*한국진로창업경영학회지 ISSN 2586-5242*
*The Journal of Korean Career·Entrepreneurship & Business Association*
*Vol. 7, No. 1, pp. 85-101, Jan. 2023*

http://dx.doi.org/10.48206/kceba.2023.7.1.85

**Received** 20 Dec 2022
**Revised** 10 Jan 2023
**Accepted** 11 Jan 2023

# 중소기업의 기술유출 대응을 위한 디지털 포렌식 개선방안*

권순범**, 김형렬***, 최선영****, 이환수*****

**[국문요약]**

산업기술 유출범죄가 점점 첨단화, 지능화, 고도화되어 감에 따라 경찰은 산업기술 유출방지에 적극적으로 대응하기 위하여 2006년 11월부터 산업기술유출수사대를 조직 및 운영하였고 2017년부터는 17개 모든 지방경찰청에 확장하였다. 이처럼 수사기관은 산업기술 유출 방지를 위하여 노력하고 있지만, 산업기술 유출 사고는 해마다 증가하고 있는 추세이다. 특히, 핵심기술 및 기밀정보에 대한 유출 80%가 전·현직 직원인 내부자에 의해 이루어지고 있으며 내부자 기술유출의 60.8%가 디지털 저장매체를 통해 이뤄지고 있다. 이에 내부정보의 유출 탐지와 신속하고 정확한 디지털 증거 확보를 위해서는 디지털포렌식을 활용한 증거수집이 필요한 상황이지만, 강제조사에 의한 영장청구 준비와 산업보안조사에서의 임의성 확보, 피해기업의 증거확보 미흡 등으로 인해 산업기술 유출범죄에 대한 디지털 증거의 신속한 수집이 어려운 상황이다. 이에 따라 본 연구는 기술유출 수사를 위한 기업의 디지털포렌식 개선방안을 제안한다. 이러한 체계 구축을 위하여 사고 전 준비 단계에서부터 기업 내부의 디지털 기기에 대한 데이터를 백업하여 사고 발생 시 초기 분석 자료로 사용할 것과 사고 발생 시 기술유출 의심자의 디지털 기기에 대한 포렌식 권한을 획득하기 위한 사전 동의를 받아둘 것을 제안한다. 또한, 유출징후를 사전에 포착할 수 있도록 기존의 연구를 토대로 기술유출 징후들을 정리하였으며, 기업의 초기대응 및 증거수집 단계에서부터의 적법성 유지를 통해 향후 생길 법적 분쟁에도 대비할 수 있도록 하였다. 연구 결과는 기술 유출 사고 발생에 대응할 수 있는 기업의 실질적인 가이드라인을 구축하였다는 점에서 의의가 있다.

**핵심주제어 : 기술관리, 기술유출, 디지털포렌식, 디지털 증거, 중소기업**

## Ⅰ. 서 론

기업의 기술력은 국가 경쟁력의 핵심 요인이다(김선욱, 2021). 기술은 패권 경쟁에서 중요한 위치를 차지하며, 현대사회는 기술 변동과 혁신의 속도가 빠르기에 어느 국가도 기술 우위에 대한 확신을 갖기 어렵다(이승주, 2022). 이에 세계 각국의 기술 경쟁과 갈등이 불가피해졌고, 각국은 자국의 산업기술을 보호하고 육성하기 위한 다양한 법과 정책을 강화하고 있다(진재근, 2021). 우리나라 역시 이러한 배경에 따라 국가 경쟁력을 높이고 기술유출을 방지하기 위하여 「산업기술의 유출방지 및 보호에 관한 법률 (이하 '산업기술보호법'이라 칭한다)」을 제정하는 등 다양한 노력을 기울이고 있다(송인옥, 2022; 김

* 본 연구는 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2022년 산업혁신인재성장지원사업)
** 제1저자, 단국대학교 일반대학원 IT법학협동과정 석사과정, kwonsb777@naver.com
*** 제2저자, 단국대학교 일반대학원 IT법학협동과정 학석사연계과정, uwhale3pb@daum.net
**** 제3저자, 단국대학교 일반대학원 IT법학협동과정 박사과정, sunyoung9479@naver.com
***** 교신저자, 단국대학교 산업보안학과 조교수, hanslee992@gmail.com

상화, 2022). 특히, 중소기업과 스타트업의 기술력은 혁신의 원천이 되기 때문에(이은아·서정해, 2017; 박상문·서종현, 2012; 이상무·문병준, 2020) 국가경쟁력 강화를 위해서는 이에 대한 지원 역시 함께 이뤄져야 한다. 이에 따라 〈표 1〉과 같이 중소벤처기업부는 중소기업과 스타트업에 대한 기술개발 지원을 꾸준히 확대하고 있는 상황이다(중소벤처기업부, 2018; 중소벤처기업부, 2019; 중소벤처기업부, 2020; 중소벤처기업부, 2021b; 중소벤처기업부, 2022b). 특히, 2023년에는 총 1조 8,246억 원 규모의 2023년 중소기업 기술개발 지원사업 통합공고를 발표하였다(중소벤처기업부, 2022a). 이는 중소기업과 스타트업의 기술개발 성과를 극대화하고 혁신생태계를 조성하여 국가경쟁력을 강화시키겠다는 정부의 의지를 보여준다.

**<표 1> 연도별 중소기업 기술개발 지원사업 규모**

| 연도 | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| 지원 규모 | 1조839 억원 | 1조744 억원 | 1조488 5억원 | 1조722 9억원 | 1조833 8억원 |

출처: 중소벤처기업부(2018); 중소벤처기업부(2019); 중소벤처기업부(2020); 중소벤처기업부(2021b); 중소벤처기업부(2022b)

이처럼 정부는 국가 경쟁력 강화를 위해 중소기업과 스타트업에 대한 기술개발지원을 집중하고 있지만, 중소기업과 스타트업의 핵심기술이 꾸준히 유출되고 있어 지원의 실효성이 문제되고 있다. 실제로 최근 5년간(2018-2022년) 발생한 총 554건의 기술유출 사건 중 497건(89.7%)이 중소기업에서 발생하였다(경찰청, 2022a; 경찰청, 2022b). 이는 중소기업과 스타트업을 통한 기술유출이 심각한 수준임을 보여준다. 이에 따라 중소기업과 스타트업에 대한 기술개발 지원의 실효성을 높이기 위해서는 기술개발 지원과 함께 기술유출 사고에 대한 대응 체계 구축 역시 함께 이루어져야 한다. 그러나 현재는 중소기업과 스타트업의 기술유출 대응체계가 미흡하여 기술유출에 대한 수사가 어려움을 겪고 있다.

이러한 기술유출 사고 대응 및 수사를 어렵게 하는 요인 중 하나는 디지털 증거다. 정보통신기술과 기기의 발달로 디지털화가 촉진되었고(김영철·구희진, 2021), 핵심기술의 유출 또한 디지털 기기를 통해 이루어지는 경우가 많아 디지털 증거에 대한 확보가 중요해지게 되었다(강구민·이재철·김창범, 2021). 그러나 디지털 증거의 방대한 분석량과 부족한 수사 인력으로 인해 기술유출 수사는 여전히 많은 어려움을 겪고 있다. 김승용·정제용(2019)의 연구에 따르면, 기술유출사건 1건당 평균 소요 시간이 약 1,700시간인 것으로 나타났으며 1일 8시간 기준으로 했을 때 7개월이 소요되는 것으로 분석되었다. 즉, 신속성을 요하는 기술유출 사건의 수사가 여러 현실적인 이유들로 인해 지연되고 있다.

또한, 최근 기업의 핵심기술 및 기밀정보에 대한 유출 80%가 전·현직 직원인 내부자에 의해 이루어지고 있으며(박현출·박진상·김정덕, 2020). 내부자 기술유출 60.8%가 디지털 저장매체를 통하여 이뤄지고 있는 점을 살펴봤을 때(이장욱, 2020), 디지털포렌식을 활용한 내부정보 유출 탐지는 필수적이다. 게다가, 향후에도 디지털 저장매체를 통한 내부자 유출 사례가 증가할 것으로 예상되는데, 디지털포렌식은 디지털 저장매체를 통한 기술유출 사건 발생 시 디지털 증거에 대한 자료수집이 즉각적으로 가능하다는 점에서 피해 기업의 피해회복을 위한 최선의 방법이 될 수 있다(강구민·이재철·김창범, 2021).

그러나 디지털포렌식의 대상인 디지털 증거는 비가시성, 변조 가능성, 복제 용이성, 휘발성의 특징을 갖추고 있기 때문에 최초 증거 수집에서부터 분석 및 보관까지의 매체별 특성에 맞는 적절한 조치가 요구되며, 디지털포렌식을 통한 디지털 증거의 수집은 일반적인 증거물에 적용되는 법률 절차 외에도 디지털매체라는 특수성으로 인해 추가적인 조치가 필요하다(이정호 외, 2022). 이에 내부정보의 유출 탐지와 신속하고 정확한 디지털 증거 확보를 위해서는 디지털포렌식을 활용한 증거수집이 필요한 상황이지만, 강제조사에 의한 영장청구 준비와 산업보안조사에서의 임의성 확보 같은 문제로 인해 산업기술 유출범죄에 대한 디지털 증거의 신속한 수집이 어려운 상황이다. 또한, 빠른 사건 해결을 위해서는 수사기관뿐만 아니라 기업 내부에서 기술유출 사고에 대응한 디지털포렌식 대응방안을 마련할 필요가 있지만, 중소기업와 스타트업의 경우 보안수준이 열약할 뿐만 아니라(조하나·하리다·이환수, 2021) 기술유출 대응에 대한 경험 역시 부족해 이에 대한 절차 역시 익숙하지 않은 상황이다. 이에 따라 기업의 기술유출 사고 대응을 위한 디지털포렌식 절차에 대한 공개적인 논의와 학술적 가이드라인이 필요한 상황이지만, 기업의 경영관점에서의 학술적 논의는 부족한 상황이다.

따라서 본 연구는 기술유출 대응을 위한 기업의 디지털포렌식 개선방안을 제안하여 신속하고 정확한 디지털 증거 확보에 기여하는 것을 목적으로 한다. 이를 위해 본 연구는 디지털포렌식에 대한 문헌연구와 기술유출 사고 발생 시 이뤄지는 디지털 포렌식 절차에 대한 문제점을 분석하고 이를 토대로 개선방안을 제시한다. 이를 통해 중소기업

이나 디지털포렌식이 용이하지 않은 기업들이 기술유출사고에 효과적으로 대응할 수 있을 것이다.

# Ⅱ. 디지털포렌식

## 2.1 디지털포렌식의 개념

포렌식은 법의학 분야에서 주로 사용하던 개념이었으나, 최근 다양한 정보기기의 활용으로 포렌식 개념은 물리적 형태의 증거뿐만 아니라 특수매체에 저장된 전자적 증거를 다루는 분야에서도 활용되고 있다(김면기·유승진, 2019). 디지털포렌식은 디지털 기기에 저장된 데이터를 수집하고 분석하여 범죄 수사를 위한 단서나 증거를 찾는 분석 기법이다(윤우성·한재혁·이상진, 2019). 디지털포렌식은 디지털 증거를 대상으로 하며(정진효·이창무, 2017). 이러한 디지털 증거는 범죄사실을 규명하여 법정에서 혐의를 입증하는데 핵심적인 역할을 한다(남기욱·이상진, 2021).

이에 디지털 증거의 수집과 분석을 위해 디지털 저장 기기의 특성 및 종류, 상태에 따라 필요한 디지털포렌식 도구들이 사용되고 있다. 국내외에 널리 상용화되어 활용되고 있는 디지털포렌식 도구로는 Guidance Software의 Encase와 AccessData의 FTK, ILook Investigate v8, Microsoft의 COFEE 등이 있으며, 그 외에 오픈소스 형태의 디지털포렌식 도구들도 많이 제공되고 있다(이태림·신상욱, 2011). 이와 같은 포렌식 도구들은 분석 대상이 되는 디지털 저장매체와 저장매체 상태에 따라 구분되어 사용된다. 우선 디지텉 저장매체에 따라 디지털포렌식 방식은 “디스크 포렌식”, “데이터베이스 포렌식”, “시스템 포렌식”, “네트워크 포렌식”으로 구분된다. 디스크 포렌식은 물리적인 저장장치(HDD, 플로피디스크 등)에서 증거수집 후 분석하는 것을 의미하며, 데이터베이스 포렌식이란 데이터베이스에 저장·은닉·삭제되어 있는 데이터 등을 복원과 같은 방법으로 디지털 증거를 분석하는 포렌식 방식을 의미한다(이규안, 2010). 그리고 시스템 포렌식이란 증거를 확보하기 위해 컴퓨터의 OS(운영체제)와 응용 프로그램 등을 분석하는 포렌식 방식이다. 마지막으로 네트워크 포렌식은 특정 도구를 활용해 네트워크상으로 전송되고 있는 암호 또는 데이터 등을 가로채거나 서버 내에 로그 형태로 저장되어 있는 것에 접근하여 분석·조사해 단서를 발견하는 포렌식 방식이다(전상덕·홍동숙·한기준, 2006).

한편, 디지털포렌식 방식은 기기 상태에 따라 “활성 포렌식”과 “비활성 포렌식”으로 구분할 수 있다. 활성 포렌식은 윈도우와 macOS에서 활용할 수 있고(정지용 외, 2019), 시스템이 활성화 되어 있는 상태에서 정보를 모으는 행위를 의미하며 주로 컴퓨터를 종료 할 경우에 삭제가 되는 휘발성의 증거를 수집 할 때에 사용하는 방식이다. 비활성 포렌식은 OS(운영체제)가 종료되어있는 상태의 컴퓨터 또는 휴대전화 등의 기기에서 정보를 수집하는 방식이다. 주로 컴퓨터 포렌식, 모바일 포렌식, 악성코드 포렌식 시 사용되며, HDD(하드 디스크 드라이브)나 플래시 메모리에서 데이터를 수집하여 분석한다(박종욱, 2020; 이규안, 2010). 이처럼 디지털포렌식에는 다양한 도구와 방식이 활용되며, 각각의 상황에 맞게 필요한 도구와 방식을 사용하는 것이 중요하다.

## 2.2 중소기업과 디지털포렌식

중소기업과 스타트업에서의 기술은 기업의 자본력 및 경영과 직결된다(이준원, 2021). 중소기업과 스타트업은 자본이 부족하여 자체 개발한 기술을 활용하여 융자 또는 투자를 받아 사업을 이어 나가는 경우가 많기 때문이다(김성원·박현애·이환수, 2020). 이처럼 기술이 중요한 중소기업과 스타트업의 지속 가능한 경영을 위해서는 기술 유출을 사전에 예방하는 것이 중요하지만(최선영·정지원, 2022), 예상치 못한 기술유출로 인한 피해가 발생하였을 때에는 빠른 피해회복을 위해 노력하여야 한다. 이를 위해서는 기술 유출 사고 발생 시 관련 증거를 신속히 수집하는 것이 중요하다.

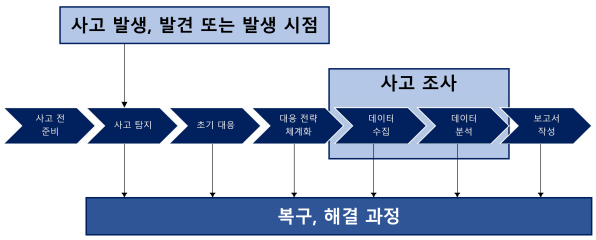
최근 기술유출 사건의 특성상 디지털포렌식을 통한 증거수집이 중요해지고 있다. 특히, 산업기술 및 기업의 핵심정보는 대부분 전·현직 임직원에 의하여 유출되고 있으며, 스마트폰·클라우드와 같은 다양한 디지털 저장매체를 활용하여 유출되고 있다(박찬수·강민지·최이중, 2019). 실제로 디지털 저장매체를 통한 기술 유출 사건은 2018년부터 2022년까지 117건, 112건, 135건, 89건, 101건으로, 매년 100건 가량 꾸준히 발생하고 있다(경찰청, 2022a; 경찰청, 2022b). 실례로 2011년에 포렌식을 통해, 삼성의 AMOLED TV 제조 기술을 중국으로 빼돌리려던 연구원 아내 명의의 이메일에서 증거를 잡아 기술 유출을 시도하던 연구원을 검거한 사건이 있었다. 당시 기술유출자는 검거 중 증거인멸을 위해 노트북을 파손하였으나, 수사기관은 디지털포렌식 기법을 활용하여 하드디스크를 복원해 증거를 확보하여 이를 통해 통화내역·메신저·이메일 기록 등을 확인하여 유출 여부를 파악할 수 있었다(최순웅, 2011). 이처럼 디지털포렌식은 물리적으로 파손된 디지털

저장매체를 복원하여 증거를 확보할 수 있다. 따라서 물리적 증거인멸이 용이하고, 손쉽게 증거의 변조가 가능한 디지털 저장매체를 통한 기술 유출 사건에서는 디지털포렌식을 활용한 복원, 분석이 중요하다.

# Ⅲ. 기술유출 사고와 디지털포렌식

## 3.1 기술 유출 사고에서 디지털포렌식 절차

포렌식 절차는 보안사고 발생 이후 이를 조사하여 향후 동일한 사고가 발생하지 않도록 취하는 조치이며, 사고 분석자가 취해야 하는 단계별 분석 절차다(김태훈 외, 2009). 한국인터넷진흥원(Korea Information Security Agency; KISA)에서 발표한 “침해사고 분석절차 안내서”는 보안사고와 포렌식에 대한 가이드라인을 제시하고 있다. 절차는 〈그림 1〉과 같이 7가지 대응 요소로 구성되어 있다(한국인터넷진흥원, 2010).



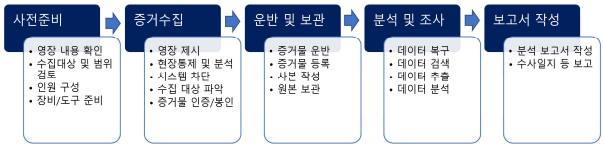

<그림 1> 침해사고 대응 7단계

KISA의 보안사고 대응 절차는 보안사고 발생 이후 사고 대응 절차로써 유용한 체계이지만, 사고 발생 이후에서야 포렌식 분석에 대한 대응이 시작된다는 점에서 디지털 증거의 신속한 수집에는 어려움이 있다. 신속한 증거수집이 중요한 이유는 시간이 지날수록 증거가 위·변조될 위험이 커져, 입증에 많은 어려움이 생기기 때문이다. 실제로 기술 유출 사고 발생 시 피해기업은 기술유출 주체에 대해서 법적 대응, 수사 의뢰, 행정구제 신청, 당사자간 합의 노력 등 외부적인 조치를 할 수 있음에도, 42.9%는 별도의 조치가 취하지 않은 것으로 나타났다. 이에 대해 별도의 조치를 하지 않은 이유는 ‘증거 등의 입증자료 부족(50%)’ 때문인 것으로 나타났다(중소벤처기업부, 2021a). 즉, 현재는 기술유출사고 발생 시 디지털 증거 확보에 많은 어려움이 있으며, 이는 피해기업의 피해회복을 어렵게 하고 있음을 알 수 있다.

## 3.2 기술 유출 사고에서의 한계점

### 3.2.1 강제조사에 의한 신속성 부족

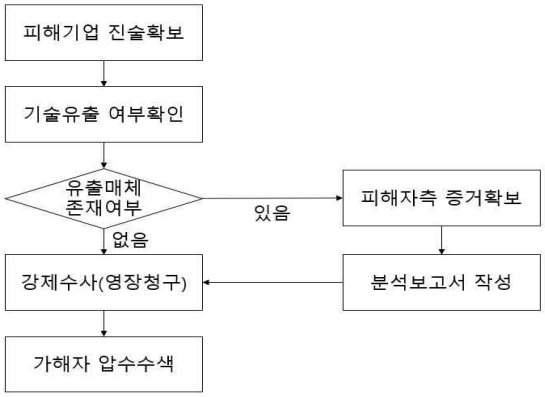
강제조사에 의한 디지털포렌식 절차는 다음과 같다. 이창훈(2011)과 노명선·백명훈(2016)의 연구를 토대로 작성한 디지털포렌식을 통한 디지털 증거 압수·수색 절차는 〈그림 2〉와 같이 5단계를 거쳐 진행된다.




<그림 2> 디지털 증거의 압수·수색 절차

〈그림 3〉과 같이 기술유출사건은 일반적인 수사와 달리 피해자 조사와 가해자 조사를 하는 두 번의 포렌식 절차를 거쳐야 한다. 특히, 피해자 조사단계에서는 압수·수색보다는 임의제출 형태로 입증자료를 제출받아야 하는데, 대부분의 피해기업은 갑작스러운 기술유출에 입증자료를 준비하는데 많은 시간과 노력이 요구된다. 또한, 디지털포렌식을 통한 피해기업에 대한 선행조사는 이미징과 해시값 확보를 통한 정당성 확보가 중요하다(이금녀, 2013). 디지털 증거는 조작이 용이하다는 특성을 가지고 있어 분석자가 마음대로 조작하기 쉽기 때문이다. 이에 디지털 증거가 법원에서 법적 증거능력을 인정받기 위해서는 증거수집 단계인 이미징 단계에서의 해시값 관리가 중요하다. 이미징(Imaging)은 저장매체의 원본을 복제하여 사본으로 만드는 과정이며(전상준, 2016), 해시(Hash)는 전자지문이라고도 불리며 파일을 생성하면 발생하는 전자값이다(김종호, 2019). 해시값은 원본과 사본의 무결성 관리에 있어 핵심적인 역할을 한다.

이처럼 기술유출 사건에서의 증거확보를 위해서는 초기 대응에 많은 시간과 노력이 필요하며 증거가 조작되지 않도록 절차의 연속성을 지키는 것이 중요하다. 또한, 강제수사를 위한 영장 청구를 위해서는 디지털 증거가 사라지기 전에 이에 대한 증거를 확보하는 것이 중요한데 피해기업의 적극적인 협조 없이는 증거수집이 어려운 상황이다. 이에 신속한 영장청구를 바탕으로 압수·수색을 시행하기 위해서는 기술유출 상황에 대비한 기업의 디지털포렌식 관리 절차 구축이 필수적이지만, 이에 대한 체계적인 절차 구축은 여전히 부족하다고 할 수 있다.




**<그림 3> 기술유출사건의 디지털포렌식 분석 절차**

### 3.2.2 임의성 확보의 어려움

산업보안조사란 산업기술과 국가핵심기술에 관련된 비밀이 직접 또는 간접적으로 유출되는 것을 미리 방지하거나 기술이 유출된 경우에 추가적인 기술유출의 차단과 원상회복을 하기 위해 종합적 대책과 전략에 필요한 조사를 의미한다(한국산업보안연구학회, 2020). 산업기술 유출사고에 있어 산업보안조사는 임의조사로써 조사의 임의성을 준수하면서 조사를 진행한다(강구민·이재철·김창범, 2021). 산업보안조사에서의 디지털포렌식 조사에 대하여 현재는 법령에 산업보안조사에서의 디지털포렌식 조사의 절차와 방법에 관해 규정되어 있지 않다(김무석·강구민, 2022). 그러나 디지털포렌식의 주체는 다르나 공정거래위원회, 경찰 등에서 정하고 있는 표준적인 디지털포렌식 절차는 존재한다(한국산업보안연구학회, 2020). 따라서 산업보안조사에 대한 디지털포렌식 절차는 이에 준용하여 설명 가능하다.

우선 산업보안조사는 본격적인 조사에 들어가기 전에 디지털포렌식과 관련된 장소, 네트워크 시스템 등의 사전 정보를 파악하여 조사 계획을 수립하고, 사전 조사팀을 구성하고, 디지털포렌식 과정에 참여할 대상자와 참여권자를 파악하여야 한다. 이후에 현장조사가 시작되고, 현장조사 시에는 현장 전체의 모습을 촬영 녹화하고 디지털포렌식 준비를 착수하고, 참여권을 보장하고 고지해주는 것이 중요하다. 그리고 디지털포렌식을 진행함에 있어 가장 중요한 것은 '임의성'을 확보하는 것이다. 산업보안조사에서 임의성을 확보하기 위해서는 대상자가 자발적 동의에 의해 조사기관에 해당 디지털 기기를 제출하여야 하며, 임의성 여부는 행정조사기관이 대상자의 임의적 제출 의사를 입증하여야 한다(강구민·이재철·김창범, 2021). 만일 대상자가 강제로 디지털 기기를 제출하게 하는 등 임의성을 인정받을 수 없을 때에는 해당 증거들은 증거능력을 인정받을 수 없다. 따라서 산업보안조사에서는 원칙적으로 피조사자에게 침해사실에 대해 인터뷰하거나 관련 자료들을 제출받아 조사한다. 이후, 조사 현장에서 수집한 증거와 디지털 기기에 대하여 디지털 증거분석관에게 증거 분석을 의뢰하여야 한다. 이때 주의하여야 하는 점은 조사원과 증거분석관은 증거물의 무결성과 연계보관성을 유지하여야 하는 것이다. 마지막으로 증거분석관은 분석을 종료한 때에는 지체 없이 디지털 증거분석결과 보고서를 작성하여야 한다.

헌법 및 형사소송법의 영장주의 적용을 받는 강제조사와 달리 산업보안조사는 영장주의의 적용을 받지 않으며, 디지털포렌식에 대한 당사자의 동의만 있으면 법관이 발부하는 영장의 엄격한 제한 조건에서 자유롭고, 변호인의 참여권 등을 거치지 않아도 된다는 점에서 강제조사보다 자료획득이 용이하며 효율적인 장점이 있다(홍지은, 2020). 즉, 산업보안조사에서의 디지털포렌식은 영장청구에 대한 준비과정을 거치지 않아도 되어서 신속한 조사가 가능하다는 장점이 있으나, 조사대상자의 자발적인 동의를 받기 어렵다는 점에 한계가 있다.

### 3.2.3 안티포렌식에 의한 증거조작

안티포렌식의 개념은 다양하게 정의가능하다. 안티포렌식의 개념에 대하여 조균희(2006)는 "컴퓨터 포렌식 기법에 대항하여 디지털 증거를 최소화하고 수사를 회피하기 위한 방법론"이라고 정의하였고, 이석희 외(2008)는 "디지털포렌식에 의한 증거 발견을 어렵게 하는 기술"이라 정의하였다. 즉, 안티포렌식은 범죄수사에 대비하여 고의적으로 디지털 증거를 훼손하는 행위라 정의할 수 있다(윤지수·이경열, 2021). 안티포렌식은 다양한 방식으로 이뤄지고 있다. 전통적인 안티포렌식은 데이터의 삭제 및 파괴, 데이터 은닉, 데이터 위·변조 등의 기법을 통해 이루어졌으나, 최근에는 디지털포렌식 기술이 발전함에 따라 데이터 복구 가능성을 저해하거나 데이터의 수집을 방해하는 등으로 디지털포렌식을 어렵게 하는 신종 유형의 안티포렌식들도 등장하기 시작하였다(윤지수·이경열, 2021). 이처럼 최근에는 다양한 안티포렌식 기법들이 나타나고 있으며 증거물의 획득 및 추적을 원천적으로 막아주는 전문 제품들이 많이 등장하고 있으며, 이에 따라 기술유출 수사나 조사를 방해할 수 있는 안티포렌식에 대한 대응이 중요해지고 있다(신원, 2014).

### 3.2.4 디지털 증거의 방대한 분석량

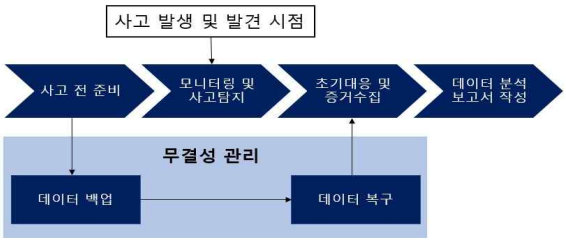
현재 일반적으로 사용되는 PC의 용량은 500GB에서 3TB이며, 1TB 디스크 기준으로 이미지 처리 시간은 2시간 44분, 분석 시간은 8시간이 걸리는 것으로 나타난다. 즉, 2TB와 3TB 디스크의 이미지 처리와 분석 시간의 총합은 약 22시간, 41시간 걸리는 것으로 나타나, 분석 대상 용량이 커질수록 이미지 처리와 분석에 걸리는 시간은 급격하게 증가할 것으로 예상된다(김민수, 2018). 그러나 현행 형사소송법에 명시된 압수·수색 영장 청구 제한 시간은 48시간이며, PC뿐만 아니라 다른 디지털 기기에 대한 증거수집도 함께 이뤄져야 한다는 점을 고려해보면 제한 시간 내에 모든 자료를 압수·수색하기에는 힘든 상황이다. 또한, 압수·수색에 성공한다고 하더라도 초기의 기초적인 분석자료 없이는 방대한 양을 가지고 있는 디지털 증거의 특성상 분석 기간이 길어질 수밖에 없는 상황이다. 따라서 기술유출사건에 대비한 백업 데이터 확보가 중요한 상황이다.

# Ⅳ. 개선방안

## 4.1 디지털포렌식 절차의 개선방안

신속한 증거수집을 바탕으로 한 빠른 사건 해결을 위해서는 수사기관뿐만 아니라 기업 내부에서부터 기술유출 사고에 대한 대응 체계 구축이 필요하다. 이에 본 연구는 KISA의 보안사고 대응 절차를 수정하여 기업의 기술유출 사고 대응을 위한 디지털포렌식 개선방안을 제시한다.

KISA는 국내의 다양한 침해사고를 대응하는 정부기관으로 KISA의 보안사고 대응 절차는 국내의 전문가들이 검증한 가이드라인이다. 다만, KISA의 보안사고 대응 절차는 사고 발생 이후에서야 디지털포렌식 분석에 대한 대응이 시작된다는 점에서 디지털 증거의 신속한 수집에는 어려움이 있었다. 이에 본 연구는 기업의 기술유출 대응을 위해 KISA 보안사고 대응 절차를 디지털 증거 확보에 용이하게 절차를 수정하였다. 모델의 전체적인 흐름은 〈그림 4〉와 같으며, 본 모델은 신속한 사실관계 파악과 기업의 조기 대응을 통한 포렌식 데이터 수집과 분석이 용이하도록 구성되어 있다.




**<그림 4> 제안 디지털포렌식 흐름도**

### 4.1.1 사고 전 준비

#### 4.1.1.1 사전 동의

디지털포렌식은 민사 또는 형사소송에 대한 법적 대응이 요구될 때 필요한 기술 중의 하나다. 이에, 기업은 디지털포렌식의 법령준수 위반 사항을 조기에 파악하고 방지하는 내부통제 절차를 확보할 필요가 있다(김종호, 2019). 사고 전 준비 절차에서 가장 중요한 것은 사고 발생에 대비하여 디지털포렌식에 대한 사전동의를 받아두는 것이다. 만일, 자신이 기술유출자로 의심되었을 경우 자신의 디지털 기기에 대한 포렌식 조사에 대한 동의를 전적으로 하여야 한다. 다만, 디지털포렌식은 디지털매체에 저장된 범죄 흔적뿐만 아니라 금융정보, 의료정보 등 사건과는 무관한 개인정보도 수집될 수 있다는 특성을 가지고 있고(이건희, 2021), 이는 향후 또 다른 법적 문제점을 야기할 수 있기 때문에 기업 내부에서 자체적으로 디지털포렌식의 목적과 방법에 대한 제한도 함께 이뤄져야 한다.

#### 4.1.1.2 실시간 백업

다음으로, 사고 발생 후의 신속한 초기대응을 위해서는 기업 내 연구원의 디지털 기기에 대한 실시간 데이터 백업이 이뤄져야 한다. 데이터 수집 시 이미징과 무결성 확보 절차에 많은 시간이 소요되는데 사고 전부터 이러한 데이터를 실시간으로 백업하고 무결성을 관리한다면 사고 발생 시 많은 시간을 절약하고 신속한 사실관계 파악이 이뤄질 수 있기 때문이다(김태훈 외, 2009). 다만, 디지털 증거는 쉽게 오염될 우려가 있기에 무결성을 유지하기 위한 기술적, 관리적 조치가 함께 취해져야 하며, 시설과 설비 기기 그리고 증거 관리 감독에 대한 체계적인 평가도 함께 이루어질 필요가 있다(권양섭, 2021).

### 4.1.2 모니터링 및 사고탐지

기술유출 혐의에 대한 디지털 증거 확보를 위해서는 기술유출 행위에 대한 빠른 발견이 중요하다. 일반적으로 기업들은 기밀자료나 영업비밀이 유출된 후 3개월 이내에 관련 사실을 인지하는데, 이럴 경우 기술 유출자는 그 기간 내에 증거를 인멸하고 해외로 도피하는 경우가 많기 때문이다. 따라서 기술유출자에 대한 빠른 대처와 유죄 입증을 위해서는 빠른 시간 내에 혐의를 발견하는 것이 중요하다(한국산업보안연구학회, 2020).

사고탐지는 이상 행위에 대한 탐지가 중요하다. 기술유출 행위는 보안 프로그램을 강제 종료하거나 안티포렌식 프로그램을 설치하는 등의 비정상 행위에서부터 시작하기 때문이다. 이에, 김현수(2017)와 김재수 외(2019)의 연구를 토대로 기술유출 징후에 대한 유형화를 시도하였다. 이에 따라 설정한 기술유출 징후는 〈표 2〉와 같으며, 사고탐지 절차에서는 이에 대한 행위를 사전에 파악하여 조사대상자를 선별하고 포렌식이 진행될 수 있도록 하는 것이 중요하다.

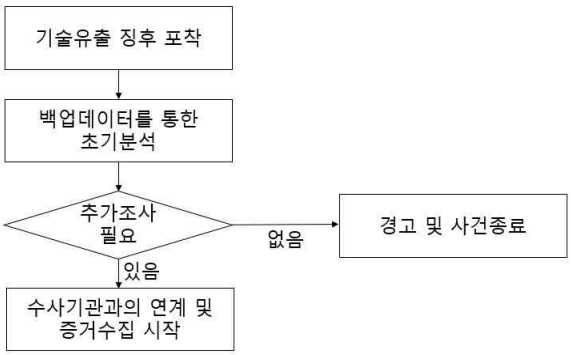
**<표 2> 기술유출 징후 탐지 항목**

| 행위 유형 | 세부사항 |
|---|---|
| 조직 내 PC단말 조작(설치)를 통한 유출징후 | 운영체제 설정환경 변경(재설치), 내부IP주소 변경, 보안프로그램 강제종료, 불법 SW 설치, 안티포렌식 SW 설치 등 |
| 중요문서의 조작을 통한 유출징후 | 중요문서 암호화 해제, 중요문서 워터마크 해제, 중요문서 복사, 중요문서 출력, 중요문서 파일명 변경, 중요문서 확장자 변경 등 |
| 외부로부터 접속을 통한 유출징후 | 허가되지 않은 외부에서 내부서버 접속(VPN/FTP) 등 |
| 전자메일을 통한 유출징후 | 외부 메신저 사용, 다른 사용자 컴퓨터에서 전자메일 송부, 중요파일 첨부, 기준크기 이상의 파일전송 등 |
| 불법접속을 통한 유출징후 | 비허가 사이트(정보교환 사이트 등)접속, 외부 저장공간(사이트) 접속 |
| 저장매체를 통한 유출징후 | 허가되지 않은 이동형 저장장치(USB/HDD) 연결, 스마트폰 저장장치로 연결, 기기(노트북/저장장치)임의 반출 등 |

출처: 김현수(2017); 김재수 외(2019)

### 4.1.3 초기대응 및 증거수집

〈그림 5〉와 같이 모니터링 및 사고탐지 단계에서 기술유출 징후가 포착되면 백업데이터를 통한 초기분석이 이뤄져야 한다. 이를 통해, 추가조사가 필요한지 여부를 신속하게 결정한 후 필요성이 있다면 수사기관과의 연계 및 증거수집 단계로 넘어가야 하며, 필요성이 없다면 의심 행위자에 대한 경고와 사건을 조기 종료하게 된다. 추가조사의 필요성이 발생했다면, 수사기관에는 백업데이터를 통한 초기분석 자료를 넘겨주는 동시에 기업 내부에서는 초기대응을 위한 증거수집을 함께 진행하여야 한다.




**<그림 5> 초기대응 및 증거수집 절차 제안 흐름도**

디지털 기기에 대한 초기 증거수집은 범죄혐의 입증에 있어 중요한 역할을 하며, 다수의 사건에서 디지털 증거는 범행 입증을 위한 핵심 증거로 채택되고 있다(권양섭, 2021). 그러나 변조되거나 삭제되기 쉬운 디지털 증거의 특성상 디지털 증거는 엄격한 증거능력 요건이 요구되며, 무결성 등이 확보되지 않은 디지털 증거는 증거능력의 효력을 잃게 된다(김영준·김완주·임재성, 2020). 이에 초기대응 시점에는 향후 생길 법적분쟁과 정확한 사실관계 파악을 위해 무결성 등의 기본원칙을 준수하여 데이터를 수집하는 것이 중요하다.

디지털 증거 수집을 위한 가이드라인 구축을 위해서는 기존 디지털포렌식 매뉴얼들을 분석할 필요가 있다. 경찰청은 「디지털 증거 수집 및 처리등에 관한 규칙」,「현장 수사관을 위한 디지털 증거압수·수색 길라잡이」, 「디지털 증거처리 표준 가이드라인」을 표준규정으로 두고 있으며, 검찰청은 「디지털포렌식 수사관의 증거 수집 및 분석 규정」, 「디지털포렌식 압수지원 절차에 관한 지침」, 「전국 디지털 수사망 운영지침」, 「과학수사 실무매뉴얼」 등을 두고 있다(정진효·이창무, 2017). 그러나 검찰청과 경찰청의 가이드라인은 압수·수색 절차에서의 행동 지침에 초점을 맞추고 있기에, 기업의 디지털포렌식 절차에 대입하기에는 무리가 있다. 이에 한국정보통신기술협회(Telecommunication Technology Association; TTA)의 디지털 증거 수집보존 가이드라인을 바탕으로 초기대응 및 증거수집 시 필요한 사항들을 정립해보았다.

우선, 사고 전 준비 단계에서 받았던 디지털포렌식에 대

한 사전 동의서를 바탕으로 기술 유출의심자의 디지털 기기 제출을 요청하고 기업 내부에서는 기술유출 의심자가 사용하던 디지털 기기에 대한 증거수집이 함께 이뤄져야 한다. 특히, 기업 내부에서는 기술유출 의심자가 있었던 현장 모든 사람들의 컴퓨터 작업을 중단시키고 현장을 장악하는 등의 신속한 조치가 필요하다(정진홍, 2010). 예를 들면, 수집 대상의 전반적인 모습과 주변장치를 포함한 모든 현장을 촬영하고, 증거수집 권한에 따라 수집대상을 구분하고 권한 외의 디지털 기기에 대해서는 수집을 배제하는 등 향후 생길 법적 분쟁에 대비하여 디지털 증거를 수집하는 것이 중요하다. 이에 대한 구체적인 가이드라인은 〈표 3〉과 같다(한국정보통신기술협회, 2017).

**<표 3> 기업 내부 현장조사 가이드라인**

| 단계별 행위 | 세부사항 |
|---|---|
| 사진 촬영 및 현장 스케치 | 수집 대상의 전반적인 모습과 모든 현장을 촬영한다. 수집 대상의 위치를 촬영으로 기록하며, 현장을 스케치 한다. |
| 수집 대상 식별 및 수색 | 디지털 증거 수집 권한에 따라 수집대상을 구분 한 뒤 권한 외의 디지털 기기에 대해서는 수집을 배제한다. |
| 휘발성 데이터 수집 | 휘발성 데이터는 사건에 있어 중요한 단서가 되는 경우가 있으므로, 휘발성 데이터 확보가 가능하다면 이에 대한 증거부터 수집을 시작한다. |
| 디지털 기기의 전원 차단 | 수집 대상의 전원이 꺼져 있다면 디지털 저장 매체 수집을 진행하며, 켜져 있는 경우에는 시스템 운영체제와 종류에 따라 전원분리방법을 결정하여 진행한다. |
| 디지털 증거 수집 | 수집 대상의 전원 차단을 완료한 이후 네트워크 및 전원 케이블 연결을 해제하고 기타 장치들을 분리한다. 수집 대상에서 직접 디지털 증거를 수집하는 경우 쓰기방지장치 및 수집 대상에서 디지털 저장 매체를 분리하여 디지털포렌식 장비를 이용하여 디지털 증거를 수집한다. |
| 원본성 확보 (해시함수 이용) | 수집한 디지털 증거 목록을 관계자에게 전달하고 사건 관계자 또는 제3의 참여자로부터 확인서 및 목록에 서명 또는 날인을 받는다. 디지털 저장 매체의 복제본을 생성할 경우에는 원본과 복제본의 해시값을 확인하고 이에 대하여 사건 관계자 또는 제3의 참여자에게 확인을 받는다. |
| 디지털 증거물 포장, 상세정보 기재 | 수집한 디지털 증거물은 충격, 전파 등으로부터 보호될 수 있는 박스를 사용하여 개별 포장하여 상세 정보를 기록하여 부착한다. |

출처: 한국정보통신기술협회(2017)

### 4.1.4 데이터 분석 및 보고서 작성

수집된 포렌식 데이터 분석은 언제, 누가, 어떻게 사고를 발생시켰는지 분석하는 단계이며, 수집된 모든 정보의 전반적인 조사를 하는 단계이다(김태훈 외, 2009). 디지털 포렌식에 의한 분석 결과는 이벤트 정보와 기록 정보로 구분 가능하며, 이벤트 정보와 기록 정보를 육하원칙에 따라 가공하여 사용자의 행동유형과 타임라인에 초점을 맞추어 분석 결과를 도출하는 것이 중요하다(윤우성·한재혁·이상진, 2019). 또한, 보고서를 읽을 상급자나 소송 관계자들을 위해 누구나 알기 쉽게 보고서를 작성하는 것이 중요하다. 이에 데이터 획득, 보관, 분석 등의 과정을 명백하고 객관적으로 육하원칙에 따라 서술하고, 사건의 세부 사항을 정확하게 기술하여 재판 과정에서 발생할 수 있는 논쟁에 대응할 수 있도록 하는 것이 중요하다(한국인터넷진흥원, 2010).

## 4.2 기대효과

### 4.2.1 사전동의를 통한 증거능력 확보

기술유출사고 발생 시 피해기업의 피해 최소화와 빠른 피해복구를 위해서는 신속한 사실관계 파악이 중요하다(정점영 외, 2021). 디지털포렌식은 기술유출사건 발생 시 디지털 증거에 대한 자료수집이 즉각적으로 가능하다는 점에서 피해기업의 피해회복을 위한 최선의 방법이 될 수 있지만(강구민·이재철·김창범, 2021), 압수·수색에서의 영장 청구 절차와 산업보안조사에서의 임의성 확보같은 절차상의 문제로 인해 신속한 디지털포렌식이 불가능한 실정이다. 즉, 영장청구를 위한 준비와 산업보안조사에서의 임의성 확보 같은 문제를 해결하기 위해서는 피해기업의 적극적인 협조가 중요한 상황이다. 이에 기업 내부의 자체적인 포렌식 조사가 중요하지만, 기업 자체의 내부 조사에 의한 포렌식이라 하더라도 포렌식 대상자의 동의 없이 이루어진 증거는 이를 토대로 영장에 의한 강제조사나 산업보안조사에 의해 최종적으로 법원에 가더라도 증거능력 인정에 문제가 발생할 수 있다. 이에, 포렌식 대상자의 사전동의를 받는 것이 중요하며, 사고 전 준비 단계에서부터 포렌식 대상자에 대한 사전동의를 통해 신속한 사실관계 파악과 향후 생길 법적 분쟁에서의 증거능력 확보에 대비할 수 있을 것으로 기대한다.

### 4.2.2 백업 데이터를 통한 신속한 초기대응

최근의 산업 환경 특성상 기술유출사고는 PC, 노트북, 외장하드 등 디지털 기기에 대한 조사가 필수다. 그러나 방대한 양의 디지털 증거로 인해 기술유출사고 조사는 많은 어려움을 겪고 있다(강구민·이재철·김창범, 2021). 기술유출사고 발생 시 기업의 피해를 최소화하고 신속한 피해회복을 위해서는 신속한 수사가 이루어져야 함에도, 기술유출사건 1건당 평균 소요 시간은 약 7개월 정도 소요되는 것으로 나타나(정점영 외, 2021) 신속한 사실관계 파악이 늦어지고 있다. 이에, 신속한 사고대응과 증거확보를 위해서는 사고 전 단계에서부터 기업 내 디지털 기기에 대한 실시간 데이터 수집이 이루어질 필요가 있다. 또한, 실시간 백업 데이터의 생성은 무결성 확보를 위해서도 중요하다. 대부분의 기업은 퇴직자의 하드디스크를 별도로 관리하지 않고, 후임 사용자가 해당 컴퓨터를 사용하는데, 이럴 경우 컴퓨터에 있는 접근시간과 실행 날짜 등 모든 것이 최근 시간으로 변경되어 하드디스크의 무결성이 사라지게 된다. 즉, 기술유출사건에서의 디지털 증거 확보가 어려워지게 되는 것이다(전창욱·유진호, 2016). 이에, 신속한 초기대응과 증거확보를 위해서는 기업 내의 디지털 기기에 대한 백업 데이터를 생성하는 것이 중요하며, 이러한 사전 조치는 기술유출사고의 대응에 있어 기업의 피해회복을 빠르게 해줄 것이다.

### 4.2.3 일반원칙 준수를 통한 증거능력 강화

디지털포렌식에 의한 증거가 재판에서 증거능력을 인정받기 위해서는 확보된 증거가 디지털포렌식의 일반원칙에 따라 획득된 증거여야 한다(노명선·백명훈, 2016). 「디지털 증거의 수집·분석 및 관리규정」 제4조에 따르면 디지털포렌식의 일반원칙에는 총 5가지 원칙이 있다. 우선 적법절차를 준수하여야 한다. 디지털 증거는 필요한 범위 내에서 적법한 절차를 엄격히 준수하여 수집되고 분석되며 관리되어야 한다. 그리고 디지털 증거는 원본성이 유지되어 법정에서 원본과의 동일성을 재현하거나 검증하는 데에 지장이 되지 않도록 수집되고 분석되며 관리되어야 한다. 그리고 디지털 증거는 압수 수색 검증한 때로부터 법정에 제출하는 데에까지 훼손 또는 변경되지 않아 무결성이 유지되어야 한다. 디지털 증거의 무결성은 원본과 사본을 비교할 수 있도록 원본이 존재하여야 하며, 제출된 시점에 획득한 해시값과 제출된 이후의 해시값이 동일하여야 충족이 된다(서기민·장기식·김기범, 2010). 이는 정확한 사실관계, 인과관계등을 파악하여 법적 판단을 하기 위해 증거의 훼손을 원칙적으로 금지하는 것이다. 또한 디지털 증거는 디지털포렌식 전문가에 의하여 신뢰할 수 있는 도구와 방법으로 수집되고 분석되며 관리되어야 한다. 마지막으로 디지털 증거는 최초로 수집된 상태 그대로 변경 없이 보관되어야 하며, 이를 위해 보관 주체들 간의 연속적인 승계 절차를 밟는 보관의 연속성이 유지되어야 한다(한국포렌식학회, 2018).

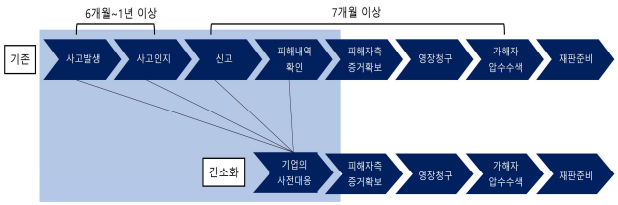
본 연구에서 제안하는 기술유출 수사를 위한 기업의 디지털포렌식 개선방안은 자체적으로 포렌식 조사에 대한 준비 절차를 구축하여 신속한 증거확보와 조사와의 연계성을 목적으로 하였다. 이에 향후 기업 자체적으로 디지털포렌식을 수행하여 획득한 디지털 증거가 법적 증거능력을 인정받기 위해서는 포렌식에 대한 동의 외에도 기업 내부 조사에서부터 포렌식의 일반원칙을 준수하는 것이 중요하다. 사전동의를 받아 디지털포렌식을 진행하더라도 제출된 증거가 이러한 일반원칙에 위반된다면 그 증거는 증거능력을 인정받을 수 없게 되어 그간의 준비가 수포로 돌아가게 되기 때문이다. 이에 기업 내의 조사에서부터 디지털포렌식의 일반원칙을 준수하는 것이 중요하며, 이러한 절차를 지켜야만 신속한 증거능력 인정과 연계성을 통해 더욱 빠른 피해 구제가 가능할 것이다.

### 4.2.4 정부기관과의 신속한 연계

기술유출 사고는 사건 해결까지 오랜 시간이 걸린다. 우선, 기술유출 사고는 사고 발생 후 이를 인지하는데도 오랜 시간이 걸린다. 실제로 2021년 중소기업 기술보호 수준 실태조사 보고서에 따르면 국내에서의 기술침해 발생 시 47.4%가 이를 인지하는데 6개월 이상인 것으로 나타나 기술유출 사고의 절반가량은 이를 인지하는데 오랜 시간이 걸린 것으로 나타났다(중소벤처기업부, 2022c). 또한, 이를 인지하고 신고를 하더라도 수사기관에서 피해기업의 증거를 확보하고 사건을 해결하는데 최소 7개월 이상의 시간이 걸리는 것으로 나타나(김승용·정제용, 2019), 피해기업의 피해회복이 늦어지고 있는 상황이다. 이는 대다수의 경우 디지털저장매체를 통해 기술유출이 이뤄지는 기술유출 사건의 특성상 방대한 분석량과 수사 인력의 부족이라는 현실적인 이유 때문이다.

이에 기술유출 사건은 피해사실을 조기에 발견하고, 기술유출에 대한 피해증거를 기업 내부에서 신속히 확보하여 수사기관과 연계하여 사건을 해결하는 것이 중요하다. 이를 위하여 본 연구는 기업의 기술유출사고대응을 위한 디

지털포렌식 개선방안을 제안하였다. 이를 적용하면, 사고 발생부터 재판 준비까지 8단계의 과정으로 이루어져 약 1~2년이 걸렸던 기존의 절차가 5단계로 단축되어 기술유출사고대응이 빨라질 것으로 예상된다. 특히, 사고 전 준비 단계에서부터 기술유출 사고에 대한 징후들을 실시간 모니터링하여 이상 징후 발생 시 바로 분석에 들어가기 때문에 기술 유출 사고인지에 시간이 단축될 것으로 예상된다. 또한, 사고 발생 후 가해자에 대한 영장청구를 위해서는 피해기업의 피해증거 확보가 필수적인데, 실시간 백업데이터를 바탕으로 한 신속한 증거확보와 사전 동의를 바탕으로 한 적법한 포렌식은 가해자에 대한 영장청구의 시간을 단축시켜 피해기업의 피해회복을 빠르게 해줄 것이다.




**<그림 6> 간소화 된 기업의 기술유출사고대응 절차**

# V. 결론

산업기술 유출범죄는 점점 첨단화, 지능화, 고도화되어가고 있다(장항배, 2015). 이와 같은 흐름 아래 경찰은 산업기술유출방지에 적극적으로 대응하기 위하여 2006년 11월부터 산업기술유출수사대를 조직 및 구성하였다. 또한, 2017년부터는 17개 모든 지방경찰청에 산업기술유출수사대를 조직하여 산업기술 유출 방지를 위하여 노력하고 있지만(최종우·이창무, 2019), 산업기술 유출 사고는 해마다 증가하고 있다(이후기·박원형, 2019). 기술력이 생명인 중소기업과 스타트업의 피해를 최소화하기 위해서는 신속한 수사가 이루어져야 하지만, 수사 인력 부족과 방대한 양의 디지털 증거, 절차상의 문제로 인해 수사가 지연되고 있다. 특히, 기술유출사고는 대부분이 내부 직원에 의해 은밀하게 이뤄지고 유출징후가 외부로 드러나지 않기 때문에 초기 단계에서 기업의 적극적인 발견 노력과 의지가 필수적이다.

이에 본 연구는 기술유출 사고 발생 시 신속한 사실관계 파악과 피해회복을 위한 기업의 디지털포렌식 수사 및 조사를 위한 모델을 제시하였다. 이를 위하여 사고 전 준비 단계에서부터 기업 내부의 디지털 기기에 대한 데이터를 백업하여 사고 발생 시 초기분석 자료로 사용할 것과 사고 발생 시 기술유출 의심자의 디지털 기기에 대한 포렌식 권한을 획득하기 위한 사전 동의를 받아둘 것을 제안하였다. 또한, 유출징후를 사전에 포착할 수 있도록 기존의 연구를 토대로 기술유출 징후들을 정리하였으며, 기업의 초기대응 및 증거수집 단계에서부터의 적법성 유지를 통해 향후 생길 법적 분쟁에도 대비할 수 있도록 하였다.

기술유출 사건의 대응에 있어서는 민관의 협력체계가 중요하다. 민관협력의 중요성은 공동생산이론(Parks et al., 1981)에 따라 설명가능하며, 범죄예방은 정부뿐만 아니라 민간의 적극적인 참여를 통해 수사의 근본적인 한계를 보완할 수 있을 것이다. 기업 내 디지털포렌식 대응 체계를 구축함으로써 기술유출 사고에 대한 수사 및 조사와의 신속한 연계를 꾀할 수 있고, 신속한 수사 및 조사와의 연계로 인하여 증거도 더욱 용이하게 확보될 것으로 기대한다. 이에 따라, 기업의 디지털포렌식 대응 체계가 구축된다면 상황적 범죄예방이론(Clarke, 1995)에서 설명하는 바와 같이 범죄 기회를 감소시키고 범죄자에게 위험 요소를 인식시켜 범죄를 예방할 수 있게 될 것이다. 결국, 이는 산업기술유출의 감소로 이어질 수 있을 것이며, 산업기술유출의 감소는 기술 패권 경쟁에서의 국가경쟁력 확보에도 많은 도움을 줄 것이다. 다만, 기업 내 디지털 기기의 실시간 데이터 백업과 기술유출사고 대응을 위한 사전 동의서 확보는 연구원들에게 가해지는 제한이 많은 만큼 이에 대한 합당한 보상 역시 병행되어야 할 것이다. 또한, 중소기업과 스타트업은 자본력이 없어 자체적으로 포렌식 절차를 구축하기에는 현실적인 어려움이 있기에, 정부의 경제적 지원과 정부·민간 보안업체가 협력과 중소기업과 스타트업 내의 포렌식 절차를 구축하는 것에 지원해줄 필요성이 있다.

본 연구의 학술적 및 실무적 의의는 다음과 같다. 우선, 학술적 측면에서 선행연구는 디지털포렌식의 기술적 측면이나 수사기관 또는 공공기관에 의한 증거수집 절차에 초점을 둔 연구가 많았는데, 본 연구에서는 기술유출 대응을 위한 기업의 디지털포렌식 대응 체계에 대한 구축방안을 기업의 경영관점에서 연구하였다는 점에 의의가 있다. 실무적 측면에서는 기술유출사고 발생에 대비할 수 있는 실질적인 가이드라인을 구축하였다는 점에 의의가 있다. 특히, 중소기업이나 스타트업의 경우에는 기술유출 사고대응 절차에 대한 경험이 없기에 본 연구와 같이 공개적인 논의를 통한 실질적인 가이드라인 구축에 대한 논의는 중소기업과 스타트업의 실무에 많은 도움을 줄 것으로 예상된다. 또한, 수사기관과의 연계를 통한 신속한 피해회복 방안을 제시하였다는 점에서도 실무적 의의가 있다. 한편,

본 연구는 방대한 양의 세부 절차를 완전히 설명하지 못했다는 점에서 한계가 있다. 또한, 본 연구는 디지털포렌식 개선방안에 대한 실증분석이나 개선방안의 검증에 대한 한계가 있다. 디지털포렌식 전문가를 대상으로 심층 인터뷰를 진행하였으나, 본 연구 결과의 타당성과 신뢰성을 확보하고 보다 구체적인 방안 제시하기 위해서는 추가적인 연구가 필요하다. 그럼에도 불구하고 본 연구는 기존 기술유출사고에서의 포렌식 문제점을 기업의 경영관리 측면에서 논의하였다는 점에서 학술적 의의가 크며 디지털포렌식의 절차와 한계점들을 체계적으로 정리하였다는 점에서 기업들에게 주는 실무적인 가치가 크다고 하겠다.

# 참고문헌


강구민·이재철·김창범(2021). 산업보안조사에 있어 디지털포렌식 조사의 임의성에 관한 연구. **한국산업보안연구**, 11(1), 117-136.

경찰청(2022a). *경찰청 국가수사본부 '산업기술유출 사범 특별단속' 결과 발표*. Retrieved (2022.12.16.) from https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20221128074145295, 경찰청.

경찰청(2022b). *경찰청 국가수사본부 국부유출 방지 및 국가경쟁력 확보를 위한 '산업기술 유출 수사' 총력 대응체제 확립*. Retrieved (2022.12.16.) from https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20220221132508525, 경찰청.

권양섭(2021). 한국형 디지털포렌식 수사절차 및 검증체계 구축 방안. **디지털포렌식연구**, 15(1), 67-82.

김면기·유승진(2019). 포렌식 미란다 원칙과 절차적 정의. **형사정책연구**, 30(4), 303-327.

김무석·강구민(2022). 현행 산업보안조사의 한계와 개선방안에 관한 연구: 디지털포렌식을 중심으로. **한국산업보안연구학회**, 12(2), 185-206.

김민수(2018). 디지털 포렌식 증거 채택 기준의 한계와 개선 방안. **융합보안논문지**, 18(4), 35-43.

김상화(2022). 정부의 창업지원정책 및 기업가정신이 창업기업의 비재무적성과에 미치는 영향에 관한 연구. **한국진로창업경영학회지**, 6(3), 111-131.

김선욱(2021). 산업스파이에 의한 국가핵심기술 유출 방지를 위한 법제적 개선방안. **원광법학**, 37(2), 33-53.

김성원·박현애·이환수(2020). 중소기업 기술보호 지원제도의 활성화 방안 연구. **중소기업연구**, 42(1), 1-17.

김승용·정제용(2019). 범국가적 산업기술 수사체계 구축 방안에 대한 연구: 산업기술유출사건의 특성 및 외국사례 중심으로. **가천법학**, 12(4), 3-12.

김영준·김완주·임재성(2020). 무결성 향상을 위한 모바일 포렌식 모델 연구. **정보보호학회논문지**, 30(3), 417-428.

김영철·구희진(2021). 디지털 증거 대상 임의제출물 압수의 문제점. **정보법학**, 25(1), 101-123.

김재수·김자원·김정욱·최유림·장항배(2019). 기술유출행위 군집화를 위한 탐색적 연구. **융합보안논문지**, 19(2), 3-9.

김종호(2019). 증거수집 방식으로서 작동중인 정보시스템에서의 포렌식 절차의 검토. **과학기술법연구**, 25(4), 37-86.

김태훈·박남규·최한나·이대윤·안종득·조용환(2009). 포렌식 데이터의 실시간 수집 절차 모델링. **한국컴퓨터정보학회논문지**, 14(12), 139-145.

김현수(2017). 내부자 정보 유출 탐지 방법에 관한 연구. 한국**인터넷방송통신학회 논문지**. 17(4), 11-17.

남기욱·이상진(2021). 디지털 포렌식 사설 업체에 위탁된 데이터 보호 방안에 관한 연구 (디지털 포렌식 랩(시설)이 구비해야 할 요건 제시). **디지털포렌식연구**, 15(1), 12-25.

노명선·백명훈(2016). **디지털 포렌식**. 고시계사.

박상문·서종현(2012). 중소기업의 기술경영 활동수준과 기술역량 및 기술혁신 애로요인간의 관계. **중소기업연구**, 34(2), 81-99.

박종욱(2020). *해시값 훼손 또는 결여시 디지털증거의 증거능력 인정에 관한 연구*. 석사학위논문, 성균관대학교.

박찬수·강민지·최이중(2019). 글로벌 기술환경 변화에 따른 산업보안 생태계 구축 방안. **정책연구**, 2019(22), 1-123.

박현출·박진상·김정덕(2020). 내부정보 유출 시나리오와 Data Analytics 기법을 활용한 내부정보 유출징후 탐지 모형 개발에 관한 연구. **정보보호학회논문지**, 30(5), 957-966.

서기민·장기식·김기범(2010). 디지털 증거의 무결성: 모든 디지털 증거의 무결성을 입증할 수 있는가?. **디지털 포렌식연구**, 4(2), 1-16.

송인옥(2022). 국가안보를 위한 국가핵심기술 관리의 실효성 확보 방안. **고려법학**, 104(0), 81-120.

신원(2014). 안티포렌식 기법 분석을 통한 안티포렌식 대응 방안. **보안공학연구논문지**, 11(6), 605-614.

윤우성·한재혁·이상진(2019). 효율적인 디지털 포렌식 조사를 위한 육하원칙 중심의 정보 처리 규격. **디지털포렌식연구**, 13(2), 127-136.

윤지수·이경열(2021). 안티 포렌식 신종기법에 대한 형사법적 대응방안. **형사정책**, 32(4), 65-99.

이건희(2021). 전자매체에 내장된 금융정보, 개인정보의 디지털 포렌식 방식 관리에 관한 연구. **신용카드리뷰**, 15(1), 108-118.

이규안(2010). *JTAG 방식을 이용한 모바일 포렌식 기법 연구*. 박사학위논문, 숭실대학교.

이금녀(2013). 기술유출사고의 포렌식 수사 절차에 대한 연구. **디지털포렌식연구**, 7(1), 33-48.

이상무·문병준(2020). 기업 핵심역량 및 경쟁우위의 결정요인과 경영성과에 관한 연구:중소·벤처기업을 중심으로. **경영경제연구**, 42(4), 75-102.

이석희·박보라·이상진·홍석희(2008). 안티 포렌식 기술과 대응 방향. **정보보호학회지**, 18(1), 11-19.

이승주(2022). 기술과 국제정치: 기술패권경쟁시대의 한국의 전략. **한국과 국제정치**, 38(1), 227-256.

이은아·서정해(2017). 스타트업의 기술지향성이 혁신성과에 미치는 영향 : 사회적 자본의 매개효과. **기업경영연구**, 24(6), 43-62.

이장욱(2020). 내부자에 의한 산업기술 침해 위험성 연구: 연구개발직 근로자를 중심으로. **시큐리티연구**, 0(63), 129-152.

이정호·강민창·강현석·장재훈·조호묵(2022). 증거능력 확보를 위한 수사용 사이버 공개정보 포렌식 도구 아키텍처 연구. **정보과학회논문지**, 49(6), 494-506.

이준원(2021). 기술수준에 따른 서비스업 혁신 중소기업의 생존기간 비교분석. **중소기업연구**, 43(3), 1-20.

이창훈(2011). 항공 응용 분야: 개인정보보호법 기반 디지털 포렌식 수사 모델 연구. **한국항행학회논문지**, 15(6), 1212-1219.

이태림·신상욱(2011). 디지털 포렌식을 위한 증거 분석 도구의 신뢰성 검증. **정보보호학회논문지**, 21(3), 165-176.

이후기·박원형(2019). 산업기술유출 발생에 따른 금전적 피해액 산출 모델 연구. **한국산업보안연구**, 9(2), 215-234.

장항배(2015). 산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구. **융합보안논문지**, 15(7), 39-45.

전상덕·홍동숙·한기준(2006). 디지털 포렌식의 기술 동향과 전망. **정보화정책,** 13(4), 3-19.

전상준(2016). 윈도우즈 시스템 포렌식. **정보보호학회지**, 26(5), 6-16.

전창욱·유진호(2016). 중소기업에서 산업보안을 위한 디지털포렌식 활용방안 연구: 이미징 처리시간 비교분석을 중심으로. **한국산업보안연구**, 6(2), 169-193.

정점영·박원효·정민수·장항배(2021). 산업기술유출수사 지연원인과 대응방안 연구: 핵심인력유출사례 분석을 중심으로. **한국산업보안연구**, 11(1), 217-241.

정지용·최지성·박정흠·이상진(2019). macOS Mojave에서의 포렌식 분석 절차 연구. **디지털 포렌식 연구**, 13(2), 76-87.

정진홍(2010). 산업스파이 범죄수사에 있어서 디지털 증거의 과학적 분석 및 처리절차에 관한 연구: 디지털포렌식 기법을 중심으로. **과학수사학회지**, 4(2), 173-182.

정진효·이창무(2017). 표준규정과 판례 비교를 통한 디지털 포렌식의 법적 증거능력 인증기준. **디지털포렌식연구**, 11(3), 41-55.

조균희(2006). *컴퓨터포렌식과 안티포렌식에 관한 고찰*. 석사학위논문, 광운대학교.

조하나·하리다·이환수(2021). 스타트업의 기술 유출 방지 방안에 관한 연구. **한국진로창업경영학회지**, 5(4), 27-40.

중소벤처기업부(2018). *2018 중소기업 기술개발 지원사업 설명회 발표자료*. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=394360&pageIndex=1&noPage=yes. 중소벤처기업부.

중소벤처기업부(2019). *2019 중소기업 기술개발 지원사업 설명회 발표자료*. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=203367&pageIndex=1&noPage=yes. 중소벤처기업부.

중소벤처기업부(2020). *2020 중소기업 기술개발 지원사업 설명회 발표자료*. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=257323&pageIndex=1&noPage=yes. 중소벤처기업부.

중소벤처기업부(2021a). *2020 중소기업 기술보호수준 실태조사 (2021.02)*. 서울시: 대·중소기업·농어업협력재단.

중소벤처기업부(2021b). *2021 중소기업 기술개발 지원사업 설명회 발표자료*. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=333788&pageIndex=1&noPage=yes. 중소벤처기업부.

중소벤처기업부(2022a). *2023 중소기업 기술개발 지원사업 통합공고*. Retrieved (2022.1.8.) from https://www.korea.kr/news/pressReleaseView.do?newsId=156544725. 중소벤처기업부.

중소벤처기업부(2022b). *2022 중소기업 기술개발 지원사업 설명회 발표자료*. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=394360&pageIndex=1&noPage=yes. 중소벤처기업부.

중소벤처기업부(2022c). *2022 중소기업 기술보호 수준 실태조사(2022.06)*. 서울시: 대·중소기업·농어업협력재단.

진재근(2021). 산업보안과 산업기술유출 대응에 관한 연구: 미국, 일본 및 독일을 중심으로. **KBM Journal(K Business Management Journal)**, 5(2), 51-60.

최선영·정지원(2022). 지속가능한 경영을 위한 산업보안 거버넌스. **한국산업보안연구**, 12(3), 137-168.

최순웅(2011). *삼성전자 핵심기술 유출, 中연구원 구속..증거인멸 시도도(종합).* 파이낸셜뉴스, Retrieved (2022.12.16.) from https://www.fnnews.com/news/201104131938364385.

최종우·이창무(2019). 산업기술유출범죄 수사 의지에 영향을 미치는 요인 분석. **한국경찰학회보**, 21(5), 105-132.

한국산업보안연구학회(2020). **산업보안조사론**. 박영사.

한국인터넷진흥원(2010). *침해사고 분석 절차 안내서(제2010-8호)*. 나주시: 한국인터넷진흥원.

한국정보통신기술협회(2017). *디지털 증거 수집보존 가이드라인(TTAS.KO-12.0058/R1).* 성남시: 한국정보통신기술협회.

한국포렌식학회(2018). **디지털포렌식 이론**. 미디어북.

홍지은(2020). 특별사법경찰의 행정조사와 수사: 진술서 작성 및 자료 제출 요구를 중심으로. **범죄수사학연구**, 6(1), 101-127.

Chang, H. B.(2015). A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident. **Journal of convergence security. Journal of convergence security**, 15(7), 39-45.

Cho, H. N., Ha, R. D., & Lee, H. S.(2021). A Study on the Protection of Technology Leakage of Startups. **The Journal of Korean Career·Entrepreneurship & Business Association**, 5(4), 27-40.

Cho, K. H.(2006). *A study on computer forensics and Anti-forensics*. Master's thesis. Kwangwoon University.

Choi, D. S. (2021). A Study on the Digital Forensic Management of Financial Information and Personal Information Embedded in Electronic. **The Credit Card Review (Credit Card Review)**, 15(1), 108-118.

Choi, J. W., & Lee, C. M.(2019). An Analysis of the Factors Affecting the Will to Investigate Industrial Technology Leakage. **The Korean Association of Police Science Review (KAPS)**, 21(5), 105-132.

Choi, S. W.(2011). *Samsung Electronics' Core Technology Leakage, Researcher in China Arrested...Attempt to destroy evidence (Round-up)*. Financial News, Retrieved (2022.12.16.) from https://www.fnnews.com/news/201104131938364385.

Choi, S. Y., & Jeong, J. W.(2022). Industrial Security Governance for Sustainable Management. **Korean Journal of Industrial Security**, 12(3), 137-168.

Chung, C. Y., Park, W. H., Jung, M. S., & Chang, H. B.(2021). Research on the Causes of Delayed Investigation into Industrial Technology Leakage and Countermeasures: Focus on Analysis of Core Human Resource Leakage Cases. **Korean Journal of Industrial Security**, 11(1), 217-241.

Clarke, R. V.(1995). Situational crime prevention. **Crime and justice**, 19, 91-150.

Hong, J. E.(2020). Administrative Investigation and Investigation of Special Judicial Police : Focusing on Writing Statement and Requiring to Submit Materials. **Criminal Investigation Studies**, 6(1), 101-127.

Jeon, C. U., & Yoo, J. H.(2016). A Study on the Digital Forensic Utilization Method for Industrial Security at Small Businesses - Based on the Comparison Analysis of Imaging Processing Time -. **Korean Journal of Industrial Securit**y, 6(2), 169-193.

Jeon, S. D., Hong, D. S., & Han, K. J.(2006). Technology Trend and Prospect of the Digital Forensics. **Informatization policy**, 13(4), 3-19.

Jeon, S. J.(2016). Windows System Forensics. **Korea Institute of Information Security and Cryptology**, 26(5), 6-16.

Jeong, J. H.(2010). Research on Scientific Analysis and Processing of Digital Evidence During the Criminal Investigation of Industrial Espionage- Focused on Digital Forensic Investigation Technique-. **Journal of Science Criminal Investigation**, 13(2), 173-182.

Jin, J. K.(2021). A Study on Industrial Security and Response to Industrial Technology Leakage: Focusing on the USA, Japan and Germany. **KBM Journal(K Business Management Journal)**, 5(2), 51-60.

Jung, J. H., & Lee, C. M.(2017). A Study on Integrity, Originality, and Reliability of Digital Forensic based on Comparison of Standard Guidelines and precedents. **Journal of Digital Forensics**, 11(3), 41-55.

Jung, J. Y., Choi, J. S., Park, J. H., & Lee, S. J.(2019). A Study on the Forensics Analysis Procedure in MacOS Mojave. **Journal of Digital Forensics**, 13(2), 76-87.

Kang, G. M. & Lee, J. C. & Kim, C. B.(2021). A Study on the Voluntariness of Digital Forensic Investigation in the Industrial Security Investigation.

**Korean Journal of Industrial Security**, 11(1), 117-136.

Kim, H. S.(2017). A Study on Method for Insider Data Leakage Detection. **The Journal of The Institute of Internet, Broadcasting and Communication (JIIBC)**, 17(4), 11-17.

Kim, J. H.(2019). A Review of live Forensic Procedures in Information Systems Operating as Evidence Gathering. **Hannam Journal of Law&Technology**, 25(4), 37-86.

Kim, J. S., Kim, J. W., Kim, J. W., Choi, Y. R., & Jang, H. B.(2019). An Exploratory Study for Clustering of Technology Leakage Activities. **Journal of convergence security**, 19(2), 3-9.

Kim, M. K. & Ryu, S. J. (2019). Forensic Miranda Principle and Procedural Justice. **Korean Criminological Review**, 30(4), 303-327.

Kim, M. S. & Kang, G. M.(2022). A Study on the Limitations and Improvement Measures of the Current Industrial Security Investigation : Focusing on Digital Forensic. **Korean Journal of Industrial Security**, 12(2), 185-206.

Kim, M. S.(2018). Limitations and Improvements of Adoption Criteria for Digital Forensic Evidence. **Journal of convergence security**, 18(4), 35-43.

Kim, S, Y., & Jung, J. Y.(2019). A Study on the Establishment of the National Industrial Espionage Investigation System. **Gachon Law Review**, 12(4), 3-12.

Kim, S. H.(2022). Effect of Government Startup Support Policy and Entrepreneurship on Non-Financial Performance. **The Journal of Korean Career·Entrepreneurship &Business Association**, 6(3), 111-131.

Kim, S. W., Park, H. A., & Lee, H. S.(2020). A Study on the Activation Plan of the Support Systems for SMEs' Technology Protection. **Asia Pacific Journal of Small Business**, 42(1), 1-17.

Kim, S. W.(2021). Legislative Improvement Plan for the Prevention of National Core Technology Leakage by Industrial Spy. **Wonkwang Law Review**, 37(2), 33-53.

Kim, T. H., Park, N. K., Choi, H. N., Lee, D. Y., Ahn, J. D., & Cho, Y. H.(2009). Modeling of Collection Process for Real-time Forensic Data. **Journal of The Korea Society of Computer and Information**, 14(12), 139-145.

Kim, Y. C., & Koo, H. J.(2021). Challenges of Voluntarily Submitted Digital Evidence. **Journal of Korea Infomation Law**, 25(1), 101-123.

Kim, Y. J., Kim, W. J., & Lim, J. S.(2020). A Study the Mobile Forensics Model for Improving Integrity. **Journal of The Korea Institute of Information Security and Cryptology**, 30(3), 417-428.

Korea Internet & Security Agency(KISA). *Infringement Incident Analysis Procedure Guide(2010-8)*. Naju-si: KISA.

Korean Institute of Forensics Sciences(2018). **Digital Forensics Theory**. Mediabook.

Korean National Police Agency(2022a). *The National Office of Investigation of KNPA announces Results of Special Crackdown on Industrial Technology Leakage*. Retrieved (2022.12.16.) from https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20221128074145295, Korean National Police Agency.

Korean National Police Agency(2022b). *Establishment of an All-out Response System for Industrial Technology Leakage Investigation to Prevent Leakage of National Wealth and Secure National Competitiveness*. Retrieved (2022.12.16.) from https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20220221132508525, Korean National Police Agency.

Kwon, Y. S.(2021). A Study on Korean Digital Forensic Investigation Procedure and Construction of Verification System. **Journal of digital forensics**, 15(1), 67-82.

Lee, C. H.(2011). Aviation Application : Study on Digital Investigation Model for Privacy Acts in Korea. **The journal of Korea Navigation Institute**, 15(6), 1212-1219.

Lee, E. A., & Seo, J. H.(2017). The Effect of Technological Orientation on Performance of Startup: The Mediating Effect of Social Capital. **Korean Corporation Management Review**, 24(6), 43-62.

Lee, H. K., & Park, W. H.(2019). A Study on the Calculation Model of Money Value Measurement Damages from Industrial Technology Leakage. **Korean Journal of Industrial Security**, 9(2), 215-234.

Lee, J. H., Kang, M. C., Kang, H. S., Jang, J. H., & Cho, H. M.(2022). A Study on the Architecture of Cyber Public Information Forensic Tools for Investigation to Obtain the Court Evidence Ability. **Journal of**

**KIISE (JOK)**, 49(6), 494-506.

Lee, J. W.(2020). A Study on the Risk of Infringement of Industrial Technology by Insiders - Focusing on R&D workers -. **Korean Security Journal**, 0(63), 43-62.

Lee, J. W.(2021). Comparative Analysis of Survival Period by Technological Capabilities of Innovative SMEs in the Service Industry. **Asia Pacific Journal of Samall Business**, 43(3), 1-20.

Lee, K. A.(2010). A study on mobile forensic methods using JTAG scheme. **A doctoral dissertation,** Soongsil University.

Lee, K. N.(2013). Study of Digital Forensic Investigative Procedure for Industrial Technology Leakage. **Journal of Digital Forensics**, 7(1), 33-48.

Lee, S. H., Park, B. R., Lee, S. J., & Hong, S. H.(2008). Anti-forensics technology and direction of response. **Korea Institute of Information Security & Cryptology(KIISC)**, 18(1), 11-19.

Lee, S. J.(2022). Technology and International Politics: Competition for Technological Hegemony and Korea's Strategy. **Korea and World Politics**, 38(1), 227-256.

Lee, S. M., & Moon, B. J.(2020). Determinants of Corporate Core Competencies, Competitive Advantage and Management Performance : Focused on Small and Medium-size Companies. **Journal of Management & Economics (MERI)**, 42(4), 75-102.

Lee, T. R., & Shin, S. U.(2011). Reliability Verification of Evidence Analysis Tools for Digital Forensics. **Journal of The Korea Institute of Information Security and Cryptology**, 21(3), 165-176.

Ministry of SMEs and Startups(2021a). *2020 Survey Research on Technology Protection Level of SMEs(2021.02).* Seoul: Korea Foundation for Cooperation of Large&Small Business, Rural Affairs.

Ministry of SMEs and Startups(2022a). *2023 Public Notification of SMEs R&D Support Project.* Retrieved (2022.1.8.) from https://www.korea.kr/news/pressReleaseView.do?newsId=156544725, Ministry of SMEs and Startups.

Ministry of SMEs and Startups(2021b). 2021 Conference Presentation of SMEs R&D Support Project. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=333788&pageIndex=1&noPage=yes, Ministry of SMEs and Startups.

Ministry of SMEs and Startups(2022b). 2022 Conference Presentation of SMEs R&D Support Project. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=394360&pageIndex=1&noPage=yes, Ministry of SMEs and Startups.

Ministry of SMEs and Startups(2022c). *2022 Survey Research on Technology Protection Level of SMEs(2022.06).* Seoul: Korea Foundation for Cooperation of Large&Small Business, Rural Affairs.

Ministry of SMEs and Startups(2018). 2018 Conference Presentation of SMEs R&D Support Project. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=394360&pageIndex=1&noPage=yes, Ministry of SMEs and Startups.

Ministry of SMEs and Startups(2019). 2019 Conference Presentation of SMEs R&D Support Project. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=203367&pageIndex=1&noPage=yes, Ministry of SMEs and Startups.

Ministry of SMEs and Startups(2020). 2020 Conference Presentation of SMEs R&D Support Project. Retrieved (2022.1.8.) from https://www.smtech.go.kr/front/ifg/no/notice01_detail.do?searchCondition=0&searchKeyword=%ec%a4%91%ec%86%8c%ea%b8%b0%ec%97%85+%ea%b8%b0%ec%88%a0%ea%b0%9c%eb%b0%9c&bitmSeq=257323&pageIndex=1&noPage=yes, Ministry of SMEs and Startups.

Nam, K. U., & Lee, S. J.(2021). A Study on the protection of personal data committed to Digital forensics private companies (A requirements for digital forensics labs). **Journal of Digital Forensics**, 15(1), 12-25.

Park, C. S., Kang, M. J., & Choi, I. J.(2019). Strategy on Building Korea's Industrial Security Ecosystem in the Global Technology Competition Era. **Policy Review**, 2019(22), 1-123.

Park, H. C., Park, J. S., & Kim, J. D.(2020). A Study on Development of Internal Information Leak Symptom Detection Model by Using Internal Information Leak Scenario &Data Analytics. **Journal of The Korea Institute of Information Security and Cryptology (JKIISC)**, 30(5), 957-966.

Park, J. U.(2020). *A study on admissibility of the digital evidence whichhas damaged hash value or non-hash value*. Master's thesis, Sungkyunkwan University.

Park, S. M., & Seo, J. H.(2012). A Relationship between Intensity of Technology Management, Technological Capabilities and Barriers to Innovations in SMEs. **Asia Pacific Journal of Small Business**, 34(2), 81-99.

Parks, R. B., Baker, P. C., Kiser, L., Oakerson, R., Ostrom, E., Ostrom, V., Percy, S. L., Vandivort. M. B., Whitaker, G. P., & Wilson, R.(1981). Consumers as coproducers of public services: Some economic and institutional considerations. **Policy Studies Journal**, 9(7), 1001-1011.

Roh, M. S., & Baek, M. H.(2016). **Digital Forensics**. Gosigyesa.

Seo, K. M., Jang, K. S., & Kim, G. B.(2010). Integrity of Digital Evidence : Can we prove whether its integrity is preserved?. **Journal of Digital Forensics**, 4(2), 1-16.

Shin, W.(2014). Countermeasures against Anti-forensics by Analyzing Anti-forensics Techniques. **Journal of Security Engineering,** 11(6), 605-614.

Song, I. K.(2022). The Direction of Protection of National Security by Securing the Effectiveness of National Core Technology Regulations. **Korea Law Review**, 104(0), 81-120.

Telecommunications Technology Association(TTA)(2017). *Guidelines for Collection, Acquisition, and Preservation of Digital Evidence(TTAS.KO-12.0058/R1)*. Seongnam-si: TTA.

The Korea Association for Industrial Security(KAIS)(2020). **INDUSTRIAL SECURITY INVESTIGATION THEORY**. Parkyoungsa.

Yoon, J. S., & Lee, K. L.(2021). A Study on the Understanding of New Anti-Forensics and Proposal of Criminal Policy Countermeasures. **Korean Journal Of Criminology (KJC)**, 32(4), 65-99.

Yun, W. S., Han, J. H., & Lee, S. J.(2019). 5W1H based Information Expression Standard for efficient digital forensic investigation. **Journal of Digital Forensics**, 13(2), 127-136.

[abstract]

# The Improvement Method of Digital Forensic for Responding to Technology Leakage of SMEs*

Soonbeom Kwon**, Hyeongryeol Kim***, Seonyeong Choi****, Hwansoo Lee*****

Industrial technology leakage is increasingly becoming sophisticated, intelligent, and advanced. So, the police organized an industrial technology leakage investigation team in November 2006 and expanded the industrial technology leakage investigation team to 17 local police agencies in 2017. Likewise, the police is trying to prevent industrial technology leakages, but it is still annually increasing. Especially, in 60.8% cases of technology leakages by insiders are done by using memory devices. Which makes digital forensic necessary in order to detect such incidents. However, problems such as shortage of man power, matters of procedure, and vast amount of digital evidence, delay fact-finding and damage restoration. This study introduces the company's digital forensic system designed for corporations which will help them obtaining digital evidences in a prompt and accurate way. This study suggests that institutes should regularly backup their datas so that they would have sufficient information to analyze incidents. Also, it proposes companies to acquire consent from their insiders before incidents happen in order to have access to suspects' digital devices and forensic it in a legal way. Furthermore, we have analyzed signs of technology leakages based on privious studies and introduced lawful means for corporates to respond to technology leakage and evidence collecting to prevent from possible disputes.

KeyWord: Technology management, Technology leakage, Digital forensics, Digital evidence, SMEs

* This work was supported by the Growth Support Project for Industrial Innovation Talent of MOTIE (P0008703).
** First Author, Dankook University, Interdisciplinary graduate program in IT Law, Master's Student, kwonsb777@naver.com
*** Second Author, Dankook University, Interdisciplinary graduate program in IT Law, Association Course Student for Master's, uwhale3pb@daum.net
**** Third Author, Dankook University, Interdisciplinary graduate program in IT Law, Ph. D. Student, sunyoung9479@naver.com
***** Corresponding Author, Dankook University, Interdisciplinary graduate program in IT Law, Assistant Professor, hanslee992@gmail.com