# 국내 포털 기사자료 분석을 통한 산업기술유출 사례와 산업보안 강화 방안 연구

양 현 정*, 이 창 무**

## 요 약

지식정보화 사회가 도래하면서 많은 국내기업이 핵심기술 및 지식재산 확보를 위해 기술개발에 많은 투자를 하고 있다. 하지만 적극적인 기술개발 투자에 비해 기업이 보유한 기술을 보호하기 위한 보안투자가 미흡한 결과 다수의 기업 및 연구소에서 기술유출 사건이 급격하게 증가하고 있다. 이러한 기술유출의 증가는 단순히 기업에 피해뿐만 아니라 국가 경제에도 직·간접적인 악영향을 미치고 있는 실정이다. 산업기술유출은 주로 전·현직 직원에 의해 이뤄지고 있지만, 이를 중점적으로 비교 분석한 연구는 많지 않다. 따라서 본 연구는 2014년부터 2016년 동안 발생한 산업기술유출 사례를 기술유출 피해기업의 유형, 회사 내 기술유출 주체자의 직위, 기술유출의 공범여부, 기술유출에 사용된 도구, 기술유출의 동기로 유형화하여 산업기술유출 실태를 파악하였다. 이러한 유형별 분석을 통해 산업기술유출의 패턴과 특징에 대해 조사하고 산업기술유출 방지를 위한 산업보안 증진 방안을 모색하였다.

# A Study on Industrial Technology Leakage and Effective Industrial Security Measures through analysis of domestic portal article data

Yang Hyun Jung*, Lee Chang Moo**

## ABSTRACT

In the knowledge-information society, many domestic companies put lots of investment in technical development to possess core technologies and intellectual property. However, in the results of passive investment in security to protect their technologies compared to the active investment in technical development, the technology leaks from many companies and research institutes are rapidly increasing. Such increase of technology leaks not only causes damage to companies, but also has harmful effects on national economy directly and indirectly. Even though it has been perceived that a lot of industrial technology leak crimes are committed by former/current workers of small and medium-sized businesses, it is hard to find researches that mainly compare and analyze them. Therefore, this study aimed to understand the actual status of industrial technology leaks by analyzing cases of industrial technology leaks from 2014 to 2016 based on the type of victimized companies, corporate internal leakers' positions, matter of complicity, tools used for technology leaks, and motivation for technology leaks. Through the analysis in each type, the patterns and characteristics of industrial technology leaks were researched, and also the exploratory research on industrial security for the prevention of industrial technology leaks was conducted.

**Key words : Industrial Security, Industrial Technology Leakage, Security Convergence, Case Analysis, Cross tabulation analysis**

접수일(2017년 3월 6일), 수정일(1차: 2017년 3월 23일), 게재확정일(2017년 3월 29일)

★ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터 육성지원사업의 연구결과로 수행되었음. (IITP-2017-2014-0-00636)

* 중앙대학교 대학원 융합보안학과 (주저자)

** 중앙대학교 산업보안학과 교수 (교신저자)

# 1. 서 론

현대 고도화사회에서 지식재산 및 기술의 중요성은 갈수록 높아지고 있다. 국내의 다양한 기업들이 첨단 기술을 보유하고 있으며 막대한 인력과 자금 및 시간을 기술개발에 투자하고 있지만, 기술유출에 대한 대응능력과 보안의식 그리고 투자는 비교적 부족한 실정이다. 때문에 산업기술 유출범죄는 계속 증가하고 있다. 이러한 산업기술 유출범죄는 기업에 직접적인 피해는 물론이고 국가 경제에도 많은 직·간접적인 악영향을 미친다. 많은 기업에서 기술유출에 대한 보안이나 대비가 매우 미비한 실정이며 중소기업의 경우 상황은 더욱 심각하다. 이로 인해 다수의 기술 유출 사건이 중소기업에서 발생하고 있다. 중소기업은 기업자체에서 보안역량을 자체적으로 향상시키기에는 한계가 있기 때문에 기술유출의 위험에 더 노출이 되어있다. 무엇보다 중소기업은 기술유출이 발생했을 때 체감적인 피해가 더 크고 회복이 어려운 점이 기업경영에 큰 악영향을 미치기 때문에 최악의 경우 해외 사업장을 철수하는 사태가 발생할 수도 있다. 이처럼 많은 중소기업을 포함해 기업 상당수는 기술보호에 대한 인식이 부족한 실정이며, 연구개발에 대한 투자에 비해 기술보호에 대한 관심과 예산 비중은 상대적으로 매우 낮은 상태이다.

산업기술유출은 외부의 스파이에 의한 유출보다 회사 내의 전·현직직원에 의해 발생하는 경우가 많다. 이는 기업의 내부자가 기술정보를 저장한 저장매체에 대한 접근이 용이하고, 기술정보를 쉽게 입수할 수 있는 인적 네트워크를 가지고 있기 때문이다. 또한 전·현직 직원은 보안구조의 허점 및 내부통제에 대한 정보 등에 대해 잘 알고 있기 때문에 기술유출을 보다 쉽게 시도할 수 있다.

그럼에도 불구하고 전·현직 직원 가운데 어떤 직위를 갖고 있는 직원들이 산업기술을 유출하는 지와 같은 구체적인 정보는 조사된 바 없다. 따라서 본 연구에서는 국내 산업기술유출 사례분석을 통해 내부자에 의한 산업기술유출의 방법, 동기 등을 파악하고 실질적인 해결방안을 제시하고자 한다. 이러한 분석을 통해 그간 제기되지 않았던 산업기술유출의 새로운 패턴이나 특징을 추가적으로 발굴함으로써 산업기술 유출 방지에 기여할 수 있을 것으로 보인다.

# 2. 이론적 배경

## 2.1 산업기술유출의 개념

산업기술유출이란 산업보안 분야의 한 부분이다[9]. 이러한 산업기술유출의 개념을 파악하기 위해서는 산업기술의 개념을 살펴보아야 한다. 산업기술은 용역 또는 제품의 개발·생산·사용 및 보급에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 소관 분야의 산업경쟁력 제고 등을 위하여 법률 또는 해당 법률에서 위임한 명령에 따라 지정·고시·공고·인증하는 기술을 의미한다[21]. 국가핵심기술을 비롯하여 건설기술, 뿌리기술, 첨단기술, 신기술 등이 여기에 해당된다. 또한 산업기술유출에서의 부정한 방법이란 산업기술을 취득해 공개하거나 사용하는데 협박, 절취, 기망 등의 수단을 사용하는 것을 말한다.

산업기술유출은 범죄학적인 관점에서 화이트칼라(White-Collar) 범죄로 볼 수 있다. Edwin Sutherland에 의하면 화이트칼라 범죄는 “사회적으로 존경받는 위치에 있는 사람이 자신의 직무와 관련해 저지르는 범죄”이다[22]. 화이트칼라범죄 연구의 권위자 중 한명인 Gilbert Geis 또한 화이트칼라 범죄의 핵심적인 요소가 ‘직권 남용’이라고 하면서 이러한 직권 남용의 기회를 가질 수 있는 직위의 사람들이 저지르는 범죄로 파악하였다(1992: 47). 따라서 현재 화이트칼라 범죄의 개념은 ‘자신의 직권을 이용해 직무와 관련한 범죄를 저지르는 것’으로 받아들여지고 있다[22].

## 2.2 일상활동이론

현재 산업기술유출 대부분은 철저하지 못한 보안시스템과 보안의식이 부족한 기업들을 중심으로 발생하고 있다. 또한 산업기술유출사건의 주체는 기술의 가치를 잘 알고 기술에 대한 접근권한이 용이한 전·현직 직원 이 다수를 차지하고 있다. 일상활동이론은 19

79년 Cohen과 Felson에 의해 주장되었으며, 그들은 특정한 개인 또는 대상의 범죄 발생과 피해는 그들만의 예측가능하고 반복되는 일상활동 또는 생활유형 패턴의 결과이자 시간·공간적 특성의 결과로 나타난다고 했다. 범죄발생의 세 가지 필수요건으로서 동기화된 범죄자, 적당한 목표물, 능력이 있는 보호자의 부재를 제시하고, 특정 범죄피해가 발생하기 위해서는 이 세 가지 요소가 모두 일정한 시·공간적으로 수렴되어야 한다고 주장하였다. 또한 범행대상과 잠재적인 범죄자 간의 물리적 근접성과 그 대상에 대한 접근가능성을 범죄피해를 결정하는 중요한 요소라고 보았다[22]. 즉, 일상활동이론은 범행대상으로서의 매력성이 클수록, 보호능력의 수준이 낮을수록, 범죄에 대한 노출이 높을수록, 잠재적 범죄와 근접할수록, 특정 범죄의 특성에 따라 범죄피해를 당할 가능성이 높아진다[12].

기업 내의 핵심기술, 보안이 필요한 정보 등이 매력적인 목표물로 범행대상으로 인식될 수 있으며 철저하지 못한 기업 내의 보안시스템과 관리는 능력이 있는 보호자의 부재로 인식될 수 있다. 또한 회사처우에 대한 불만, 경쟁업체의 스카우트 등 산업기술유출 동기는 잠재적인 범죄자로 하여금 동기부여를 통해 범죄자로 전환시킬 수 있는 기회를 제공한다. 이러한 일상활동이론 관점에서 산업기술유출을 예방하기 위해서는 매력적인 목표물인 기술을 제거하기 힘들기 때문에 동기화된 범죄자와 능력이 있는 보호자의 부재를 억제해야 한다고 판단된다. 즉, 산업기술유출은 범죄자의 범행 동기를 파악하여 그 동기를 낮추거나 억제하고, 산업기술유출의 목표가 될 만한 기술과 정보는 보안과 관리를 철저히 함으로써 범죄를 예방할 수 있다. 본 연구에서는 산업기술유출 사례분석을 통해 범행의 동기와 기술유출방법 등의 파악하여 산업기술유출 범죄의 예방법과 대응방안을 제시하고자 한다.

### 2.3 선행연구 및 독창성

이희선(2012)은 기술유출범죄를 범죄원인론적인 관점에서 살펴보고 국내의 기술유출범죄 실태와 문제점을 분석하였다[11]. 또한 국내의 기술유출범죄 실태와 문제점을 분석하여 기술유출범죄에 효과적으로 대응하기 위한 방안들에 대하여 살펴보았다. 이 연구에서는 기술유출 범죄에 대응하고 예방하기 위해서 현실적인 법 ·제도적 개정이 필요하다고 주장하였고, 기술유출범죄를 기업 내 문제가 아닌 국가 차원의 문제로 인식을 전환해야 한다고 강조했다. 그리고 기술유출범죄는 사후대응보다 사전에 예방하는 것이 중요하기 때문에 보안 관리의 감독체계 구축이 무엇보다 중요하다고 강조하고 있다.

김신혜, 박준석, 박길준(2013)은 산업기밀보호센터의 자료를 통해 국내 산업기술유출의 유형 및 실태를 분석하였으며, 국내에서 실시하고 있는 산업기술유출 방지를 위한 대응책에 대한 문제점을 분석하였다[3]. 그리고 이를 토대로 적절한 산업기술 유출방지를 위한 정책 개선방안을 제시하였다. 본 연구는 법률적 개선방안으로 기술유출자에 대한 법적제제강화 방안을 제시하였다. 또한 제도적 개선방안으로 산업보안의 조정기관의 신설에 대한 필요성을 제기하였다.

조호대(2012)는 산업스파이와 기술 유출에 대한 개념과 이론적인 근거를 살펴보고, 기술 유출 유형과 그 특성을 분석하고자 한다[17]. 또한 산업기술유출 사례를 검토하여 효과적인 대응방안을 제시하였다. 본 연구는 4건의 기술유출 사례를 분석하여 기술유출의 경로 및 특징을 살펴보고자 하였으며, 이를 토대로 기술유출 사전예방 프로그램 구비, 개별적 인원관리, 피해기업 구조시스템 구축 등의 대응방안을 제시하였다.

이준복(2014)은 산업기술유출 의의와 유형에 대해 살펴보고 각 유형별 산업기술유출 대응방안에 대해 모색하였다[8]. 산업기술유출 유형을 산업스파이에 의한 기술유출과 기업 M&A에 따른 기술유출로 구분하였으며, 각 유형별로 법적 관점의 대응방안을 제시하였다. 미국, 일본, 중국, EU 등의 법률적 현황을 토대로 다양한 산업기술보호의 법제도적 개선방향을 제시하였다.

박찬수(2013)는 현재 국내의 산업기술보호 현황 및 문제점을 살펴보고 국내 첨단기술의 보호를 위한 범국가적 대응을 위한 정책적 과제를 제시하였다[5]. 본 연구는 국내의 산업기술 보호의 문제점으로 실질적 기술보호제도 운영효과 미흡, 정부의 관리역량 미흡, 기업

의 유기적 관리체계 미비 등을 지적하였다. 이를 토대로 기술유출 대비 민·관 공동 대응체계를 구축하고 범국가적 대응을 위해 정부에서 중소기업의 기술보호 관련 정책을 지원 확대하고 보안산업을 미래 신산업으로 육성해야한다고 말하고 있다.

장항배(2015)는 국내외 산업기밀 유출범죄 분석을 통하여 산업기밀 유출에 따른 피해실태를 파악하고 다양한 분류체계를 통하여 산업기밀 유출범죄의 발생원인, 유출경로 등을 알아보고자 하였다[14]. 본 연구는 국가정부기관의 조사에 따른 데이터를 통해 산업기술유출의 심각성과 산업기술범죄에 대한 노력과 투자가 피해규모에 비해 부족한 점을 지적하고 이를 위해 피해실태를 파악하고 발생원인과 유출경로 등 유출범죄에 대한 전반적인 흐름을 파악하고자 했다. 이러한 산업기밀 유출범죄의 피해 실태 및 범죄 유형을 바탕으로 각 6가지 유형별 시사점 및 대응방안에 대해 제시하였다.

산업기술유출에 대한 선행연구를 조사 및 분석하였을 때 대부분의 연구는 산업기술유출 범죄에 대한 개념적 정의 및 실태를 파악하고 이를 토대로 산업기술유출 범죄의 유형을 분석하고자 하였다. 산업기술유출 실태분석의 경우 대부분의 연구가 국가정보원 산업기밀보호센터의 자료만을 토대로 분석을 실시하고, 산업기밀 유출범죄의 피해 실태 및 범죄 유형을 파악하고자 하였다. 그 결과 많은 연구들이 동일 자료만을 토대로 분석함에 따라 산업기술 유출범죄의 유형이 비슷하게 나타났다. 또한 이러한 유형을 토대로 산업기술유출 범죄의 대응방안을 제시함으로써, 산업기술유출의 직접적인 원인 분석을 통한 실질적인 대응방안 제시가 아닌 보안체계 구축, 법률 및 제도적 개선방안 등의 일반적인 대응책만을 제시하고 있었다. 이에 따라 본 연구에서는 실제 발생한 산업기술유출 사례분석을 통해 산업기술유출이 발생된 원인을 유형별로 분석하고 이를 통해 실효성 있는 예방법과 대응방안을 제시하는 것에 초점을 두고자 한다.

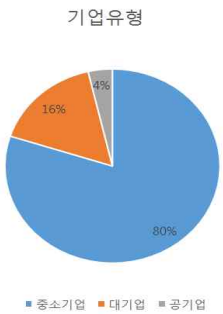
### 2.4 연구의 범위 및 방법

본 연구는 외부자에 의한 기술유출행위보다는 내부자에 의한 산업보안 사고에 초점을 맞추어서 산업기술유출의 현황을 파악하고자 한다. 연구 데이터는 산업기술유출 관련 뉴스를 토대로 효과적인 산업보안을 위한 예방대책과 해결방안을 도출하기 위하여 산업기술유출의 사례분석을 교차분석 방법을 통해 시도하였다. 사례분석을 위해 “네이버 뉴스”에서 2014년부터 2016년 사이에 “산업기술의 유출방지 및 보호에 관한 법률”과 “부정경쟁방지 및 영업비밀보호에 관한 법률”이란 키워드를 통해 검색된 산업기술유출 55건의 사건을 비교 분석 하였다. 네이버 뉴스를 통해 검색된 55건 사례를 피해기업유형, 기술유출자의 회사 내에서의 직위, 공범 여부, 기술유출에 사용된 도구, 기술유출의 동기로 유형화하여 비교 분석할 것이다. 피해기업유형은 중소기업, 대기업, 공기업으로 나누었으며 기술유출자의 회사 내에서의 직위는 퇴직 직전에 근무했던 직위로 정리하였다. 또한 공범여부는 같은 법률로 같이 구속된 사람들을 공범이라고 보았으며 기술유출도구, 기술유출 동기는 뉴스에 나온 사실을 토대로 기재하였다.

## 3. 산업기술유출 사례분석 결과

### 3.1 산업기술유출 피해기업의 유형

산업기술유출의 기업유형은 중소기업, 대기업, 공기업, 기타 순으로 많이 발생하였으며, 특히 중소기업이 55건 중 44건으로 높은 비율을 차지하였다. 자세한 사항은 (그림 1)과 같다.




(그림 1) 산업기술유출 피해기업의 유형

앞에서도 언급한바와 같이 중소기업은 우리나라 90% 이상으로 다수를 차지하고 있으며, 경제의 역동성 제고와 성장 동력의 원천으로서 신산업창출과 기술혁신의 중심 주체로 부각되고 있다. 그러므로 이러한 분석 결과는 기저율처럼 보일 수 있으나, 중소기업의 경우 기술유출방지를 위한 기술보안보다 기술개발에 중점을 두고 회사를 운영하기 때문에 기술유출에 대한 보안이 매우 미비한 실정의 결과라고 볼 수 있다. 또한 중소기업은 자원 및 인력부족으로 인해 기업의 보안역량을 자체적으로 향상시키기에는 한계가 있어 기술유출의 위험이 더 노출되어 있다.

조사된 55건의 사건 중 70%가 기업의 성장을 위해 보안에 대한 투자보다 기술발전에 초점을 두고 있는 실정이었다. 이러한 기업을 대상으로 기업 스스로 보안의 중요성을 인지하도록 산업기술 보안교육 및 보유주체의 보호기능을 강화시켜야 한다. 그럼에도 불구하고 중소기업의 인력과 자원은 한정되어 있기 때문에 산업보안의식 고취를 위한 교육을 기업에게만 전가하지 않고 국가차원에서의 매뉴얼 등을 제정 및 마련하여 배포하고 의무적으로 교육을 이수할 수 있도록 해야 한다.

이러한 보안의 중요성을 고취시키기 위서는 전반적인 사회인식 변화가 뒷받침되어야 한다. 따라서 각종 기술유출 사건 등이 발생한 기업부터 일반 사회까지 사회적인 관심을 유발시키고, 보안 의식을 고취시키는 정부차원의 홍보가 뒷받침되어야 한다. 하지만 무엇보다 산업기술을 보유하고 있는 주체들이 스스로 보호기능을 강화할 수 있도록 적극적으로 지원하여야 한다.

조사된 사건 중 중소기업에서 산업기술유출이 발생했을 때 재귀가 불가능할 정도로 피해를 입은 경우가 40%였다. 피해를 최소화 하는 방법은 기술유출 징후 확인 시 자체적으로 보안을 유지함과 동시에 관계기관과 신속히 공조해야한다. 또한 기술보호 유관기관과 협력관계를 구축하고 보안사고의 자체 해결이 불가능하다고 판단 될 시 보안을 유지한 상태로 신고하여 법적 사후조치를 시행해야 한다.

### 3.2 산업기술유출자의 회사 내에서의 직위

회사 내에서 산업기술 유출자의 직위를 비교한 결과, 고위직임원인 경우 10건, 중간관리직인 경우 22건, 연구원인 경우 16건이었다. 그 중에서도 중소기업에서의 중간관리직에 의한 기술유출이 20건, 연구원에 의한 기술유출이 12건이었다. 자세한 사항은 <표 1>와 같다.

<표 1> 산업기술유출자의 직위

| | | 고위직임원 | 중간관리직 | 연구원 | 직위미상 | 전체 |
|---|---|---|---|---|---|---|
| 중소기업 | 빈도(건) | 7 | 20 | 12 | 5 | 44 |
| | 직위중 | 70% | 91% | 75% | 71% | |
| | 전체 | 16% | 45% | 27% | 11% | 100% |
| 대기업 | 빈도(건) | 2 | 2 | 4 | 1 | 9 |
| | 직위중 | 20% | 9% | 25% | 14% | |
| | 전체 | 22% | 22% | 44% | 11% | 100% |
| 공기업 | 빈도(건) | 1 | 0 | 0 | 1 | 2 |
| | 직위중 | 10% | 0% | 0% | 14% | |
| | 전체 | 50% | 0% | 0% | 50% | 100% |
| 합계 | 빈도(건) | 10 | 22 | 16 | 7 | 55 |
| | 직위중 | 100% | 100% | 100% | 100% | |
| | 전체 | 18% | 40% | 29% | 13% | 100% |

산업기술유출은 고위직임원에 의한 산업기술유출보다 해당 기업의 기술에 대하여 가치성을 잘 알고 접근권한이 용이한 중간관리직에 의한 유출이 22건으로 40%를 차지하고 있었다. 또한 정부기관 연구소 및 대학

교의 경우 직접 기술개발에 참여하여 기술의 가치 및 활용도에 대하여 가장 잘 알고 있는 연구관련 종사자들도 16건으로 산업기술유출을 많이 시도하였다. 이와 같이 중간관리직에 의한 산업기술유출 문제를 해결하기 위해서 각각의 기술에 접근할 수 있는 접근권한이 있는 자를 업무용도에 한해 한정 지어야 한다. 또한 정당한 사용자가 업무서버에 접근했는지 보안시스템 로그를 주기적으로 확인해야 하며, 서로 다른 직역의 중요정보는 교차하여 함께 취급할 수 없도록 관리해야한다.

연구원에 의한 산업기술유출 16건 중 10건이 자신이 연구 혹은 개발한 결과물이 회사의 자산이 아닌 자신의 것이라 주장하였다. 따라서 연구원이 있는 기업에서는 연구결과물의 유출을 방지하기 위해 기술개발 과정의 연구데이터와 결과물은 진행과정을 정확히 파악하여 이력관리를 해야 하며, 기술 개발에 대한 적절한 포상을 부여해야한다.

조사된 사건 중 회사의 영업비밀 등 중요한 정보를 알고 있는 영업직원에 의한 산업기술유출 또한 다수 있었다. 사내 IT 담당 직원 및 영업직원은 업무 특성상 민감한 내부 정보를 접할 기회가 많으므로 보안의식 제고 및 통제를 강화해야한다. 이러한 관리와 통제를 전제로 내부 고급정보를 다루는 관리자급 직원들에 대한 보안의식과 직업윤리 교육 및 상시 교육을 통한 임직원 직업윤리의식을 고양하고 윤리경영을 정착화시키도록 해야 한다. 접근 권한자에 의한 기술유출은 기술을 적절히 취급하는 것에 대한 중요성을 인식하고 자신의 책무를 다할 수 있도록 만드는 것이 중요하다.

### 3.3 산업기술유출의 공범여부

산업기술유출의 공범여부는 단독으로서 범행을 저지르는 경우보다 한 명 이상이 범행을 저지르는 경우가 더 많은 것으로 나타났다. 2명 이상이 공모한 기술유출 범행은 55건 중 38건, 단독으로 진행된 기술유출 범행은 17건 이였다. 이 중에서도 중소기업에서 2명 이상이 공모한 경우가 32건이었다. 자세한 사항은 <표 2>와 같다.

<표 2> 산업기술유출자의 공범여부

| | | 공범 有 | 공범 無 | 전체 |
|---|---|---|---|---|
| 중소 기업 | 빈도(건) | 32 | 12 | 44 |
| | 공범 여부 중 | 84% | 71% | |
| | 전체 | 73% | 27% | 100% |
| 대기업 | 빈도(건) | 4 | 5 | 9 |
| | 공범 여부 중 | 11% | 29% | |
| | 전체 | 44% | 56% | 100% |
| 공기업 | 빈도(건) | 2 | 0 | 2 |
| | 공범 여부 중 | 5% | 0% | |
| | 전체 | 100% | 0% | 100% |
| 합계 | 빈도(건) | 38 | 17 | 55 |
| | 공범 여부 중 | 100% | 100% | |
| | 전체 | 69% | 31% | 100% |

공범이 있었던 사건을 분석하였을 때, 한 명의 중간관리직원이 기업 내의 주요한 기술에 대해 잘 알고 있는 다른 비슷한 직위의 직원 혹은 평소에 친분이 있는 직원을 포섭하여 범죄를 저지르거나 같이 기술 개발에 참여했던 연구와 관련된 사람들이 함께 공모를 하는 경우가 34건이었다. 또한 공범이 있었던 경우 퇴직한 직원이 친분이 있던 현직에 있는 직원에게 요청을 하여 회사 내부의 자료를 요청하기도 하였다. 이와 같은 문제를 해결하기 위해서 직원들에게 개인적 친분에 의한 대가가 없는 내부정보 유출행위도 범죄가 될 수 있음을 주의시키고 주기적으로 산업보안 의식 제고 교육을 시행해야한다. 또한 주요부서와 보직에 혈연, 지연,

학연 등에 따른 특정 인맥이 형성되지 않도록 인사를 배치해야 하며, 인력에 대한 관리가 주기 및 계속적으로 필요하다.

또한 공범이 있었던 38건의 사건 중 29건이 일정한 기간을 두고 퇴직을 하는 공통적인 패턴이 존재하였으며, 한 명이 우선적으로 회사를 퇴사한 후 동종기업을 창설하고 다음 공모한 직원이 유출한 기술을 가지고 해당기업으로 이직하는 경우도 있었다. 따라서 주요 인력의 순차 퇴직이 동반하여 발생할 경우 기술유출 연관성을 파악해야하며, 그리고 핵심인력의 순차적 퇴직이 발생할 시 기술유출 징후 확인 및 주변 동향을 파악하며, 개별적으로 영업비밀 계약 준수여부를 확인해야한다. 이와 더불어 집단적인 핵심인력 이탈 상황에 대비한 퇴직 절차 매뉴얼을 마련하고 직원 퇴사 시 영업비밀보호서약서를 제출받도록 해야 한다.

### 3.4 산업기술유출에 사용된 주된 도구

산업기술유출의 유출방법은 이동식저장매체가 55건 중 33건으로 가장 많이 사용되었다. 그 중에서도 중소기업에서 이동식저장매체에 저장하여 기술을 유출한 경우는 29건 있었다. 자세한 사항은 <표 3>과 같다.

<표 3> 산업기술유출 사용 도구

| | | 이동식저장매체 | e-mail | 기술유출도구기타 | 기술유출도구미상 | 전체 |
|---|---|---|---|---|---|---|
| 중소기업 | 빈도(건) | 29 | 3 | 4 | 8 | 44 |
| | 기술유출도구중 | 85% | 50% | 67% | 90% | |
| | 전체 | 66% | 7% | 9% | 18% | 100% |
| 대기업 | 빈도(건) | 3 | 3 | 2 | 1 | 9 |
| | 기술유출도구중 | 9% | 50% | 33% | 10% | |
| | 전체 | 33% | 33% | 33% | 33% | 100% |
| 공기업 | 빈도(건) | 2 | 0 | 0 | 0 | 2 |
| | 기술유출도구중 | 6% | 0% | 0% | 0% | |
| | 전체 | 100% | 100% | 100% | 100% | 100% |
| 합계 | 빈도(건) | 33 | 6 | 6 | 10 | 55 |
| | 기술유출도구중 | 100% | 100% | 100% | 100% | |
| | 전체 | 60% | 60% | 60% | 60% | 100% |

작업의 전산화됨에 따라 대부분의 주요정보를 서버나 개인PC에 많이 저장하고 손쉬운 휴대성으로 인해 기업의 기밀을 손쉽게 저장해 외부로 반출할 수 있는 장점으로 인해 USB를 기술유출 도구로 많이 사용되어지고 있다. 이외에도 하드디스크, 외장하드 등과 같은 이동식저장매체와 노트북에 주요정보를 저장하여 유출하는 방법이 많이 사용되어지고 있었다. 이와 같은 문제를 해결하기 위해서 기술적, 물리적, 관리적 요소를 모두 고려하여 다차원적으로 문제를 접근하려고 해야 한다. 기술적인 대책으로는 우선적으로 업무용 시스템으로의 로그인 계정과 패스워드는 반드시 공유하지 말아야하며, 개인 소유의 이동식저장매체를 통제하기 위하여 매체제어시스템을 도입하고 운영해야한다. 또한 E-discovery 시스템을 자체적으로 구축 및 운영하거나 접문업체의 서비스를 이용하여 정보 유출 시 증거를 확보할 수 있는 시스템을 구축해야한다.

물리적인 대책으로는 통제구역 출입 시 보안검색을 실시하고 출입등급에 따른 통제 조치를 취해야한다. 사옥 입·출입 시 회사 소유의 장비나 물건 휴대여부 관찰 또는 검색하고 휴일에는 회사 출입구를 최소화 운영하고 내부 직원도 사전에 용무가 허가된 자만 신

원을 확인하여 출입토록 해야 한다. 또한 중요 개소마다 CCTV를 설치하여 자산 손실과 이상 행동을 감시하고 인적이 드문 취약 시간대는 반드시 녹화된 영상을 확인 및 관리해야한다. 그리고 보안구역 출입 시 전자기기 수거 또는 렌즈와 마이크에 보안스티커를 부착하거나 자동으로 녹화 및 녹음이 방지되는 보안시스템을 도입해야한다. 연구소나 생산 공정의 경우에는 연구자료 및 산출물 등은 비밀로 지정하고 온오프라인 사용, 연구진행 모니터링, 주요 업무 서보와 네트워크에 대한 보안관제 시행으로 이상행위 탐지 및 이상패턴을 감시해야한다.

마지막으로 관리적인 대책은 무엇보다 중요하다. 우선적으로 이동식저장매체는 사내 반출입하지 못하게 혹은 무단 사용할 수 없도록 관리해야하며, 개인용 USB의 사용을 금지하고 업무용 보안 USB를 사용하도록 해야 한다. IT기기는 업무 용도로만 지급하여 사용하게 해야 하며, 주요정보의 유통은 사내 웹하드 등 저장공간 중앙 집중화를 통해 이루어져야한다. 이뿐만 아니라  또한 산업기밀에 해당하는 자료는 보안조치가 된 별도의 저장매체에 보관하도록 해야 하며, 개인 IT기기의 회사 반입 금지 또는 사용을 통제해야한다. 업무용으로 지급된 IT기기 외에 사내에서의 개인용 정보통신기기 사용을 통제하고 퇴사자의 업무용 PC는 곧바로 전용하지 않고 일정기간 그대로 보존해야한다. 그리고 E-메일에 대한 보안 매뉴얼을 만들어야하며, E-메일은 업무용 메일로 사용을 한정해야한다. 외부로 수·발신 시 보안 부서를 경유하여 사용해야하며, 보안성 검토 프로세스를 추가하여 E-메일 보안에도 신경을 쓰도록 해야 한다. 또한 업무용 IT기기는 도입 시 고장 및 유지보수를 대비하여 사전 보안조치가 된 여유분을 비치하여 활용해야하며, 일반적인 사무공간과 IT기기 운영 공간을 분리하고 데이터 장치에는 임의탈착이 불가하도록 잠금장치 등을 부착해야한다.

### 3.5 산업기술유출의 주된 동기

산업기술유출의 유출 동기는 금품 및 향응제공인 경우가 35건으로 가장 많은 비중을 차지하고 있었다. 그 중에서도 중소기업에서의 금품 및 향응제공에 의한 경우는 28건 이었다. 자세한 사항은 <표 4>과 같다.

<표 4> 산업기술유출 범행의 주된 동기

| | | 금품 및 향응 제공 | 스카우트 | 회사 우대처에 대한 불만 | 기술 유출 동기 미상 | 전체 |
|---|---|---|---|---|---|---|
| 중소기업 | 빈도(건) | 28 | 3 | 11 | 2 | 44 |
| | 기술유출 동기 중 | 80% | 75% | 100% | 40% | |
| | 전체 | 64% | 7% | 25% | 5% | 100% |
| 대기업 | 빈도(건) | 6 | 1 | 0 | 2 | 9 |
| | 기술유출 동기 중 | 17% | 25% | 0% | 40% | |
| | 전체 | 67% | 11% | 0% | 22% | 100% |
| 공기업 | 빈도(건) | 1 | 0 | 0 | 1 | 2 |
| | 기술유출 동기 중 | 3% | 0% | 0% | 20% | |
| | 전체 | 50% | 0% | 0% | 50% | 100% |
| 합계 | 빈도(건) | 35 | 4 | 11 | 5 | 55 |
| | 기술유출 동기 중 | 100% | 100% | 100% | 100% | |
| | 전체 | 64% | 7% | 20% | 9% | 100% |

금품 및 향응제공을 위해 산업기술을 유출한 사건 중 33건은 유출한 기술을 타 회사로 판매하여 직접적인 금전적인 이득을 취하거나 유출한 기술을 직접 활

용하여 경쟁회사를 설립을 통해 금전적인 이득을 취하려고 하였다. 이와 같은 문제를 해결하기 위해서 신제품 개발에 공적이 있거나 직무발명을 한 임직원에게는 정당한 보상을 시행해야하며, 한 직원과 회사 비전 공유 등으로 의사소통을 활성화하고 주인의식을 고취하도록 해야 한다.

회사처우에 대한 불만을 가지고 산업기술유출을 한 경우는 인사 및 승진에 대한 불만, 기밀자료 불법취급·공급횡령 등과 같은 내부 감사에 의한 적발, 경영상태의 약화 등 심리적 변화로 인한 우발적 범행을 저질렀다. 따라서 업무 실적에 대한 평가는 합리적 기준에 따라 임직원이 납득할 수 있게 시행하고 제도의 한계로 부득이하게 불이익을 입은 직원에게는 대체 보상안을 제시해야한다. 이외에도 계속적으로 경영 상황을 임직원들에게 투명하게 공개하고 상호소통 하는 기업문화를 정착시켜 일체감 조성 및 불만에 대한 동요를 방지해야한다. 그리고 경영진과 주요부서의 장들에게는 상호 소통, 조직 소속감, 윤리의식 등을 높일 수 있는 프로그램을 계획하여 정기적인 행사를 진행할 수 있도록 해야 하며, 핵심인력에 대한 성과보상기준 수립 및 시행으로 소속감을 고취시켜야한다. 이외에도 개인영리를 위해 타 회사의 스카우트 제의를 승낙한 기술유출도 빈번하게 발생하고 있었다. 따라서 기업은 업계 연구 및 기술 인력에 대한 스카우트 업계 동향을 주시하여 인력 이탈에 대비해야하며, 관련 학계 및 업계의 연구개발 동향은 수시로 파악하여 기술보호업무와의 연관성을 파악해야한다. 무엇보다 장기 재직 후 퇴직한 연구 인력에게는 보상 프로그램을 제공하고 영업비밀 준수의무 부과 및 준수여부를 확인해야한다

## 4. 결론 및 제언

기존 연구에서는 산업기술유출자가 주로 전·현직 직원들로 제시되었지만, 본 연구 결과 전·현직 직원 이외에도 공동연구에 참여하는 연구원에 의해 발생하는 경우도 많은 것으로 밝혀졌다. 또한 산업기술 유출범죄의 직위와 관련해 중간관리직에 의한 산업기술유출이 40%로 기업에서 기밀자료 등에 대한 접근권한이 보다 수월한 사람들에 의한 산업기술유출의 경우가 많은 부분을 차지하고 있었다. 그 외에도 연구소장 및 연구원 등 기술개발에 직접적으로 참여하고 있는 인원에 의해 유출되는 경우도 적지 않았다. 이렇게 유출한 기술의 활용은 금품 및 향응을 제공받는 등 개인의 경제적인 이득을 목적으로 하는 경우가 가장 높게 나타났으며, 회사처우에 대한 불만인 경우가 두 번째로 많이 나타났다. 또한 산업기술 유출은 2인 이상의 공모로 많이 발생되고 있음을 알 수 있었으며 피해기술이나 유출수단의 경우 usb, 외장하드 등 이동식저장매체에 옮기는 경우가 대부분을 차지하였다.

본 논문에서는 산업기술유출의 사례분석을 통하여 산업기술유출의 심각성과 현황을 살펴보고 피해기업 유형, 기술유출자의 직위, 공범여부, 기술유출도구, 기술유출동기를 살펴보았으며 이에 대한 시사점과 해결방안은 다음과 같다.

첫째, 산업기술유출 범죄는 1명이 아닌 다수에 의해 진행되는 경우가 많기 때문에 핵심인력의 순차적 퇴직이 발생할 시 기술유출 징후 확인 및 주변 동향을 파악하여 범죄에 신속한 대응을 할 수 있다. 또한 산업기술유출 범죄는 단기간에 의한 범죄가 아닌 기술 확보, 퇴직, 동종업계 재취직 혹은 설립 등 단계에 걸쳐 발생하는 범죄이기 때문에 큰 피해가 발생하기 전에 예방하고 범죄를 차단할 수 있다.

둘째, 산업기술유출은 고위직임원에 의한 범죄보다 기술에 대한 가치를 잘 알고 접근 권한이 용이한 중간관리직에 의한 유출이 다수였기 때문에 직무발명보상제도의 도입과 실시를 통하여 기술유출을 억제할 수 있다. 또한 집중적이고 전문적인 인력을 통해 주기적인 보안시스템 관리와 상시적인 보안의식 및 직업윤리 교육 등 물리적 보안과 보안교육의 교차적인 관리를 통해 범죄를 예방할 수 있다.

셋째, 산업기술유출 범죄는 금품 및 향응제공을 위해 타 회사로 기술을 판매하거나 유출한 기술을 직접 활용하여 경쟁회사를 설립한 경우가 많았기 때문에 기업에서는 능동적으로 동종 업계의 연구개발 동향을 수

시로 파악하여 기술보호업무와의 연관성을 파악해야 한다. 또한 퇴직한 핵심 인력에게는 영업비밀 준수의무 부과 및 준수여부를 상기시키도록 해야 한다. 무엇보다 이를 뒷받침하기 위해 기술유출에 의한 수익을 제제할 수 있는 법적 강화 방안이 강구되어야 한다.

이와 같이 본 연구는 국내에서 발생한 산업기술유출에 대한 사례분석을 통해 산업기술유출에 따른 피해현황을 파악하고 다양한 분류체계를 통해 기술유출의 피해기업유형, 기술유출자의 직위, 범죄의 공범여부, 기술유출도구 등을 알아보았다. 산업기술유출은 점점 지능화 · 첨단화 · 고도화 되어 가고 있기 때문에 이에 따른 예방법과 대응방안을 마련하는 것이 필요하다. 따라서 본 논문을 통해 산업기술유출범죄에 대한 전반적인 흐름과 특징을 파악하고 실무와 관련 연구에 기초자료가 될 수 있기를 기대한다. 그러나 본 연구는 연구방법에 있어서 표본 수가 55건에 불과하다는 한계를 갖고 있다. 이는 연구결과의 일반화를 저해하는 문제점으로 작용한다. 향후 후속 연구에서는 충분한 표본수를 확보해 연구결과의 일반화가 가능하도록 보완해야 할 것이다.

## 참고문헌

[1] 강욱·전용태, “산업보안 담당자의 보안정책 준수에 영향을 미치는 요인”, 한국경찰연구학회논문지, 제13권, 제3호, pp. 273-298, 2014.

[2] 국신욱, “중소기업 기술유출 방지를 위한 법제 연구”, 산업재산권학회논문지, 제46권, pp. 201-239, 2016.

[3] 김신혜, 박준석, 박길준, “산업기술유출 범죄의 대응에 관한 연구”, 한국사회안전학회지, 제9권, 제1호, pp.91-109, 2013.

[4] 노호래, “산업기술 유출범죄에 대한 정책적 대응방안”, 한국공안행정학회, 제30권, pp. 46-77, 2008.

[5] 박찬수, 황정하, “기술유출에 대한 범국가적 대응방안“, 과학기술정책연구원논문지, 제120권, pp. 1-33, 2013.

[6] 서봉성, 임유석, “산업보안범죄의 실태 및 대응방안”, 융합보안학회논문지, 제15권, 제6호, pp. 141-149, 2015.

[7] 이윤호, 김도우, 유병재, “사이버 공간에서의 일상활동과 범죄피해”, 한국공안행정학회보논문지, 제44권, pp. 214-240, 2011.

[8] 이준복, “산업스파이 및 M&A에 따른 산업기술유출 대응방안에 관한 법적 연구”, 경찰학연구논문지, 제14권, 제3호산업스파이 및 M&A에 따른 산업기술유출 대응방안에 관한 법적 연구, pp. 89-120, 2014.

[9] 이창무, “산업보안의 개념적 정의에 관한 고찰”, 산업보안연구학회논문지, 제2권, 제1호, pp. 73-90, 2011.

[10] 이훈재, “산업스파이 범죄실태 및 대응정책의 개선방안 연구”, 경찰학논총학회논문지, 제6권, 제1호, pp. 179-202 ,2011.

[11] 이희선, “기술유출범죄의 실태분석 및 대응방안에 관한 연구”, 민간경비학회논문지, 제20권, pp. 281-302 ,2012.

[12] 임하늘, 최재용, 유영재, “성별에 따른 청소년 범죄피해 원인 연구: 자기통제이론, 일상활동이론을 중심으로”, 한국경찰학회보논문지, 제52권, pp. 273-298, 2015.

[13] 장항배, “산업기술 유출방지를 위한 보안시스템 평가 탐색적 연구”, 산업보안연구학회논문지, 제1권, 제1호, pp. 50-61, 2009.

[14] 장항배, “산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구”, 융합보안논문지, 제15권, 제7호, pp. 39-45, 2015.

[15] 정덕영, 정병수, “산업스파이 현황과 대응방안”, 한국콘텐츠학회논문지, 제7권, 제11호, pp. 205-214, 2007.

[16] 정진홍, “산업스파이 범죄에 대한 원인분석과 대응방안 연구”, 과학수사학회논문지, 제2권, 제2호, pp. 153-157, 2008.

[17] 조호대, “기술유출 사례 분석을 통한 효과적 산업

보호 방안", 한국경찰학회논문지, 제37권, pp. 335-354, 2012.

[18] 주성빈, 최응렬, "외국인 산업스파이에 의한 산업기술유출 대응방안에 관한 연구 : 단기 출입국자를 중심으로", 한국부패학회논문지, 제18권, 제2호, pp. 73-93, 2013.

[19] 최관, "산업보안기밀 유출원인에 관한 연구", 산업보안연구학회논문지, 제5권, 제1호, pp. 73-93, 2015.

[20]최순호, 정우일, "경찰의 산업보안활동 활성화 방안", 제 11권, 제1호, pp. 227-252, 2009.

[21] 황현동, 이창무, "산업기술유출과 자기통제력, 조직애착도의 관계에 관한 연구", 한국경호경비학회논문지, 제47권, pp. 119-137, 2016.

[22] 이창무, 김민지, '산업보안이론', 법문사, 2013.

## [저 자 소 개]

양 현 정 (Hyun-jung Yang)
2016년 2월 한남대학교 경찰행정학사
2016년 3월 ~ 현재 중앙대학교 융합보안학과 석사

email : hj20126@cau.ac.kr

이 창 무 (Chang-moo Lee)
1985년 2월 연세대학교 정치외교학사
1994년 ~ 2002년 뉴욕시립대학교 형사사법학 석사 및 박사
2003년 ~ 2014년 한남대학교 경찰행정학과 교수
2015 ~ 현재 중앙대학교 산업보안학과 교수

email : cmlee@cau.ac.kr