디지털 포렌식 준비도 설계에 관한 연구

박광민*, 박상호**, 박리원***, 장항배****
*더존비즈온 포렌식센터
,*중앙대학교 융합보안학과
****중앙대학교 산업보안학과
e-mail: *gmpark@douzone.com
{**sanghopark, ***lwpark, ****hbchang}@cau.ac.kr

A Study on Design of Digital Forensic Readiness

Gwangmin Park*, Sangho Park**, Leewon Park***, Hangbae Chang****
*Forensics Center, Douzone ICT Group
,*Department of Security Convergence, Chung-Ang University
****Department of Industrial Security, Chung-Ang University

요 약

최근 시간과 장소에 얽매이지 않고, 언제 어디서나 편리하게 근무함으로써 업무효율성을 향상시킬 수 있는 업무환경 개념인 스마트워크(Smartwork)가 각광을 받고 있다. 그러나 스마트워크 환경에서는 모든 업무가 정보통신망과 정보시스템을 통해 처리되기 때문에 정보유출 위협이 존재한다. 또한, 디지털 포렌식 분야에서 조사 및 수사대상이 점점 다양화되고 있다. 내부정보 유출과 같은 보안사고 발생 후, 디지털 증거는 대부분 제한적으로 수집될 수밖에 없으며, 전문업체 의뢰 시 높은 의뢰비용과 장기간의 분석 시간이 소요된다. 기존의 내부정보 유출 방지 시스템에만 의존할 것이 아니라, 유출 행위 탐지에 중점을 둔 선제적 감사 활동을 수행하기 위한 디지털 포렌식 준비도가 필요한 상황이다. 따라서, 본 논문에서는 다양한 디지털 포렌식 준비도 관련 모델들에 대한 분석을 기반으로 미래 스마트워크 환경에서 보안사고에 대응하기 위한 디지털 포렌식 준비도 모형을 연구하였다.

1. 서론

최근 IT 기술의 이용 및 활용을 통해 시공간에 얽매이지 않고, 언제 어디서나 편리하고 똑똑하게 근무하여 업무효율성을 향상시킬 수 있는 업무환경 개념인 이른바 스마트워크(Smartwork)가 주목을 받고 있다[1]. 그러나, 스마트워크 환경에서는 모든 업무가 정보통신망과 정보시스템을 통해 처리되기 때문에 정보유출 위협이 존재하고 있으며, 특히, 다수의 기업과 공공기관들이 클라우드 컴퓨팅 도입, 유·무선 원격업무시스템 도입 등을 구축하고 있어 항시 해킹 및 정보유출 위협의 노출되어있다. 그러나 기업의 내부정보 유출과 같은 보안사고 발생 시 디지털 증거 확보에 있어 디지털 증거의 다양성, 확보한 디지털 증거의 분석 시간 증가로 인해 보안사고를 해결하는데 어려움이 있다. 디지털 환경의 변화에 따른 디지털 증거확보, 분석 방법의 변경, 분석시간의 지연은 디지털 포렌식 분야에서 반드시 해결되어야 할 문제점이다[2].

기존의 디지털 포렌식의 경우, 보안사고 발생 시 사고 발생 전의 상태로 원상복구 하려는 데에 초점이 맞춰지다 보니 디지털 증거 확보 및 현장보존이 제대로 이루어지지 않고, 이로 인해 보안사고 원인을 제대로 규명하지 못하고 법정 문제에서 어려움을 겪는 사례가 늘어나고 있는 것도 디지털 포렌식 분야에서 반드시 해결되어야 할 문제점으로 떠오르고 있다.

이러한 문제를 해결하기 위해 인해 기업의 내부 정보 유출 등과 같은 보안사고 발생원인을 규명하고, 무결성이 보장된 디지털 증거를 확보하기 위한 디지털 포렌식 역량이 기업 전반에 걸쳐 요구되고 있다. 보안사고에 드는 비용과 디지털 증거분석시간 단축을 위해 디지털 포렌식 역량을 미리 갖추어 사전적 디지털 포렌식 준비를 요구하는 디지털 포렌식 준비도(Digital Forensic Readiness)에 대한 필요성이 제기되고 있다.

2. 선행연구

2.1 디지털 포렌식과 디지털 증거

과거에는 포렌식(Forensic)이라는 개념이 DNA, 지문, 감식, 모발, 변사체 검시 등 법의학 분야에서 주로 사용되었다. 하지만, 최근 다양한 디지털 기기들의 보급 및 활용과 정보의 생산 및 유통에 있어서 90% 이상이 디지털 형태로 전환되고 이용됨에 따라 포렌식이라는 개념이 물리적 형태의 증거뿐만 아니라 디지털 증거(Digital Evidence)까지 다루어졌고 이는 디지털 포렌식이라는 새로운 분야를 탄생시켰다[3].

디지털 포렌식의 주된 목적은 내부정보 유출 등과 같은 보안사고의 근본 원인을 규명하고 위법성 및 책임여부를 파악한 뒤 해당 사용자를 성공적으로 기소하는 것이다. 디지털 포렌식은 단순히 보안사고 조사를 위한 과학적인 방법 및 절차를 연구하는 학문이 아니라 디지털 증거의

증거능력을 부여하기 위한 법적인 영역의 한 분야까지 확장된다[4].

디지털 증거는 이진수로 이루어진 정보의 형태로 기록되고 저장되기 때문에 육안으로는 직접 디지털 정보의 내용을 인지할 수 없다(비가시성). 따라서 디지털 증거가 재판에서 증거로 인정받기 위해서는, 디지털 형태(이진수)로 저장된 정보를 육안으로 확인할 수 있는 증거로 변환하는 과정이 필수적으로 요구된다. 이변환과정에는 디지털 정보의 변환과 관련한 프로그램 및 기술들이 필요하기 때문에 이에 관한 관련 전문가의 참여가 필요하다[5].

이처럼 디지털 증거의 특성으로 인해 획득한 디지털 증거가 재판에서 증거로 인정받기는 쉬운 일이 아니며, 해당 증거가 증거로 인정받기 위해서는 아래의 <표 1>과 같이 디지털 증거 수집 및 분석에 있어서 적법한 절차를 거쳐야 한다.

<표 1> 디지털 증거 수집 시 고려사항

항목	설명
적법절차 준수	증거능력 보존 및 조사행위에 대한 정당성 확보
보관 연속성 유지	신뢰성의 확보를 위한 증거 경로 및 작업내역 기록
증거 수집과 분석과정 문서화	표준화된 절차 및 방법으로 증거를 수집하여 과정의 정확성, 객관석, 적정성 등을 확보
증거분석 도구의 신뢰성 확보	숙련된 전문가 및 검증 받은 포렌식 도구를 사용하여 분석
원본증거의 안전한 보존과 무결성 유지	증거의 훼손이 용이한 전자증거의 특성을 고려

2.2 디지털 포렌식 준비도

디지털 디지털 포렌식 준비도는 2009년 영국에서 제도화되면서 널리 알려지기 시작했다. 디지털 포렌식 준비도 개념은 2000년대 초반부터 등장하기 시작해서 다양한 학자들에 의해 이론화 및 연구가 수행되고 있다. 디지털 포렌식 준비도를 최초로 개념화한 Tan은 디지털 포렌식 준비도를 신뢰할 수 있는 디지털 증거를 수집할 수 있는 환경과 역량을 극대화시키는 기술로 정의하고 있으며, 보안사고 대응 동안 디지털 포렌식 비용의 최소화 및 증거에 대한 활용 가능성을 최대화하는 것을 목적으로 규정하고 있다.[6] 예를 들어 디지털 포렌식 준비도란 물리적 공간에서 조직의 자산을 보호하기 위해 구성되는 CCTV 감시, 출입기록과 같은 물리적 보안장치를 디지털 공간에 구현하는 것이다.

디지털 포렌식 준비도는 단순한 시스템 설정이나 하드웨어 도입 요구에 머물지 않고 기업이 자산 목록과 위협 시나리오 식별, 위험평가, 증거소스 위치파악 등을 거쳐 자신의 환경과 위험에 맞는 적절한 비용효율적인 대응책을 수립할 수 있게 해주는 절차를 갖출 것을 요구한다. 이러한 점에서 디지털 포렌식 준비도는 기존의 단순 로그저장 및 보존 컴플라이언스 등과 같은 기술을 제시한 Tan의 주장과는 많이 구분된다[7].

디지털 포렌식 준비도 모델은 비기술적인 정책 요구사항과 기술적 요구사항으로 구분된다. 정책 요구사항은 다시 각각 조직 외부와 조직 내부 요구사항으로 구분된다. 디지털 증거의 증거능력 확보를 위해 디지털 포렌식 분석가와 도구의 신뢰성을 보장되어야 하고, 문서화된 절차를 갖추어야 하기 때문에 기본적으로 신뢰할 수 있는 디지털 포렌식 전문가·도구 및 기술·절차를 구성요소에 포함해야 한다.

디지털 포렌식 준비도 모델 분석 결과 최근에는 정책적인 요구사항의 중요성이 높아지고 있으며, 기존의 단순 절차 모델에서 벗어나 종합적인 구조 모델로 변화하고 있는 추세이다. 즉, 조직 내부에 디지털 포렌식 관련 기술 인프라를 준비해놓는 것을 포함하여 조직 내·외부의 기술적·비기술적 요구사항들을 아우르는 디지털 포렌식 거버넌스의 형태로 진화하고 있다.

3. 디지털 포렌식 준비도 설계

선행연구를 통해 분석한 기존 디지털 포렌식 절차 분석을 정리하면 <표 2>와 같다.

본 연구에서 정리한 디지털 포렌식 준비도 절차는 보안사고 대응 디지털 포렌식 준비도 절차를 기반으로 하고, 기업자산 및 개인정보를 자산으로 한다. 그리고 관련된 스마트워크 이용 행위 등과 관련된 시나리오를 정의하고, 각종 기관에서 발행한 스마트워크 가이드라인에서 요구하는 사항과 제한사항을 식별하는 분석이 포함된다는 점에서 일반적인 디지털 포렌식 준비도 절차와 구분된다.

<표 2> 디지털 포렌식 준비도 절차

절차	주요활동
디지털 증거 식별	• 조직 내 보유하고 있는 정보자산 식별 • 시나리오 정의 • 보안사고 식별 및 분류 • 잠재적 증거 식별
요구사항 식별	• 법적 요구사항 및 제한사항 식별 • 조직 내 요구사항 식별 • 근무 환경별 요구사항 식별 • 인적, 기술적, 정책적 요구사항 식별
구현 및 실행	• 디지털 증거 수집 및 보존 정책 수립 • 시스템 아키 ㅐㄱ처 정의 및 구현 • 포렌식 준비도 테스트 및 평가 • 증거 수집 및 보존(사전/실시간/사후) • 테스트 및 평가
지속적 관리	• 지속적인 모니터링 및 감사 • 지속적인 직원 교육훈련 및 인식제고

앞서 기존 디지털 포렌식 준비도 관련 문헌분석을 통해 디지털 포렌식 준비도 모델을 구성해보면 <표 3>과 같다. 본 모형은 크게 기술적인 부분과 정책적인 부분으로 나누어 반영하였다. 특히, 기술적 준비도 부분은 행위 분석에 초점을 맞추어 구성요소를 설계하였다.

본 모형은 스마트워크 환경 관련 비즈니스 프로세스와 위험 시나리오, 내부정보 유출에 대응하는 디지털 포렌식 준비도 모델로써, 기술적인 요구사항은 물론 비기술적인 정책 요구사항을 모두 포괄하고 있다. 또한, 조직 외부의 법적 요구사항은 물론 내부의 비즈니스 요구사항을 반영하여, 법적 증거능력 확보를 위한 무결성, 신뢰성 등의 요건을 만족하도록 구성하였다.

기술적인 요구사항으로는 유출 행위에 대한 분석에 초점(사람 중심)을 맞추어 선제적으로 내부정보 유출을 방지할 수 있도록 구성하였다. 노트북 및 PC의 데이터를 외장하드 및 USB를 이용하여 복제 및 반출하는 행위는 USB 및 외장하드 접속 및 데이터 전송흔적을 분석한다(레지스트리 및 윈도우 시스템 로그분석, 링크파일분석(최근 열어본 문서의 바로가기 파일 등).

메일을 통해 기밀문서에 대해 전송하는 행위는 e메일 전송 흔적 및 첨부 파일을 분석한다(아웃룩 데이터 파일(PST, OST) 분석, 기타 메일 데이터베이스파일의 복구분석). 데이터 삭제도구의 사용 흔적과 고의적으로 훼손하는 행위는 삭제도구 사용 흔적과 삭제 데이터를 분석한다(레지스트리 및 프리패치(실행프로그램 작동 흔적), 데이터 카빙을 통한 삭제데이터 복구).

기밀 문서 및 도면, 기획서 등의 자료에 대한 위·변조 및 복제하는 행위는 원본문서 작성자와 관련 문서 위·변조 여부를 분석한다(도큐먼트 메타데이터 분석, 해시 함수를 이용한 파일 무결성 분석, 퍼지해시를 이용한 파일 유사성 검증).

웹하드 및 기타 웹사이트 접속을 통해 정보를 유출하는 행위는 웹사이트 접속내역 분석과 공유네트워크 접속 흔적을 분석한다(웹 브라우저 사용흔적분석(임시인터넷폴더 분석), 네트워크관련 레지스트리 분석).

마지막으로 해당 매체의 사용자 확인 및 OS 설치 정보 확인을 위해 OS 설치정보 확인 및 타임라인을 분석한다(시계열 분석을 통한 사용자 이용패턴(정황)분석, OS 아티팩트 분석을 통한 설치정보분석).

<표 3> 디지털 포렌식 준비도 모형

영역		구성요소	설명
정책적 준비도	조직 외부	• 디지털 포렌식 관련 표준/가이드라인 준수 • 법적 요구사항 준수	• 증거에 대한 무결성/ 신뢰성 확보 • 적법 절차 준수 (적정성/ 객관성 확보)
	조직 내부	• 포렌식 솔루션 구비 (사전/정밀 분석 도구) • 포렌식 장비 구비 (쓰기방지 장치, 복제기 등) • 정보자산 식별 및 분류 • 보안서약서 등 확보 • 증거보존 시스템(서버) 구축 • 검증된 포렌식 도구 사용 • 전담 포렌식 부서(인력) 구성 • 증거보존 정책 수립 • 직원감사 정책 수립	• 신뢰성/ 객관성 확보 • 내부 감사에 대한 정당성 확보 • 원본증거의 안전한 보존 및 무결성 유지 • 증거의 경로 및 작업내역 기록
기술적 준비도	시스템 정보	• 시스템 기본 정보 분석 • 시스템 온/오프 시간 분석 • 네트워크 정보 분석 • 설치 프로그램 내역 분석 • 공유폴더 내역 분석 • 자동실행 프로그램 내역 분석 • 외장형 저장장치 연결 내역 분석	• 시스템 환경 분석 • 사용자 행위 분석 • 사용자 이용패턴 분석
	사용자 정보	• 사용자 계정 정보 분석 • 방문 웹사이트 정보 분석 • 포털 검색어 분석 • 최근 열어본 문서 분석 • 최근 실행한 프로그램 분석 • 실행한 명령어 분석	• 사용자 행위 분석
	타임 라인	• 윈도우 아티팩트 타임라인 분석 • 파일 MAC 타임라인 분석 • 타임라인을 통한 행위 분석	• 사용자 이용패턴 분석
		• 신속한 파일 검색 지원 • 확장자 변경을 통한 파일은닉 분석 • 검색파일에 대한 해시값 추출 • 비인가 파일 소유여부 분석 • 암호화 파일 탐색 및 암호해독	• 파일 본문 내 지정된 키워드 검색 제공 • 검색 신뢰도 향상 • 파일에 대한 무결성 보장 • 색인으로 인한 시스템 저하 방지
	단말기	• 플래시메모리 수집/획득 • microSD 카드 수집/획득 • USIM 카드 수집/획득	• 단말기 분석을 위한 데이터 수집 • 모바일 데이터 획득

4. 결론 및 향후연구

다양한 디지털 포렌식 준비도 관련 문헌 분석을 통해 기존 디지털 포렌식 준비도 절차 및 구조 모델 연구를 수행하였고, 기존 정보보호 중심의 보안사고 조사와 비교되는 디지털 포렌식 준비도에 대한 개념 및 특성을 알아보았다. 또한, 스마트워크 환경의 특성을 분석하고 추출하여 이를 반영한 스마트워크 환경 디지털 포렌식 준비도 모형 설계를 위한 구성요소들을 제안하였다. 그러나, 향후 연구를 통해 본 연구에서 제시한 디지털 포렌식 준비도 모형의 타당성을 평가하여 검증할 필요가 있다.

본 연구는 스마트워크 환경에서 디지털 포렌식 준비도에 대한 올바른 이해와 사회적 필요성을 명확히 정립하고, 디지털 포렌식 준비도 모형이 갖추어야 할 요구사항을 제시하여 연구를 수행하였다는 점에서 디지털 포렌식 연구 분야에 기여할 수 있을 것으로 예상된다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (H8501-17-1018)

참고문헌

[1] 신수연, "외국계 금융종사자가 인지하는 스마트워크 환경이 조직몰입과 혁신행동에 미치는 영향", 이화여자대학교 석사학위 논문, pp.1-108, 2014.

[2] 신용녀, 신승목, "대용량 디지털포렌식 서비스에 대한 실증적 연구", Internet and Information Security, Vol.1, No.2, pp.83-100, 2010.

[3] 노명선, "국제기준에 적합한 디지털포렌식 기술교육의 표준모델 개발", 미래창조과학부, 2012.

[4] 윤주희, 이동휘, 김미선, "활성 포렌식 기술을 활용한 피해 유형별 침해사고 대응 절차 연구", 융합보안논문지, Vol.16, No.4, pp.69-78, 2016.

[5] 김재천, "산업유형별 포렌식준비도 기반의 데이터 분석 및 검증 설계", 부경대학교 박사학위논문, pp.1-108, 2015.

[6] Tan, J., "Forensic Readiness", ATstake Inc, pp. 1-23, 2001.

[7] 백승조, 임종인, "개인정보보호 강화를 위한 포렌식 준비도 모델 및 도입방안 연구", Internet and Information Security, Vol.3, No.2, pp.34-64, 2012.