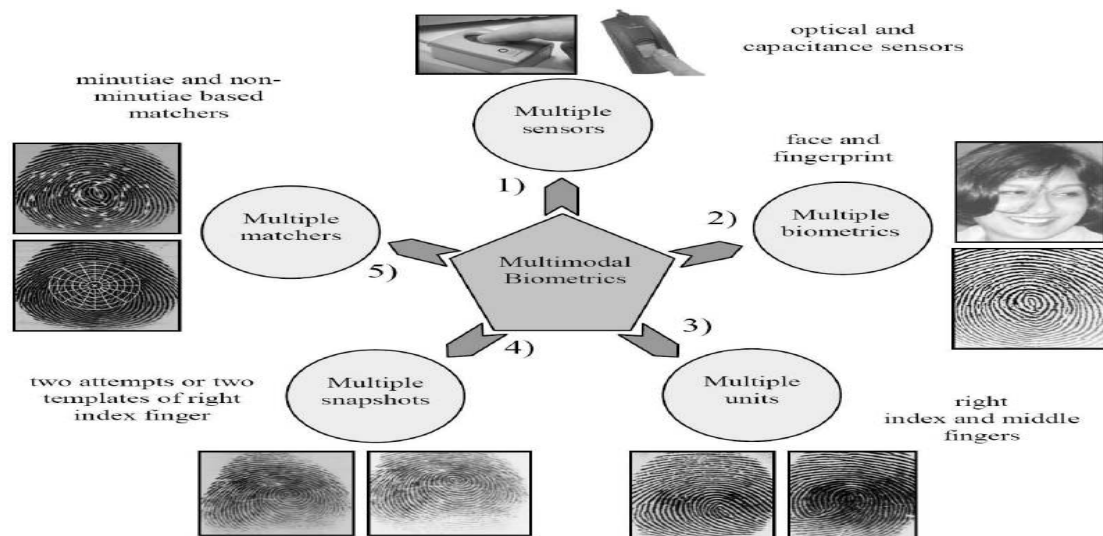
이 개발되어야 할 것이다.

다중생체인식 시스템은 다음 세 가지의 필요성에 의해서 각광받고 있다. 첫 번째는 신뢰성 향상 측면으로 두 가지 이상의 생체인식기술을 사용함으로써 매칭의 신뢰성을 높일 수 있어 단일인식 시스템으로 발생가능한 오류를 보완할 수 있게 된다. 두 번째는 인식성능의 향상을 위해서 다중 생체인식이 필요하다. 생체인식 기술이 고도의 보안을 요하는 분야에 적용되기 위해서는 정확도가 매우 높아야 한다. 하지만 시스템이 가동되는 과정상에서 발생가능한 방법상의 한계로 인해 완벽한 인식 성능을 가진 생체인식 시스템을 구현하기는 어렵다. 따라서 두 가지 이상의 생체인식 기법을 사용함으로써 상호보완적인 인식률의 향상을 기대할 수 있다. 세 번째는 기능향상을 위함이다. 예를 들어 얼굴인식의 경우를 살펴보면, 얼굴인식은 빠르고 편리하다는 장점이 있는 반면에 쌍둥이와 같은 경우에는 인식하기가 어렵다는 한계와 본인 스스로의 얼굴변화, 다시 말해서 수염이나 헤어스타일의 변화, 장신구에 의한 얼굴의 변화에 취약하다는 단점이 있다. 반면, 지문인식은 얼굴인식보다 인식률이 좋다는 장점이 있지만, 처리속도가 상대적으로 느리고 사용자가 지문입력기에 직접 손을 접촉해야 하기 때문에 약간의 거부감을 느끼게 되는 단점이 있다. 그러나 얼굴인식과 지문인식의 다중 생체인식 시스템을 사용함으로써 이런 기능적인 면을 향상시킬 수 있다(김재희, 2001: 82-83).

<그림 3>은 이러한 다중 생체인식 시스템을 구조화시킨 것으로 크게 네 가지로 구분하여 설명할 수 있다. 첫 번째는 다중센서(Multiple sensor)다. 다중센서는 하나의 생체 특징을 여러 가지 센서로 인식하는 것으로 지문인식을 할 때 광학적·전기적 센서 등의 인식방법을 함께 쓰기도 한다. 두 번째는 다중 생체특징(Multiple biometrics)이다. 이는 여러 가지 생체인식시스템을 함께 사용하는 것으로 지문과 얼굴 인식시스템을 하나로 묶어 활용하는 것을 예로 들 수 있다. 세 번째는 다중 유닛(Multiple units)이다. 이는 하나의 생체인식 시스템이 여러 가지 생체를 인식하는 것이다. 생체는 같은 부분에 여러 가지 특징이 있기 마련이다. 지문인식 시스템을 사용할 때 열 손가락을 모두 인식하거나 홍채인식 시스템에서 양쪽 눈의 홍채를 모두 입력해야 하는 것, 장문인식에서 양손을 사용하는 방법 등이 있다. 네 번째는 다중 획득(Multiple instances)이다. 다중 획득은 하나의 생체 특징을 여러 번 인식시키는 방법(Multiple matchers, Multiple snapshots)으로 인식 수를 늘려 정확도와 신뢰도를 높이게 된다.

그러나 생체인식 기법은 기술의 특성상 개인의 신체적 특징을 사용하는 관계로 신체의 자유에 해당하는 프라이버시 침해요인과 자신의 동의 없이 자신의 생체정보가 취득되어 자신을 감시하는 목적으로 사용될 수 있다는 부정적인 견해가 상존하고 있으므로 신중하게 접근되어야 할 필요성은 있다.

&lt;그림 3&gt; 다중 생체인식 시스템(Multimodal Biometric Systems)



자료: Ross & Jain, 2004: 1221-1224.

### 3. 통합 신원정보 공유시스템 구축

외국인 출입국자에 의한 산업기술 유출을 막기 위한 가장 좋은 방법은 입출국시 신속한 신원확인일 것이다. 어떤 범죄보다도 시공간적 제약을 적게 받는 범죄임을 감안할 때 신속한 신원확인은 산업스파이 검거에 있어 매우 중요하다.

신속한 신원확인은 일선의 출입국관리사무소와 같은 신원자료 수집기관을 통한 광범위한 외국인 신원자료의 확보, 경찰 등 신원확인 수요기관에 의한 원활한 정보검색 및 활용을 통해서만 가능하다. 게다가 만일 신원확인절차의 복잡성이나 관리시스템의 기술적 한계로 말미암아 신원을 확인하는데 많은 시간이 소요된다면, 첫째, 외국인 산업스파이가 출국을 하지 않더라도 컴퓨터 등 각종 첨단매체를 이용한 유출이 가능할 것이고, 둘째, 기술유출이 되었더라도 출국과정에서 기술유출과 관련된 산업스파이들을 검거하지 못하여 범죄집단의 인적 네트워크 역시 파악하지 못하는 최악의 결과를 낳게 된다. 따라서 신속·정확한 신원확인 시스템의 구축이 반드시 필요하다.

현재, 국내 체계를 살펴보면 신속하게 신원을 확인하는 것과 관련 유관기관으로 정보 공유의 유기적인 연계는 미약하다고 볼 수 있다. 이를 극복하기 위한 방편으로 2012년 법무부와 경찰은 2011년 9월부터 수집한 입국·체류 외국인들의 지문정보를 수사에 활용하기 위한 특별전문위원회를 구성하고 시스템을 통합하기 위한 방안 마련에 나섰다. 만약 경찰이 지문정보 데이터베이스에 직접 연결해 지문정보를 활용할 경우 24시간 내내 언제나 신원을 확인할 수 있어 초동수사에 많은 도움을 받을 수 있다.

하지만 기관별로 사용하는 시스템이 달라 법무부의 지문정보 데이터베이스를 경찰에



연결해도 경찰이 이를 직접 활용할 수 없어 통합적인 시스템 구축에는 일정 시간이 소요될 것으로 여겨진다. 물론 다른 기관간의 네트워크 특성으로 인하여 기관간 시스템 통합이 쉬운 문제는 아니겠지만 산업스파이와 같은 국제적인 범죄를 사전에 예방하고 분석하는 자료를 보유하고, 외국인에 의한 범죄와 기술유출 범죄의 증가세가 뚜렷해지는 상황에서 치안공백을 최소화하기 위해서라도 신속한 대처가 요구된다.

그리고 시스템의 통합과 더불어 사전 승객정보 분석시스템(APIS) 정보수집이 당장 어렵다면, 현재 법무부(출입국관리사무소)에서는 재량사항으로 경찰청, 국가정보원 등 유관기관에 통보해 주고 있는 체계를 주요 수사기관에서 요청하면 법무부나 항공사에서 이를 즉시 제공하도록 하는 의무규정을 제정할 필요가 있다(박기륜, 2007: 153-154).

## V. 결론

이 연구는 산업기밀 유출의 주체에 관한 것이다. 하지만 기존 연구와는 달리 외국인 출입국자에 의한 산업기밀 유출에 중점을 두고 논의를 전개하였다. 즉, 기존의 연구는 산업기술 유출이 주로 전·현직 직원에 의한 것이 대부분임을 주지하고 그에 대한 대응방안을 마련하였다면, 이 연구는 미국에서 산업기술 유출의 주된 주체가 단기 출입국하는 외국인 사업가, 과학자, 기술자, 학생 그리고 학자들이라는 결과에 주목하고 국내 실태는 어떠한지, 문제점은 무엇인지에 대하여 고민해 보았다.

이러한 과정에서 먼저, 외국인들이 국내에 첫 발을 내딛는 출입국시스템에 관심을 가졌고, 관련 기관간에 업무를 진행함에 있어 협조·공유 정도는 어떠한지 살펴보았는데 그 구체적 내용은 다음과 같다.

첫째, 출입국시스템 운영의 일관성을 유지해야 한다. 이는 국내에서는 신분제택을 통한 불법입국 기도자, 국익 위해자의 입국을 차단하고, 범법외국인을 추적·조사할 수 있는 외국인 신원관리시스템의 필요성이 제기되었고, 2010년부터 외국인 지문제공을 의무화하는 내용으로 「출입국관리법」을 개정·시행하고 있다. 하지만 「출입국관리법」이 2003년 12월 31일에 일부개정되기 전까지 시행되고 있던 외국인 입국 시 지문날인 제도를 외국인들에 대한 인권침해 우려로 인하여 폐지되었던 사례가 있다. 외국인의 인권과 국내 안보사이에서 명확한 잣대없이 개정, 재개정을 반복하는 것은 분명한 국가적 낭비이다. 결국 제도 도입 여부에 대한 정책적 판단은 외국인 개개인의 인권보장이라는 소극적 가치와 국가안보나 자국민보호 나아가 절차의 간소화·합리화에 따른 편익증대라는 적극적 가치 상호간의 비교형량의 문제라고 한다면, 그 결과는 마땅히 보다 중대하고 보다 공익적인 성격이 강한 후자의 가치를 우선시해야 할 것이다.

둘째, 지문인식시스템 보완의 필요성이다. 지문인식시스템이 국내에 출입국하는 외국인의 신상정보를 검색하고 보유하는데 효율적인 방법 중의 하나이지만 그 결과를 100% 신뢰할 수는 없다. 그 이유는 지문의 위조 가능성과 지문인식기술의 오차율 때문

인데 이 부분을 보완하기 위하여 지문인식 외에 개발되어 있는 다양한 생체 인식시스템을 검토하는 것이 필요하다. 또한 향후에는 단편적인 기술분야의 접근보다는 지문인식과 얼굴인식, 화자인식과 얼굴인식과 지문인식, 홍채인식과 얼굴인식 등과 같이 각각의 독립적인 생체인식 기술을 융합해서 사용하는 다중생체인식시스템이 활용되어야 할 것이다. 물론 현재로 지문인식 및 얼굴인식과 같은 방법들은 병행해서 활용되고 있지만, 방법들간 장단점이 존재하므로 외국에서 출입국한 산업스파이를 검거하기 위해 적합한 생체인식 기술 조합이 개발되어야 할 것이다. 그러나 생체인식 기법은 프라이버시 침해요인과 자신의 동의 없이 자신의 생체정보가 취득되어 자신을 감시하는 목적으로 사용될 수 있다는 점에서 신중하게 접근되어야 할 필요성은 있다.

세 번째는 통합 신원정보 공유시스템의 구축이다. 외국인 출입국자에 의한 산업기술 유출을 막기 위한 가장 좋은 방법은 입출국시 신속한 신원확인일 것이다. 어떤 범죄보다도 시공간적 제약을 적게 받는 범죄임을 감안할 때 신속한 신원확인은 산업스파이 검거에 있어 매우 중요하다. 이는 관계기관 간 신속한 정보공유를 통해 가능한 부분으로 각 기관간 공유가 가능한 시스템을 구축하는 것이 선행되어야 한다. 또한 공유시스템 구축 시까지 발생하는 치안의 공백기간에는 현재 법무부(출입국관리사무소)에서 재량사항으로 경찰청, 국가정보원 등 유관기관에 통보해 주고 있는 체계를 주요 수사기관에서 요청하면 법무부나 항공사에서 이를 즉시 제공하도록 하는 의무규정을 제정할 필요성에 대해서도 논의해 보아야 한다.

다만, 이러한 제도적 개선은 필연적으로 인권침해의 문제와 항상 맞닿아 있음을 부인할 수 없다. 이 연구가 산업기술유출의 대응방안 마련에 중점을 두고 전개하고 있어 신원자료의 오·남용이나 관련정보의 대외유출 등 인권침해의 소지가 있다는 점은 구체적으로 다루고 있지 않다. 이와 관련된 부분은 후속 연구를 통해 보완하고자 한다.

## 참 고 문 헌

### 국내문헌

- 경찰청. (2012), 「경찰백서」.
- 권정훈. (2011), “독일의 정보 수집 관련 테러대응 법제와 한국의 방향”, 「한국치안행정논집」, 8(3): 205-226.
- 김민배·김경준. (2007), “산업기술의 유출방지 및 보호에 관한 법률과 쟁점”, 「산업재산권」, 23: 1-36.
- 김성준·김우현·이영석. (2011), “해외 M&A시 산업기술 유출 방지를 위한 법 개선 연구”, 「한국경호경비학회지」, 29: 7-34.
- 김순석·신제철. (2010), “산업기술 유출방지를 위한 핵심인력 관리방안에 관한 연구”, 「한국경호경비학회지」, 25: 109-130.
- 김재희. (2001), “생체인식의 최후 관문: 다중 생체인식 시스템”, 「시큐리티월드」, 82-83.
- 박기륜. (2007), “외국인 신원확인 시스템의 문제점과 개선방안”, 「한국경찰학회보」, 14: 133-159.
- 반성범·문지현·정용화·김학일. (2001), “지문 인식 기술 동향”, 「전자통신동향분석」, 16(5): 47-54.
- 법무부. (2011), “새로운 입국심사 시스템 도입으로 안전한 국경관리 시대 열어”, 「법무부 보도자료」.
- 법무부 출입국·외국인정책본부. (2012), 「2011 출입국 외국인정책 통계연보」.
- 산업통상자원부. (2007), 「산업기술의 유출방지 및 보호에 관한 기본계획(안)」.
- 이창한. (2010), “국내체류 외국인의 국제범죄 개입유형 및 대응방안”, 「한국공안행정학회보」, 39: 281.
- 이희선. (2012), “기술유출범죄의 실태분석 및 대응방안에 관한 연구”, 「한국민간경비학회보」, 11(2): 283-301.
- 최응렬·송봉규·이영일·박경민. (2012), “산업기술 유출경로 연구”, 「치안정책연구」, 26(1): 225-259.
- 한국무역정보통신. (2005), 「APIS 사용설명서」.

### 국외문헌

- Crane Andrew. (2005), “In the company of spies: When competitive intelligence gathering becomes industrial espionage”, *Business Horizons*, 48: 233-240.
- Chang-Moo, Lee. (2013), “Industrial Espionage and Police Investigation”, *International Journal of Security and its Applications*, 7(1): 155-162.
- Holmes, Chad & Walmsley, Shaun. (2005), “Biometric Security in Today’s Market: An introduction to fingerprint, retinal, and iris scanning technologies”, *Frontiers in Information Technology*, 1-35.

- Jennings, Karen. (1987), "Espionage: Anything Goes?", *Pepperdine Law Review*, 14(3): 647-666.
- National Counterintelligence Center. (2006), *2005 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*.
- Ross, Arun & Jain, Anil K.. (2004), Multimodal Biometrics: An Overview, *Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO)*, 1221-1224.
- Prabhakar, S. & Jain, A. K. (2002), "Decision-level fusion in fingerprint verification", *Pattern Recognition*, 35(4): 861-874.
- U.S. Department of Homeland Security. (2012), *Nonimmigrant Admissions to the United States: 2011, Annual Flow Report*.
- Zuev, Y. & Ivanon, S. (1996), The voting as a way to increase the decision reliability, in *Foundations of Information / Decision Fusion with Applications to Engineering Problems*, 206-210, Washington, D.C.: Government Printing Office.

#### 기타

- 국가법령정보센터, <http://www.law.go.kr/>.
- 로앤비, <http://www.lawnb.com/>.
- 산업기밀보호센터, <http://service4.nis.go.kr/>.
- 중앙일보, <http://article.joinsmsn.com/>.
- 한국일보, <http://news.hankooki.com/>.
- International Biometric Group, <https://ibgweb.com/>.

투고일자 : 2013. 05. 08  
수정일자 : 2013. 06. 10  
게재일자 : 2013. 06. 22

국문초록

## 외국인 산업스파이에 의한 산업기술유출 대응방안에 관한 연구 - 단기 출입국자를 중심으로 -

주성빈(동국대)·최응렬(동국대)

우리나라는 핵심기술 확보를 위해 지속적으로 노력하고 있고, 그 결과 2012년 1월 30일 기준, 전기전자 8건, 자동차 8건, 철강 6건, 조선 7건, 원자력 4건, 정보통신 17건, 우주 5건, 생명공학 3건 등 전체 58건의 분야별 국가핵심기술을 국가에서 지정·관리하고 있다.

하지만 이러한 기술적 성장은 기술유출범죄에 의한 피해가 매년 증가하고 있는 원인이 되고 있으며, 이는 막대한 국가적 피해를 초래하는 결과로 이어지고 있다.

현재 기술유출의 주체는 주로 전·현직 직원으로 알려져 있지만 앞으로는 국내 산업기밀을 유출할 계획을 치밀하게 준비하고 입국한 외국인들에 의한 피해도 점차 증가할 것으로 예상된다.

이 연구에서는 기술유출범죄에 대한 실태를 살펴보고, 우리나라에 출입국하는 외국인에 의한 기술유출범죄를 대응함에 있어 예상되는 문제점을 분석하였다. 이러한 문제점을 토대로 이들에 의한 기술유출범죄에 효과적으로 대응하기 위한 방안들에 대하여 살펴보았다.

구체적인 대응방안으로는 첫째, 출입국시스템 운영의 일관성을 유지하고, 둘째, 지문인식시스템을 보완하는 것이며, 셋째, 통합 신원정보 공유시스템 구축 방안을 들 수 있다.

전통적인 범죄유형과는 달리 산업스파이에 의해 산업기밀이 유출된다면, 이후 범인을 체포하더라도 이미 유출된 유·무형의 산업기밀에 대한 피해회복은 거의 불가능하다. 이로 인하여 국가와 기업의 피해는 막대하기 때문에 기술유출범죄는 사후대응보다 사전에 예방하는 것이 기술유출범죄를 가장 효과적으로 대응하는 것이다.

따라서 출입국시스템, 통합시스템 구축 등은 무엇보다도 중요하다.

주제어: 외국인, 산업기술유출, 산업스파이, 비이민자, 사전 승객정보 분석시스템

