중소기업 기술유출사고 유형에 따른 디지털증거기반 대응방안 연구

[1] 왕재윤, [2*]장항배

Research on digital evidence-based countermeasure depending on the type of small and medium-sized enterprises technology leakage accident

[1]Jaeyun Wang, [2*]Hangbae Chang

요 약

우리나라 산업과 경제의 근간에는 중소기업이 뿌리의 역할을 하고 있으며 대부분의 기술적 혁신은 대기업보다 중소기업에서 일어나고 있다. 기술개발과 기술혁신만이 중소기업이 치열한 경쟁구도 가운데 생존할 수 있는 유일한 길이기에 매진하는 한편 기술보호에는 관심과 투자가 인색한 편이다. 그로 인해 산업기술유출 사고가 빈번히 일어나고 있으며 이에 대한 개선대책을 중소기업 여건상 충족시키기 어렵다. 유출사고가 발생하였을 때 범죄 행위를 입증하기 위해서는 가장 핵심인 디지털증거가 필요하지만 관리상 허점으로 인해 디지털증거가 훼손되고 삭제되거나 하는 등의 문제가 발생하곤 한다. 따라서 본 연구를 통해 기술유출사고 유형에 따른 디지털증거기반의 대응방안을 설계하고자 한다. 실제로 발생하였던 기술유출사고 유형을 분류하고 내부정보유출방지솔루션을 운영하는 중소기업 보안환경에서 디지털증거 확보 방안을 연구하려 한다.

Abstract

Small and medium-sized enterprises play a fundamental role in the foundation of our country's industry and economy, and most technological innovations occur in small and medium-sized enterprises rather than large corporations. Technology development and innovation are the only way for small and medium-sized enterprises to survive in a fiercely competitive environment, so they focus on it, but interest and investment in technology protection tend to be stingy. As a result, industrial technology leakage accidents occur frequently, and it is difficult to meet improvement measures. When a leak occurs, digital evidence is required to prove criminal activity, but problems such as digital evidence being damaged or deleted due to management loopholes often occur. Therefore, through this study, we aim to design a digital evidence-based countermeasure depending on the type of technology leak accident. We will classify the types of technology leak incidents that actually occurred and study ways to secure digital evidence in the security environment of small and medium-sized businesses that operate internal information leak prevention solutions.

Keywords: *Small and medium-sized enterprises, technology protection, Industrial technology leakage, Digital evidence, Data loss protection*

[1] *중앙대학교 대학원 융합보안학과 석사과정(howard81@naver.com)*
[2*교신저자] *중앙대학교 산업보안학과 교수(hangbae.chang@gmail.com)*

Received: Nov. 28, 2023, Revised: Dec. 15, 2023, Accepted: Dec. 18, 2023

I. 서론

우리나라 산업과 경제의 근간에는 중소기업이 뿌리의 역할을 하고 있으며 대부분의 기술적 혁신은 대기업보다 중소기업에서 일어나고 있다. 기술개발과 기술혁신만이 중소기업이 치열한 경쟁구도 가운데 생존할 수 있는 유일한 길인 것이다. 우리나라의 전체 산업에서 95% 이상의 비중을 차지하고 있는 중소기업은 주변 환경변화에 대한 유연성과 민첩성이 뛰어나다는 장점을 가지고 있으며 대부분의 혁신은 대기업보다 중소기업에서 일어나고 있다[1].

하지만 중소기업은 대기업에 비해 보안인프라 투자 및 보안인력 보유가 매우 열악하여 기술유출 사고가 빈번하게 일어나고 있으며 이로 인해 도산하거나 경영사정이 매우 어려워지는 현실을 뉴스나 매체를 통해 자주 접할 수 있다. 국정원에 따르면 2017 년도부터 2023 년 6 월까지 해외로 기술유출이 발생한 사건은 총 128 건이었으며 이중 76(59%)건이 중소기업에서 발생하였다고 하였다.

중소기업의 이러한 기술유출 사고의 원인으로는 다양한 설문자료 및 연구가 이뤄져 왔으며 이를 바탕으로 원인에 대한 개선대책은 많은 전문가를 통해 발표되어 왔다.

중소기업은 기술유출 대응체계가 매우 미흡하여 기술유출에 대한 수사와 증거 확보에 있어 어려움을 겪고 있으며 이러한 요인 중 하나가 디지털 증거이다.

IT 기술의 끊임없는 발전은 우리 주변의 사무 환경을 크게 변화시키고 있으며 기술유출에 대한 디지털 증거를 컴퓨터 하드디스크에서 거의 확보 가능하던 현실에서 스마트폰, 태블릿, USB 등 디지털 기기의 다양성은 디지털 증거 확보를 복잡하게 만들고 있다[2].

본 연구에서는 중소기업의 기술보호 현황 분석을 통해 기술유출 사고 발생 시 신속하고도 신뢰할 수 있는 디지털 증거 확보를 할 수 있는 모형 설계를 목표로 하고 있다. 이를 위해 중소기업에서 운영중인 내부정보유출방지솔루션의 로그를 통해 기술유출사고 유형별 시나리오를 모델화하여 그에 따라 보안감사 차원에서 어떠한 행위들을 유심히 모니터링해야 중소기업 기술유출 사고 발생을 사전에 인지할 수 있는지와 사후 복구를 위한 디지털 증거 수집에 관한 효과적인 모델을 연구하고자 한다.

II. 이론적 배경

2.1 산업보안의 이해

산업보안의 이해에 앞서 ‘산업’과 ‘보안’에 대한 개념을 먼저 이해하고 산업보안의 개념을 살펴보도록 하겠다. 산업이란 재화나 서비스를 생산하는 활동을 말한다. ‘표준국어대사전’은 산업을 “인간의 생활을 경제적으로 풍요롭게 하기 위하여 재화나 서비스를 창출하는 생산적 기업이나 조직, 농업·목축업·임업·광업·공업을 비롯한 유형물의 생산 이외에 상업·금융업·운수업·서비스업 따위와 같이 생산에 직접 결부되지 국민경제에 불가결한 사업도 포함하며, 좁은 뜻으로 공업만을 가리키기도 한다”고 구체적으로 정의하고 있다. 사실상 사람들이 삶을 영위하기 위한 모든 경제활동을 포함한다고 볼 수 있다.

보안의 의미는 매우 다양하게 쓰이고 있으며 그러다보니 명확하게 정의하기도 힘든 문제가 있다. 보안이라는 용어는 표준국어대사전에 의하면 “안전을 유지함”, “사회의 안녕과 질서를 유지함” 이라고 정의하고 있지만 보안이라는 단어 하나의 조합만으로는 산업계에서 해석하기에 명확한 개념을 잡기가 어렵다.

보안은 결국 산업보안을 비롯해, 정보보안, 사이버보안, 물리보안, 방산보안, 융합보안 등 각각의 산업별, 주제별로 보안이란 단어와 결합된 용어들이 널리 사용되고 있다. 광범위하고 모호한 보안개념을 명확하고도 이해도를 높이기 위해서는 보안 개념을 보다 엄밀하게 규정할 필요가 있다.

그렇다면 산업보안이라 함은 인간의 생활을 경제적으로 풍요롭게 하기 위한 재화나 서비스를 창출하는 기업 또는 유무형의 생산물을 보호하기 위한 일체의 노력이라고 볼 수 있다.

2.2 산업기술의 이해

'산업기술'이라 함은 제품 또는 용역의 개발・생산・보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 행정기관의 장(해당 업무가 위임 또는 위탁된 경우에는 그 위임 또는 위탁받은 기관이나 법인・단체의 장을 말한다)이 산업경쟁력 제고나 유출방지 등을 위하여 법률에서 위임한 명령에 따라 지정・고시・공고・인증하는 9 개 목의 어느 하나에 해당하는 기술을 말한다. 하지만 2016 년 전력기술관리법 제 6 조의 2 가 삭제됨에 따라 8 개의 기술만 해당되며 현재 법률 개정을 준비중에 있다.

산업기술은 국가핵심기술을 포함하는 개념으로 기술상 정보만을 말한다. 그리고 영업비밀은 기술상 또는 경영상의 정보까지 포함하고 있어 영업비밀의 기술상 정보는 산업기술에 포함된다고 본다. 산업기술과 국가핵심기술, 영업비밀의 관계에 대한 도식화를 해보면 그림 1 과 같다.

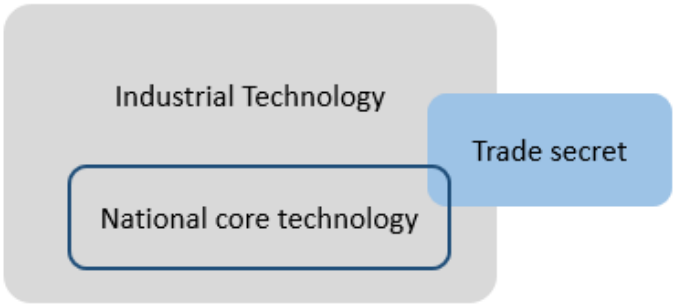

Figure 1. Relationship between industrial technology, trade secrets, and national core technology
그림 1 산업기술, 영업비밀, 국가핵심기술의 관계[3]

2.3 산업기술 및 영업비밀 현행 법제도

2000 년도 들어 우리나라 기술의 위상이 높아짐에 따라 불법으로 산업기술이 해외로 유출되는 사례가 발생하였지만 당시 법률로는 기술유출에 대한 마땅한 처벌 법적조항을 찾는 것이 상당히 어려운 실정이었다. 정부는 2006 년 10 월「산업기술의 유출방지 및 보호에 관한 법률」(약칭:산업기술보호법)을 제정하여 국내 산업기술을 보호하여 국가 경쟁력 강화 및 국민경제의 안정을 도모하고자 하였다.

산업기술보호법은 '산업기술' 과 '국가핵심기술' 을 그 보호대상으로 하고 있으며 부정한 방법으로 타인의 산업기술을 취득・사용・공개하는 행위를 금지하고 있다. 산업기술을 부정한 방법으로 유출한 자의 경우 해외유출은 15 년 이하의 징역 또는 15 억원 이하의 벌금에 처하며, 국내유출의 경우는 7 년 이하의 징역 또는 7 억원 이하의 벌금에 처하되 징역형과 벌금형을 병과할 수 있다. 또한, 미수범과 예비・음모한 자의 경우에도 처벌할 수 있게 법이 제정되어 있다.

영업비밀은 「부정경쟁방지 및 영업비밀보호에 관한 법률」(약칭:부정경쟁방지법)에서 정의하고 있다. 영업비밀이란 "공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 비밀로 관리된 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다. 따라서 영업비밀로서 보호받기 위해서는 ① 공공연히 알려져 있지 않을 것(비공지성), ② 비밀로서 관리되고 있을 것(비밀관리성), ③ 독립된 경제적 가치를 가진 것으로서 생산방법・판매방법 기타 영업활동에 유용할 것(경제적 유용성) 이 3 가지 조건을 갖추어야만 영업비밀이 성립되는 요건을 갖추게 된다.

비밀관리성은 초기에는 "상당한 노력" 으로 비밀을 유지할 것을 요구하였지만 보안투자 예산이 턱없이 부족한 중소기업에게는 비밀로 유지하기 위한 보안인프라를 충분히 갖추기란 쉽지 않았다. 이에 개정법은 "상당한 노력" 에서 "합리적인 노력" 으로 완화하였고 2019 년 1 월 다시 동법을 개정하여 "합리적인 노력" 이 없더라도 비밀로 유지되었다면 영업비밀로 인정받을 수 있도록 요건을 대폭 완화하였다.

2.4 중소기업 기술유출 현황

2017 년도부터 2021 년까지의 산업기술・영업비밀 유출사범 검거현황을 보면 표 1 에서와 같이 총 593 건의 산업기술유출사건을 수사하여 1,638 명을 검거하였다. 피해기업의 규모를 보면 중소기업이 540 건(91%)으로 피해가 심각한 것으로 나타났으며 대부분 국내 유출로 인한 사고로 조사되었다.

Table 1. `17~`21 Status of industrial technology and trade secret leak investigation
표 1. `17 년~`21 년 산업기술.영업비밀 유출 수사 현황[4]

Year	Arrest (case)	Arrest (number of people)	Technology type		Size of damaged company		Domestic and international leaks	
			Industrial technology	Trade secret	Small and medium-sized enterprises	major company	Domestic	Inter national
2017	140	336	12	128	128	12	127	13
2018	117	352	10	107	106	11	97	20
2019	112	381	6	106	104	8	100	12
2020	135	345	7	128	122	13	118	17
2021	89	224	10	79	80	9	80	9
Total	593	1,638	45	548	540	53	522	71

중소기업의 기술유출 사고는 해마다 줄어들지 않고 있으나 정부의 R&D 예산 투입 대비 기술보호 예산 투입은 매년 제자리 걸음 수준이다.

중소벤처기업부・대중소기업농어업협력재단에서 발표한 2022 중소기업 기술보호 수준 실태조사 보고서에 따르면 기술침해 주체는 내부직원 또는 전직직원에 의한 유출이 58.3%를 차지하였고 협력업체 등 제 3 자를 통한 유출이 25%로 집계되었다[5].

2010 년~2014 년 5 년간 기술유출 주체별 직급을 보면 임원(33%), 부장(29%), 연구원(23%), 연구소장(8%) 등 기업의 핵심 기술에 대한 가치를 알고 가장 손쉽게 접근할 수 있는 직원에 의한 기술유출 행위가 빈번히 이뤄진다[6]. 이들의 유출 동기는 대부분 금전적인 유혹과 회사처우에 대한 불만, 회사 경영상태 악화 등 계획범죄와 우발적 범죄로 나뉘어진다.

그렇다면 위의 자료와 같이 인력에 의한 기술유출은 어떠한 수단과 방법에 의해 이뤄지는지 보면 양현정(2018) 연구에서는 2007 년부터 2017 년까지 산업기술유출 수단별 건수자료에서 다음과 같이 분석하였다. 이동식 저장매체가 142 건(56%)으로 가장 높은 수치를 보였으며 다음으로는 E-mail 을 통한 기술유출이 38 건(15%)으로 조사되었다[7].

해당 실태조사 자료 뿐만 아니라 언론을 통해 접하는 기술유출 사고를 보면 상당수가 USB 와 E-mail 관리 부재로 인해 기술유출 사고가 일어나는 것을 심심치 않게 접할 수 있다.

이는 문서가 전자화되면서 대용량의 파일을 아주 간결하게 옮길 수 있는 수단이 오래전부터 유출 수단의 하나로 자리매김하였으며 이는 곧 중소기업의 내부정보유출방지솔루션의 부재가 가장 큰 요인일 것이다. 내부정보유출방지솔루션이란 악성코드, 멀웨어와 같은 사이버 위협인자들을 대응하는 것이 아닌 임직원들의 이메일, 클라우드 스토리지, 이동형 저장매체, 메신저, P2P 등을 통제하거나 행위에 대한 로깅을 할 수 있도록 만들어진 것으로써 PC 를 통한 다양한 정보유출 경로를 통제하고 이력을 서버에 저장해 정보유출 사고를 예방할 수 있다.

내부정보유출방지솔루션은 구성방식에 따라 3 가지로 구분할 수 있으며 Endpoint DLP, Network DLP, Storage DLP 로 구분한다. 이 세가지 구성방식 중 대다수의 중소기업은 Endpoint DLP 를 사내에 구축하는 편이며 이를 통해 다양한 기술유출 경로들을 통제하고 있다.

기술유출 사고를 인지한 후 기업은 사고수습을 위해 갖은 노력을 하지만 증거자료 확보에 상당한 어려움을 호소한다. 퇴직자가 사용하던 PC 의 무결성과 퇴직자의 유출행위를 판단할 수 있는 자료가 훼손되거나 다양한 이유로 보존되지 못하는 경우가 많기 때문이다. 중소벤처기업부 실태조사에 따르면 중소기업은 기술유출 사고 이후 법적 대응 시 자료 수집의 어려움이 매우 많다고 응답하였으며 두 번째로는 법적 대응에 소요되는 긴 시간 및 높은 비용을 말하였다[8].

중소기업이 법적 소송 시 소요되는 시간의 장기화에 대해서는 정점영(2022) 연구에 따르면 기업이 보유한 기술이 비밀로 관리되고 있었다는 입증을 해야하기에 수사 과정이 장기화 된다고 하였다. 그리고 핵심인력이 사용한 하드디스크 등 정보저장매체에 대한 원본 확보를 위한 부분도 상당 시간 소요되는 일부분 중 하나의 요인이라고 하였다[9].

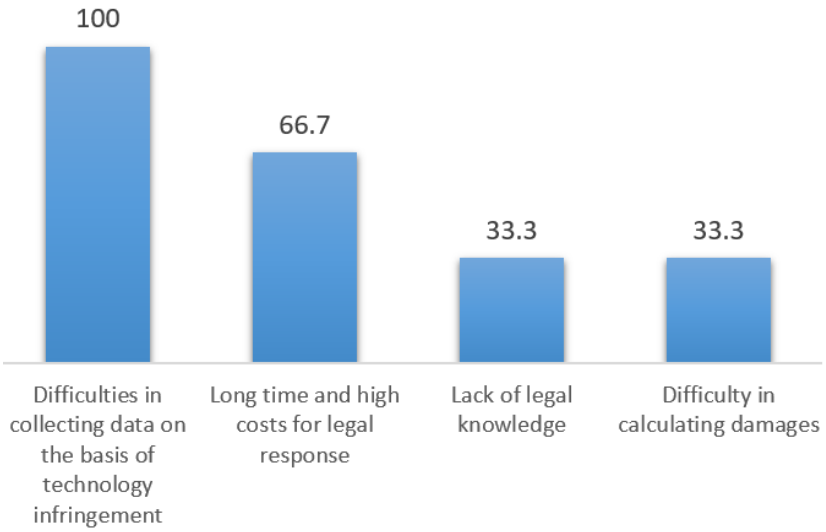

Figure 2. Difficulties in legal response after technology infringement
그림 2. 기술침해 이후 법적 대응 조치 시 어려움

2.5 디지털증거와 디지털 포렌식

2.5.1 디지털증거의 이해

디지털증거는 범죄와 관련하여 증거로서의 가치가 있는 전자정보를 말하고 수사목적을 달성하는데 필요한 최소한의 범위에서 수집되는 정보를 말한다[10].

또한 “컴퓨터 시스템 또는 그와 유사한 장치에 의해서 디지털로 생성・저장・전송되는 증거가치가 있는 디지털 데이터” 또는 Network 상에서 정보를 작성, 전송, 접속기록 등에서 생성되거나 저장된 모든 자료를 디지털증거라고 정의를 내릴 수 있다[11].

디지털 증거 7 개의 특성을 가지는데 매체독립성, 복제 가능성, 무체정보성, 변조용이성 및 취약성, 대량성, 전문성, 네트워크 관련성이란 특성을 가진다. 매체독립성이란 어떠한 형태를 가지고 있거나 지각할 수 있는 것이 아니며 매체에 저장되어 있거나 전송중인 ‘정보’ 그 자체라는 특성이다[12].

복제 가능성이란 디지털 증거는 위・변조 및 삭제가 매우 용이하여 수집된 증거가 원본 또는 복사본인지 불명확한 경우가 대부분이므로 내용이 동일한 데이터라고 할지라도 복사되거나 다른 방법에 의해 새로 저장되었을 경우, 데이터가 생성되거나 접근한 시간이 서로 달라지기 때문에 증거수집 절차상 각별한 주의가 필요하며 이를 위해서는 기술적 대책과 절차가 필요하다[13].

무체정보성은 전자적 기록매체에 기록, 보존되는데 이는 눈에 보이지 않는 0 과 1 의 조합인 디지털 형태로 작성되기 때문에 그 상태를 사람의 지각으로 바로 인식할 수 없고, 증거로 사용되기 위해서는 사람이 인식할 수 있도록 기술적 절차를 거쳐야 한다는 특징이다[14].

변조용이성 및 취약성은 하나의 명령만으로도 수많은 디지털 자료를 삭제하거나 변경시키는 것이 용이하여 위.변조 및 삭제가 매우 용이하다[15]는 뜻이며 온도, 습도, 충격, 전자기파 등 주변의 환경에 영향을 받을 수 있는 취약성이 있다[16].

대량성이란 특성은 저장매체의 발전과 더불어 데이터의 양이 과거 킬로바이트 기준에서 현재 기가바이트, 테라바이트까지의 대용량 매체를 쉽게 접하게 되었고 이에 따라 디지털 증거도 대량의 데이터가 생성되고 있다는 특성을 말한다.

전문성이란 디지털 증거의 수집과 분석에 전문적 기술이 사용되고 전문가가 개입해야 가독성, 가시성 있는 자료로 제시하고 내용을 해석할 수 있다는 것이며 네트워크 관련성은 증거가치 있는 디지털 정보를 수집하기 위해서는 네트워크를 통해 시스템 자원에 접근해야 하는데 이러한 디지털 증거의 특성을 ‘네트워크 관련성’이라고 한다[17].

2.5.2 디지털 포렌식의 이해

디지털 포렌식은 디지털 증거의 수집과 분석에 관한 일련의 절차와 기술을 통칭하는 개념으로서 디지털 증거에 대한 과학적인 조사와 기술적 기법 뿐만 아니라 위법수집 증거배제법칙과 적법절차가 적용되는 법과학의 분야이다. 일반적으로 법적인 증거로 사용된다는 관점에서 컴퓨터 시스템이나 디지털 기기로부터 디지털 자료를 수집하는 단계로부터 이를 분석하고 분석된 자료에 대한 보고서를 작성하고 증거를 보존하는 일련의 절차 및 기술을 통칭하여 디지털 포렌식이라고 한다. 즉 디지털 포렌식은 디지털 소스로부터 디지털 증거를 보존(Preservation), 수집(Collection), 증명(Validation), 식별(Identification), 분석(Analysis), 해석(Interpretation), 기록(Documentation), 제출(Presentation)하기 위하여 과학적으로 이끌어내고 증명하는 방법이라고 할 수 있다[18].

III. 연구방법 및 분석결과

3.1 기술유출사고 유형분류에 따른 모형 설계

본 연구는 앞서 기술유출 현황에서 보여지는 기술유출 수단들을 통해 일어날 수 있는 행위들을 큰 범주에서 5 가지 유형으로 구분하였다. 5 가지의 유형에서 첫 번째 인자는 HDD 변경, 두 번째 인자는 취업사이트 접속, 세 번째 인자는 USB・이동식 저장매체, 네 번째는 E-mail, 마지막은 출력물로 정하여 각 유출경로별로 발생 가능한 기술유출 시나리오를 그림 3 과 같이 도식화하였다.

그림 3 을 기반으로 하여 중소기업에서 수집되는 로그들로 분석 가능한 이상징후 시나리오 28 개를 모델로 설계하였다.

연구의 대상은 중소기업 1,041 개 기업을 모집단으로 하였으며 해당 기업은 내부정보 유출방지 솔루션(DLP(Data Loss Prevention)솔루션)을 운영하여 기술유출 수단별 로그가 확보가 되는 기업이었다.

22 년도 한 해 동안 1,041 개 중소기업에서 발생하는 내부정보유출방지 솔루션의 모든 로그들을 빅데이터화하여 이상징후 시나리오와 매칭되는 결과값을 찾아 실시간으로 중소기업 보안담당자에게 이메일을 통해 통보해 주었다.

28 개의 시나리오 모형은 회사 내의 문서가 정상적인 범주에서의 반출이 아닌 비정상적으로 반출될 수 있는 행위 인자들을 나열하여 각각의 인자들을 시간과 파일 개수를 임계치로 구성하였다. 또한, 하나의 인자와 다른 인자간에 상관관계를 구성하여 복합적인 시나리오도 만들어 분석할 수 있도록 하였다.

시나리오별 중소기업에서 기술유출 발생 시 사고복구를 위한 증거자료 확보에 가장 유의미한 인자값들이 어떤 것들이 있는지 파악해보고 이를 통해 본 연구의 주제인 기술유출사고 유형별에 따른 디지털증거기반 대응 모델을 만들어보고자 한다.

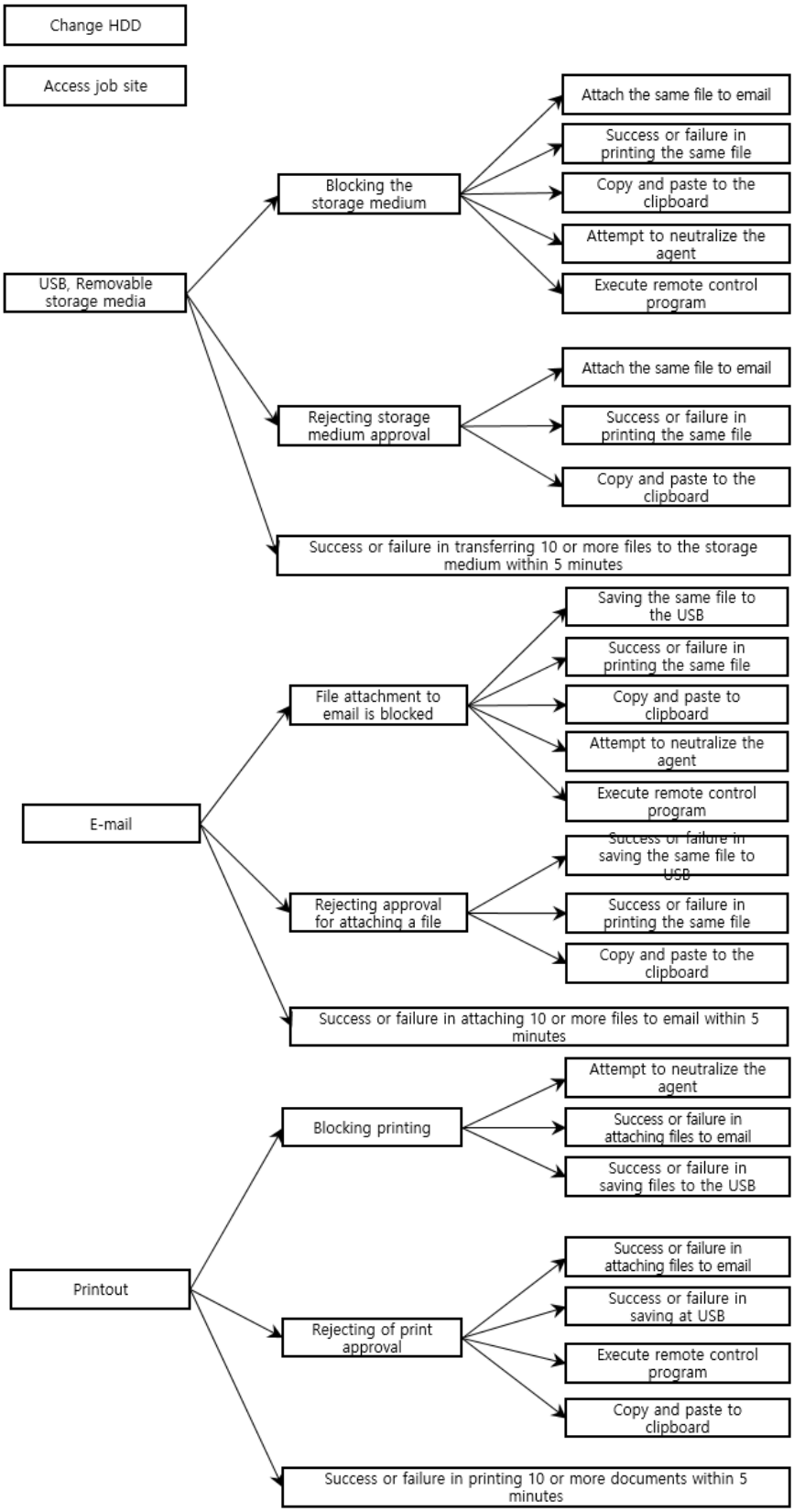

Figure 3. Technology leakage path extraction model diagram
그림 3. 기술유출 경로 추출 모형도

3.2 기술유출사고 유형 분류에 따른 시나리오 탐지 결과 분석

1 년간 중소기업의 내부정보유출방지솔루션에 의해 탐지된 시나리오는 총 28 개의 시나리오 중 15 개의 시나리오에 의해서만 행위가 탐지되었고 총 1,007,266 건을 이상징후로 판단하였다. 이 중에서 가장 많이 탐지된 징후로는 취업사이트 접속에 관한 것이었다. 사내에서의 취업사이트 접속은 단순 인사담당자로서의 업무와 관련된 접속도 있을 수 있지만 그 외 직원들의 이직활동에 관해 미리 동향을 알 수 있고 이를 바탕으로 퇴직예정자들의 중요문서에 관한 반출행위를 보다 면밀하게 들여다볼 수 있기에 유출사고를 사전에 대비할 수 있을 것이라 판단된다.

다음으로 가장 많이 탐지된 시나리오는 이동식 저장매체에 파일을 저장하는 행위가 차단된 후 24 시간 이내 원격제어 프로그램이 PC 에서 실행된 시나리오로써 327,746 건 탐지되었다. 해당 시나리오는 외부에서 사내 PC 로의 원격 접근을 통해 PC 내의 자료에 접근하거나 외부로 반출할 수 있다는 점에서 기술유출 측면에서 고려해야 되는 부분이다.

보안담당자로서 면밀히 모니터링 해야하는 행동패턴 중 세 번째는 이동식 저장매체로 파일 저장이 차단된 후에 PC 내에 설치되어 있는 내부정보유출방지솔루션을 무력화하는 행위로 나타났다. 무력화라함은 내부정보유출방지솔루션을 강제 삭제하는 행위나 프로세스를 강제 종료하려는 행위가 있는 경우를 말한다. 무력화에 성공하게 되면 회사 보안정책으로 차단되어 있던 이동식 저장매체는 다시 활성화가 되며 파일을 저장하는 행위에 대한 로그가 쌓이지 않아 보안담당자는 중요문서의 외부반출에 대해 전혀 확인이 불가한 상황에 놓이게 된다. 28 개 시나리오별 세부적인 탐지건수는 표 2 와 같다.

Table 2. Number of abnormal symptom scenario detections
표 2. 이상징후 시나리오 탐지건수

No.	Contents	Number of detections
1	Change HDD on purpose	0
2	Visit job sites more than 3 times for more than 3 minutes in a week	625,198
3	Attach the same file to email within 24 hours after blocking the storage medium	0
4	Success or failure in printing the same file within 24 hours after blocking the storage medium	1,038
5	Copy and paste to the clipboard within 5 minutes after blocking the storage medium	8
6	Attempt to neutralize the agent within 24 hours after blocking the storage medium	25,967
7	Execute remote control program within 24 hours after blocking the storage medium	327,746
8	Success or failure in attaching the same file via email within 24 hours after rejecting storage medium approval	30
9	Success or failure in printing the same file within 24 hours after rejecting storage medium approval	0
10	Copy and paste clipboard within 1 hour after rejecting storage medium approval	0
11	Success or failure in transferring 10 or more files to the storage medium within 5 minutes	2,344
12	After file attachment to email is blocked, save the same file to the storage medium within 24 hours	2,181
13	Success or failure in printing the same file within 24 hours after blocking file attachment to email	1,776
14	Copy and paste to clipboard within 5 minutes after blocking file attachment to email	113
15	Attempt to neutralize the agent within 24 hours after blocking file attachments to emails	1,893
16	Execute remote control program within 24 hours after blocking file attachment to email	18,433
17	Success or failure in saving the same file to the storage medium within 24 hours after rejecting the approval for attaching a file to email.	0
18	Success or failure in printing the same file within 24 hours after rejecting approval for attaching a file to email.	0
19	Copy and paste to the clipboard within 1 hour after rejecting approval for attaching a file to email.	4
20	Success or failure in attaching 10 or more files to email within 5 minutes	532
21	Attempt to neutralize the agent within 24 hours after blocking printing	0
22	Success or failure in saving 5 or more files to the storage medium within 1 hour after blocking printing	3
23	Success or failure in attaching 5 or more files to email within 1 hour after blocking printing	0
24	Success or failure in attaching file to email within 24 hours after rejecting of print approval	0
25	Success or failure in saving at Storage medium within 24 hours after rejecting of print approval	0
26	Execute remote control program within 24 hours after rejecting of print approval	0
27	Copy and paste to clipboard within 1 hour after rejecting of print approval	0
28	Success or failure in printing 10 or more documents within 5 minutes	0

그렇다면 중소기업의 기술유출 현황에서와 같이 유출수단으로 가장 많이 활용되었던 USB, 이동식 저장매체의 경우 본 연구조사에서도 가장 많이 집계된 유출수단 인자로 나타났는지 분석해보면 본 조사대상 중소기업에서도 동일한 결과값이 나타났다.

Table 3. Number of detections by technology leakage incident type
표 3. 기술유출사고 유형별 탐지건수

Means of leakage	USB, Removable storage media	E-mail	Printout
Number of detections	359,287	24,932	2,817

표 3 에서와 같이 유출수단별 탐지건수는 각각의 유출수단이 단순조건 또는 복합조건으로 들어간 시나리오에 대한 모든 수치를 합산한 것으로 USB 와 관련한 로그가 E-mail 에 비해 14 배 가량 높은 것으로 분석되었다.

IV. 결론

중소기업은 산업기술 유출 사고가 끊이지 않고 있으며 사고의 원인에 대한 개선대책은 매번 발표되고 있지만 현실적으로 중소기업에서 해결방안을 갖추고 대응하기에는 많은 어려움이 있다. 이러한 보안사각지대에서 기술유출 사고가 발생하고 중소기업이 지닌 기술이 산업기술과 영업비밀 사이에서 어떠한 법으로 유출자를 처벌할지 결정해야 하는 가운데 결국 증거수집과 기업의 기술보호에 대한 노력은 법정에서 다뤄지는 중요한 잣대가 되곤 한다.

산업기술은 산기법에서 정의한 산업기술 범주에 들어가거나 '산업기술 확인제도'를 통해 국가가 지정한 첨단기술 또는 신기술의 범주에 들어갈 경우 산기법(산업기술의 유출방지 및 보호에 관한 법률)에 의해 기술을 보호받을 수 있지만 그러지 못한 기술은 부정경쟁방지법(부정경쟁방지 및 영업비밀보호에 관한 법률)에 의해 비공지성, 경제적 유용성, 비밀 관리성을 충족해야지만 법정 소송에서 유리하다.

기업의 기술을 지키기 위해 대기업만큼의 각고의 노력을 중소기업에게 기대할 수는 없지만 기업 스스로 최선의 노력을 다해야 할 것이다. 그것의 일환으로 내부정보유출방지솔루션 구축을 통해 기업의 자료에 대한 모니터링과 통제를 통해 기술보호 체계를 견고히 구축하는 것이 무엇보다 중요하다. 이는 증거수집에 소요되는 시간을 단축시키고 포렌식을 위한 비용을 최소화하여 중소기업이 법적분쟁에 투입되는 피로도를 줄이는데 기여할 수 있을 것이다.

연구과정에서 이상징후 시나리오가 기업 내 중요문서에 대한 행위들을 기술유출로 판단할 수 있는지에 대해 검증을 이행하기는 어려웠지만 기업에서 유심히 지켜봐야할 중요문서에 대한 이상징후 행동패턴들을 도출한 점에서 의의를 찾을 수 있을 것이다. 또한, 기술유출 행위라고 판단할 수 있는 간접적으로 관련이 있는 이상징후 시나리오를 도출한 점에서도 의의가 있다고 볼 수 있을 것이다.

본 연구의 결과값을 통해 기업은 유출사고 유형별 디지털증거들에 대한 관심을 고취시키고 지속적으로 중요문서에 통제 능력을 강화한다면 유출사고를 미연에 방지할 수 있는 위기관리 능력이 함양될 것으로 보이며 유출 사고 발생 시에는 신속한 증거수집으로 법정에서 기술유출이란 악의적인 행위를 증명하는데 일조할 것으로 본다.

그러나 본 연구의 한계로는 이상징후 시나리오가 실제로 발생한 다수의 기술유출 사건의 유출자 행위기반에 근거하여 만들어지지 못하였고, 이에 따라 신뢰가 보장된 기술유출 행위라고 단정하기에는 어려운 점이 있었다. 이러한 한계는 실제 기술유출 사건들의 행위들을 시계열로 나열하여 빅데이터를 확보한 후 기술유출 행위라고 판단할 수 있는 가장 신뢰할만한 결과를 연구할 필요가 있다. 이러한 점은 차후 연구가 필요할 것으로 보인다.

V. 참고문헌

[1] S. M. Lee, B. J. Moon. Determinants of Corporate Core Competencies, Competitive Advantage and

Management Performance : Focused on Small and Medium-size Companies. Journal of management & economics. Vol. 41, 76
[2] G. M. Park. The Design of Digital Forensic Readiness in Smartwork Environment, Master's Thesis. Chung-ang University, 2017.
[3] E. R. Choi, B. G. Song, Y. I. Lee, K. M. Park. A Study on the Leaking Channels of Industrial Technology. Vol. 26, No.1, 231, Mar. 2012
[4] Moneytoday. (2022.2.20). from https://news.mt.co.kr/mtview.php?no=2022021908575039630.
[5] 2022 Survey on the level of technology protection for small and medium-sized enterprises. 344. 2023
[6] H. B. Chang. A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident. Vol. 15, No. 7, 39~45. 2015
[7] H. J. Yang. Case Analysis of Industrial Technology Leakage Crime : Focused on Domestic Portal Site News. Master's Thesis. dissertation, Chung-ang University, 2018.
[8] 2022 Survey on the level of technology protection for small and medium-sized enterprises. 355. 2023
[9] C. Y. Chung. A Research on Countermeasures for Investigation into industrial Technology Leakage Accident by key Personnel. PH. D. Chung-ang University. 2018
[10] The National Police Agency. Rules regarding processing of digital evidence, etc. 2021.8
[11] K. C. Song. A Study on Digital Forensic Readiness for Improving Internal Information Leakage Prevention Technology. Master's Thesis. Dongguk University 2015
[12] S. S. Chun. A Study on Search, Seizure and Admissibility of Digital Evidence in Criminal Procedure. Ph. D.12-16. 2011
[13] K. S. Kim. A Study on the authenticity of Digital Evidence - Focusing on Digital Forensics procedures. Master's Thesis. Yonsei University. 2014
[14] K. S. Kim. A Study on the authenticity of Digital Evidence - Focusing on Digital Forensics procedures. Master's Thesis. Yonsei University. 2014
[15] M. G. Jeon. Collection and Admissibility of Digital Evidence. Korean Law Society. Vol.1, No. 41, 317~336. 2011
[16] K. S. Kim. A Study on the authenticity of Digital Evidence - Focusing on Digital Forensics procedures. Master's Thesis. Yonsei University. 2014
[17] K. S. Kim. A Study on the authenticity of Digital Evidence - Focusing on Digital Forensics procedures. Master's Thesis. Yonsei University. 2014
[18] S. S. Chun. A Study on Search, Seizure and Admissibility of Digital Evidence in Criminal Procedure. Ph. D. 2011

저자소개

왕재윤 (*Jaeyun Wang)*

2008 년~2010 년 ㈜한매기술 정보보안 엔지니어
2011 년~현재 (사)한국산업기술보호협회 팀장

관심분야 : 산업보안, 정보보안, 기술유출 모니터링

장항배 (*Hangbae Chang*)

2007 년~2012 년 대진대학교 경영학과 조교수
2012 년~2013 년 상명대학교 경영학과 조교수
2014 년~현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 정보등급화, 보안데이터분석, 연구보안, 전자폐기물