韓國컴퓨터情報學會 論文誌
第14卷 第12號, 2009. 12.
2009-14-12-3-4

포렌식 데이터의 실시간 수집 절차 모델링

김태훈*, 박남규**, 최한나**, 이대윤**, 안종득*, 조용환**

Modeling of Collection Process for Real-time Forensic Data

Tae-Hoon Kim*, Nam-Kyu Park**, Han-Na Choi**,

Dae-Yoon Lee**, Jong-Deuk Ahn*, Yong-Hwan Cho**

요 약

본 논문에서는 관리자가 시스템 운영과 감사 측면에서 침해사고에 대응하고 사고 발생 즉시 포렌식 데이터를 수집 분석 및 복구할 수 있는 포렌식 데이터의 실시간 수집 절차 모델을 제안한다. 제안한 모델은 기능 요소별로 구별된 7단계 절차를 가지며 추상적이고 관리적인 기존의 포렌식 절차와는 달리, 관리자가 시스템 운영과 감사 측면에서 침해사고에 대응하고, 사고 발생시 포렌식 데이터를 수집 분석 및 복구할 수 있는 절차들이 포함되어 있다. 또한 즉각적인 대응이 어려운 경우 기존의 절차와 마찬가지로 종합적이고 조직적인 대응이 가능하도록 대응 전략 체계화 단계를 통한 포렌식 데이터 수집 단계로의 피드백 절차를 둔다.

Abstract

This study proposes a model of collection process for real-time forensic data , in which the manager was to respond to infringement incidents in terms of system operation and inspection and to collect, analyze and restore forensic data immediately after an incident took place. The suggested model was modeled in seven processes according to functional elements. Unlike the old abstract and managerial forensic processes, the model allowed the manager to react to infringement incidents in the aspects of system operation and inspection and to follow the processes of collecting, analyzing, and restoring forensic data in case of an incident. There also was a feedback process designed towards the step of gathering forensic data through the stages of systematizing reaction strategies in order that he or she be able to bring about comprehensive and structural responses to an incident like the former processes in which it is difficult to bring about instant responses.

▸ Keyword : Digital Forensics, Forensics, hacking, Security, Crime

• 제1저자 : 김태훈 교신저자 : 조용환
• 투고일 : 2009. 05. 25, 심사일 : 2009. 06. 08, 게재확정일 : 2009. 12. 24.
* 주성대학 ** 충북대학교 전자정보대학
※ 이 논문은 2007년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음(This paper was supported by the research grant of the Chungbuk National University in 2007)

Ⅰ. 서 론

침해 사고 이후 복구 및 분석을 다루는 컴퓨터 포렌식(forensic) 분야는 선진 외국에서 국가적 전략 기술로 인정받으며 상당한 발전을 거듭해왔지만 국내에서는 최근에 일부 포렌식 도구들을 이용한 포렌식 절차 개발이 논의되기 시작 했다. 포렌식 절차는 침해사고가 발생한 경우 이를 철저히 조사하여 향후 동일한 사고가 발생되지 않도록 조치를 취하는 것이며, 사고 분석자가 취해야 할 단계별 침해사고 분석절차이다[1].

DFRWS(Digital Forensic Research Workshop)에서 제시된 디지털 포렌식 절차 모델은 2001년 First Digital Forensic Research Workshop의 결과 리포트로 식별(Identification), 보존(Preservation), 수집(Collection), 시험(Examination), 분석(Analysis), 공표(Presentation), 판결(Decision) 등 7가지 클래스로 구성되어 있다[2].

미국 법무부(The U.S Department of Justice)에서도 컴퓨터 포렌식 절차에 대한 연구를 계속해오고 있는데, 2001년에 미국 법무부 산하 법무연구소(National Institute of Justice)의 'Technical Working Group for Electric Crime Scene Investigation'에서 '전자적 범죄현장 수사 가이드(Electronic Crime Scene Investigation : A Guide for First Responders Series)'라는 지침서를 발행하였다[3].

이 지침서에서는 포렌식 절차를 특정한 기술이나 방법론에 의존하지 않고 수집, 시험, 분석, 보고 등과 같이 추상적인 포렌식 절차를 제시하고 있다.

Mandia와 Prosise는 포렌식 분석 절차를 침해사고 대응 방법론 측면에서 접근하였다. 침해사고 대응 절차는 준비단계, 침해사고 탐지단계, 초기대응, 대응전략 결정단계, 정밀조사를 위한 자료 이중화 단계, 조사단계, 보안조치 수행 단계, 네트워크 모니터링 단계, 복구 단계, 보고 단계, 후속조치 단계 등 11단계로 구성되었으며 Windows, UNIX, Cisco Router 등에 대한 다양한 방법론을 제시하고 있다[4].

2006년 11월 KISA(Korea Information Security Agency)에서 출판한 "침해사고 분석절차 가이드"에서는 Mandia의 침해사고 대응 절차를 그대로 따르고 있으며 침해사고와 포렌식 측면에서 절차 가이드를 제시하고 있다. 여기서 제시된 절차는 7가지 대응 요소로 나누어지며 그림 1과 같다[5][6].

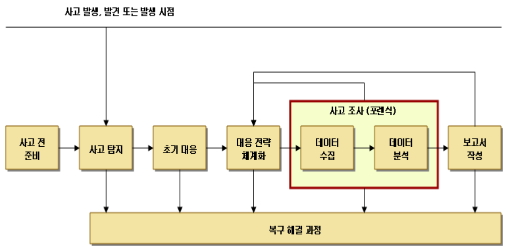


그림 1 침해사고 대응 7단계
Fig. 1 Infringement incidents response 7 phase

Mandia 와 KISA의 포렌식 절차는 침해사고 대응팀 등 조직적인 체계를 마련하고, 정보보호시스템 및 네트워크 장비를 이용하여 이상 징후를 탐지한 후 포렌식 절차를 수행하도록 되어 있다. 이 절차는 대규모 침해 사고가 발생하여 전면적인 조사가 필요할 경우에는 유용한 체계이지만, 일상적인 운영 차원에서의 즉각적인 사고에 대한 대응 절차로 사용하기에는 어렵게 구성되어 있다.

그러므로 침해사고 대응 절차는 대규모 사고가 발생하여 전면적인 조사가 발생할 경우 유용한 체계이지만 일상적인 시스템 운영 차원에서의 사고에 대한 대응 절차로 사용하기에는 어려움이 있다. 일상적인 시스템 운영 차원에서의 사고에 대한 대응 절차를 위해서는 시스템 관리자와 네트워크 관리자가 분리되어 있는 환경을 고려하여 각각에 대한 체계화된 대응 절차가 필요하다.

본 논문에서는 기존 포렌식 절차의 문제점인 추상적이고 관리적인 포렌식 절차를 벗어나 관리자가 실질적으로 침해사고에 대응할 수 있도록 포렌식 데이터의 실시간 수집 절차 모델을 제안한다.

Ⅱ. 포렌식 데이터의 실시간 수집절차 모델링

2.1 실시간 수집절차 모델 제안

제안한 모델은 크게 7단계로 구성 되어 있다. 이 절차는 추상적이고 관리적인 기존의 포렌식 절차와는 달리 관리자가 시스템 운영과 감사 측면에서 침해 사고에 대응하고, 사고 발생시 포렌식 데이터를 수집 분석하고 복구할 수 있도록 구성된다. 그림 2는 제안 모델의 절차 흐름도를 나타내고 있다. 여기서 제시된 절차는 그림 1의 침해 사고 대응 7단계와 같이 7단계 대응 요소로 구분되고 있지만 대응 방법과 절차를 달리하고 있다.

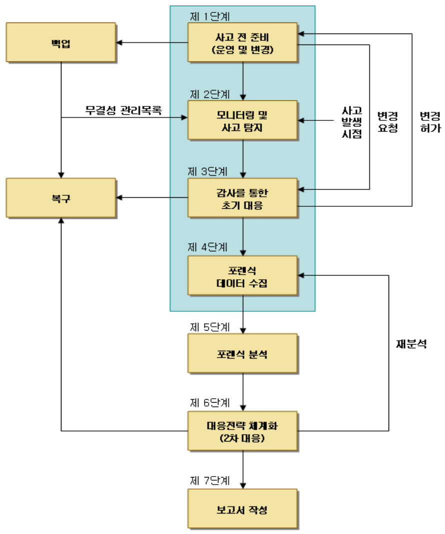


그림 2 제안 모델의 흐름도
Fig. 2 Flowchart of proposal model

2.2 모델의 단계별 프로세스

2.2.1 제 1단계 : 사고전 준비단계(운영 및 변경)

시스템 관리자들이 수행하는 일반적인 시스템 운영과 변경에 대해 관리하는 사고전 준비 단계이다.

침해 사고는 시스템의 운영이 관리자의 통제 및 예측을 벗어난 상태에서 운영될 때 발생된다는 것을 고려할 경우, 사건이 언제 어떤 방식으로 일어날지 알 수 없다. 사고전 준비 단계는 사고 대응 및 복구를 위해 평상시 시스템 운영 차원에서 수행되는 체계로서 그림 3과 같이 시스템 운영 관리, 시스템 백업 관리, 시스템 변경 관리 등의 기능요소로 구성된다.

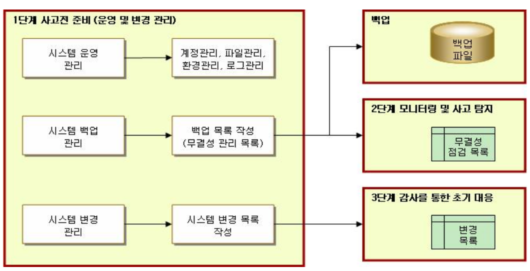


그림 3 사고전 준비 과정
Fig. 3 Preparation process before infringement incidents

시스템 백업 관리 기능 요소는 장애 또는 사고 발생 시 시스템 및 서비스를 복구하고 정상화시키기 위해 필요한 데이터를 백업하는 것이다. 시스템 백업관리를 위해 시스템 관리자는 백업할 데이터 목록을 작성하고 이를 기반으로 데이터를 백업하여야 한다. 백업 데이터 목록은 시스템 및 서비스 운영에 중대한 영향을 미치는 데이터들로 구성하며 제 2단계에서 시스템 관리자가 불법적인 시스템 변경을 감시하기 위한 무결성 점검 목록으로 사용한다.

시스템 변경 관리기능 요소는 시스템 및 응용의 패치, 업데이트, 구성 변경 등이 발생할 경우 시스템 관리자가 변경 계획 수립하고 변경하는 절차들로 구성된다. 시스템 변경 관리를 위해 시스템 관리자는 시스템 변경 목록을 작성하고 절차에 따라 변경 작업을 수행한다. 변경 작업이 이루어진 후 제 4단계에서 시스템 변경 목록과 비교하여 변경 범위 내에서 정확히 작업이 이루어졌는지 감사한다.

2.2.2 제 2단계 : 모니터링 및 사고 탐지

모니터링 및 사고 탐지 단계에서는 중요 시스템 파일 및 서비스 파일 등에 대하여 주기적으로 모니터링하고 무결성을 점검하며. 변경이 발생하였을 경우 침해사고로 식별하며, 그림 4와 같이 나타 낼 수 있다.

시스템 환경이나 주요 서비스 환경의 불법적인 변경을 시스템 관리 측면에서의 사고나 침입으로 분류한 후, 이를 모니터링 및 탐지하도록 하였다. 제 1단계의 시스템 백업 관리 기능 요소에서 작성된 백업 데이터 목록을 제 2단계에서 무결성 점검 목록으로 사용한다.

그림 5는 커널 레벨에서 실시간 감사를 수행하는 흐름도이다. 실시간 사고 탐지를 위하여 시스템 콜을 인터셉트하여 사용자 행위를 모니터링 하고 시스템 변경발생 시 실시간으로 탐지할 수 있도록 한다.

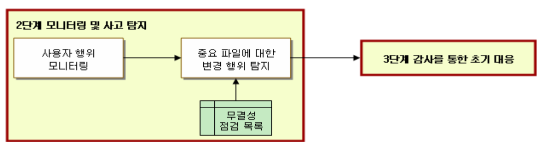


그림 4 모니터링 및 사고 탐지 과정
Fig. 4 Monitoring and infringement incidents detection process

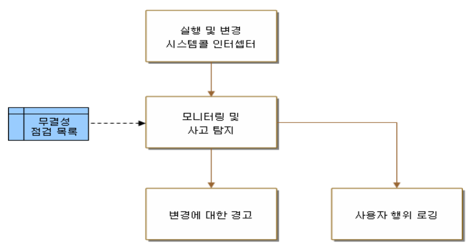


그림 5 커널 레벨에서의 실시간 감사
Fig. 5 Real-time inspection on kernel level

2.2.3 제 3단계 : 감사를 통한 초기 대응

감사를 통한 초기 대응 단계로서, 이 과정에서는 허가된 변경 범위 내에서 작업이 이루어 졌는지 또는 불법적인 변경이 발생하였는지에 대해 시스템 감사자에 의해 조사하게 된다. 감사를 통한 초기 대응은 그림 6과 같다.

제 2단계에서 시스템 변경이 발견되면 시스템 변경 요청이 있었는지 조사한다. 시스템 변경 요청이 없었을 경우 이는 불법적인 시스템 변경으로 보고 제 4단계인 포렌식 데이터 수집 단계를 수행한다.

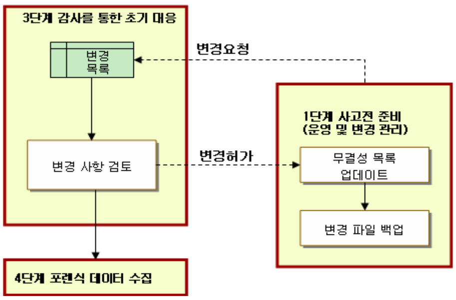


그림 6 감사를 통한 초기 대응 과정
Fig. 6 Initial response process in inspection

시스템 변경 요청이 있었을 경우 제 1단계의 시스템 변경 관리 과정에서 작성된 변경 목록과 비교한다. 허용된 범위를 벗어나 변경이 발생하였을 경우 불법적인 시스템 변경으로 보고 제 4단계 포렌식 데이터 수집 단계를 수행한다.

변경 목록과 비교하여 허용된 범위에서 작업이 이루어 졌을 경우, 다시 제 1단계로 돌아가 변경된 파일의 무결성 목록을 업데이트하고 변경 파일을 백업한다.

2.2.4 제 4단계 : 포렌식 데이터 수집

포렌식 분석을 위하여 필요한 휘발성 정보수집, 디스크 이미징, 시스템 정보 및 로그파일 수집하고 포렌식 분석 시스템으로 전송하는 포렌식 데이터 수집 단계이다[7][8][9].

휘발성 데이터는 사고 발생 즉시 수집되는 정보가 가장 유용하게 사용되며 시스템이 종료될 경우 복구할 방법이 없다. 따라서 포렌식 데이터 수집 모듈에서 가장 우선적으로 하는 것은 휘발성 데이터에 대한 수집이다. 휘발성 데이터에 대한 수집이 완료되면 정상적인 운영 상태에서 수집될 수 있는 시스템 정보 데이터, 시스템 로그 데이터, 사용자 행위 로그 데이터를 수집하고, 필요시 파일시스템에 대한 이미지를 생성하여 포렌식 분석 시스템에 전송한다.

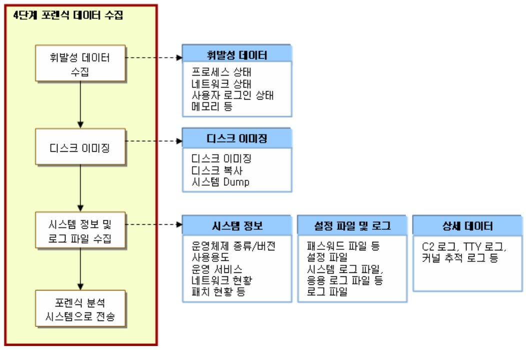


그림 7 포렌식 데이터 수집 과정
Fig. 7 Forensic data collecting process

2.2.5 제 5단계 : 포렌식 분석

수집된 포렌식 데이터를 이용하여 언제, 누가, 어떻게 사고가 일어났는지 분석하는 포렌식 분석 단계이며, 모든 수집된 정보의 전반적 조사를 의미한다.

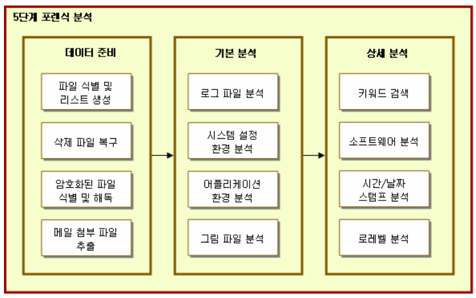


그림 8 포렌식 분석
Fig. 8 Forensic data analysis

그림 8과 같이 포렌식 분석을 위해서는 우선 파일을 식별하고 리스트를 생성하며 삭제된 데이터의 복구, 암호화된 파일의 식별 및 해독, 메일 첨부 파일의 추출 등 데이터 준비 단계가 필요하다.

다음으로 로그 파일에 대한 분석, 시스템 설정 환경에 대한 분석, 서비스 및 응용 환경의 분석, 그림 파일의 분석 등 기본분석 작업이 이루어진다. 또한 상세 분석이 필요한 경우 키워드 검색, 소프트웨어 분석, 시간/날짜 스탬프 분석, 로레벨 분석 등이 이루어진다.

2.2.6 제 6단계 : 대응 전략 체계화

포렌식 분석 결과를 기반으로 포괄적으로 재분석할 것인지, 자체 조치 사항인지 또는 수사기관 공조 사항인지 여부를

판단하는 대응 전략 체계화 단계이다.

대응전략 수립 단계에서는 주어진 사건의 환경에서 가장 적절한 대응전략을 결정하는 것이다. 대응전략은 침해 사고의 환경에 많은 영향을 받으며 정책, 기술, 법, 업무 등의 사고와 관련된 적절한 요인들을 고려해야 한다.

재조사가 필요한 경우 사고조사를 위해 얼마나 많은 자원이 더 필요한지, 증거의 완벽한 확보를 위해 저장 매체를 완전히 복사하는 포렌식 이미징 작업이 필요한지, 형사소송 또는 민사소송을 할 필요가 있는지, 대응전략에 다른 관점이 있는지를 결정해야 한다. 또한 대응 방법에 따라 조직이 영향을 받을 수 있기 때문에 대응 전략은 조직의 업무 목표를 고려해야 하며, 상위 관리자의 승인이 있어야 한다.

2.2.7 제 7단계 : 보고서 작성

보고서 작성은 가장 어렵고도 중요한 단계이다. 보고서를 읽게 되는 상급자 또는 소송 관련자들은 컴퓨터에 대한 기본 지식이 부족한 경우가 많기 때문에, 누구나 알기 쉬운 형태로 작성되어야 한다.

데이터 획득, 보관, 분석 등의 과정을 육하원칙에 따라 명백하고 객관적으로 서술해야 한다. 또한 사건의 세부 사항을 정확하게 기술하고, 의사 결정자가 이해하기 쉽게 설명되어야 하며, 재판 과정에서 발생하게 될 논쟁에 대응할 수 있도록 치밀하게 작성되어야 한다.

III. 제안 포렌식 절차 모델에 대한 고찰

표 1은 기존 포렌식 모델과 본 논문에서 제안한 포렌식 모델을 비교하고 있다.

기존 포렌식 절차 모델과 본 논문에서 제안한 포렌식 절차 모델을 비교하면 DEFWF 모델이나 JoD 모델과는 많은 차이를 보이고 있으나 Mandia/KISA 모델과 유사하다.

그러나 Mandia/KISA 모델은 추상적인 포렌식 모델인 반면 본 논문에서 제안한 포렌식 모델은 실질적인 시스템 포렌식 모델로 표 2에서 비교 하고 있다. Mandia/KISA 모델은 대응팀을 구성하고 협의체를 통하여 체계적으로 포렌식 절차를 수행하도록 되어 있다. 그러나 사건이 탐지되지 않으면 대응을 할 수 없는 구조로 되어 있으며 사건이 발생하고 문제화된 후 처리되는 구조로 포렌식 데이터에서 휘발성 데이터는 수집하기 어려우며 수집되는 다른 데이터에 대한 신뢰도가 떨어진다.

본 논문에서 제안한 모델은 사고 발생시 실시간으로 포렌식 데이터를 수집하여 분석하고 침입자를 추적할 수 있는 절차로 되어 있으며 즉각적인 대응이 어려운 경우 대응 전략 체계화를 통하여 재분석하는 구조로 되어 있다. 그러므로 시스템 운영 부서에서 쉽게 적용할 수 있는 구조이며 실시간 감사 체계를 통하여 실제 사이트에서 운영할 수 있다.

표 1 기존 포렌식 모델과의 비교
Table 1 Compare existed forensic model with proposal forensic model

	사전준비 (조직정비)	침해사고대응	데이터수집	데이터분석	공표	침해사고종결
DERWS 모델						
식별(Identification)		✔				
보존(Preservation)			✔			
수집(Collection)			✔			
시험(Examination)				✔		
분석(Analysis)				✔		
공표(Presentation)					✔	
판결(Decision)						✔
DoJ 모델						
수집(Collection)			✔			
시험(Examination)				✔		
분석(Analysis)				✔		
보고(Reporting)					✔	
Mandia / KISA 모델						
준비(Preparation)	✔					
사고탐지(Intrusion Detection)		✔				
초기대응(Initial Response)		✔				
대응전략(Response Strategy)		✔				
데이터수집(Data Collection)			✔			
데이터분석(Data Analysis)				✔		
보고(Reporting)					✔	
제안 모델						
사고전 준비		✔				
모니터링 및 사고탐지		✔				
초기대응		✔				
데이터 수집			✔			
데이터 분석				✔		
대응전략 체계화		✔				
보고					✔	

표 2 포렌식 절차 비교
Table 2 Compare forensic process

구분	기존 포렌식 절차 (Mandia / KISA 모델)	제안 절차
1 단계	사고전 준비	사고전 준비
	침해사고 대응팀 등 조직적 정비 필요	시스템 운영 절차에 따른 준비과정 수행
2 단계	사고 탐지	모니터링 및 사고 탐지
	정보보호 및 네트워크 장비에 의한 이상 징후 탐지 ⇒ 사고 식별에 따른 오판이 있음	시스템 변경 및 운영 감사에 따른 사고 탐지 ⇒ 사고 식별에 따른 오판이 적음
3 단계	초기 대응	감사를 통한 초기대응
	사고 대응팀 소집 및 관련 부서 통보 ⇒ 사고 발생 후 초기대응에 대한 시간이 소비됨	변경 범위 내에서 작업이 이루어졌는지 조사 ⇒ 사고 발생 후 즉각적인 초기 대응이 가능
4 단계	대응 전략	포렌식 데이터 수집
	주어진 사건의 환경에서 가장 적절한 대응전략 결정 - 정책, 기술, 법, 업무 등의 사고와 관련된 적절한 요인 고려	사고 탐지 즉시 데이터를 수집하여 휘발성 데이터를 포함한 충분한 포렌식 데이터를 확보할 수 있음
5 단계	데이터수집	포렌식 분석
	호스트 기반정보, 네트워기반정보 그리고 일반정보 수집 ⇒ 시간이 많이 소요되고 경우 증거 자료의 인멸의 우려가 있음	조직적이고 체계적인 대응 전략 수립 후 승인 ⇒ 데이터 수집 및 분석에 따라 대응 전략을 수립함으로써 증거 자료의 우선 확보 및 체계적 대응이 가능
6 단계	데이터 분석	대응 전략 체계화
	수집된 정보의 전체적인 조사 ⇒ 사고탐지 후 초기 대응, 대응전략 체계화 후 데이터를 수집하여 분석하므로 충분한 포렌식 데이터를 확보하기 어려움	대응전략 체계화에 따른 세부 분석이 필요할 경우 이에 따른 추가 포렌식 데이터를 수집하고 분석하여 증거 데이터를 확보
7 단계	보고서 작성	보고서 작성
	의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서 작성	의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서 작성

IV. 결 론

본 논문에서는 관리자가 시스템 운영과 감사 측면에서 침해사고에 대응하고 사고 발생 즉시 포렌식 데이터를 수집 분석 및 복구할 수 있는 포렌식 데이터의 실시간 수집 절차 모델을 제안하였다.

제안된 모델은 기능 요소별로 구별된 7단계 절차로 모델링 하였다. 각 기능요소는 제 1단계에 사고 전 준비(운영 및 변경), 제 2단계에 모니터링 및 사고 탐지, 제 3단계에 감사를 통한 초기 대응, 제 4단계에 포렌식 데이터 수집, 제 5단계에 포렌식 분석, 제 6단계에 대응 전략 체계화 그리고 제 7단계에 보고서 작성으로 구성하였다. 제안된 모델은 추상적이고 관리적인 기존의 포렌식 절차와는 달리, 관리자가 시스템 운영과 감사 측면에서 침해사고에 대응하고, 사고 발생시 포렌식 데이터를 수집 분석 및 복구할 수 있는 절차들이 포함되어 있다. 또한 즉각적인 대응이 어려운 경우 기존의 절차와 마찬가지로 종합적이고 조직적인 대응이 가능하도록 대응 전략 체계화 단계를 통한 포렌식 데이터 수집 단계로의 피드백 절차를 두었다.

향후 제안된 실시간 수집 절차 모델을 바탕으로 사고 발생 즉시 이를 탐지하여 행위로그, 보안로그, 휘발성 데이터 등을 수집할 수 있도록 실시간 수집 시스템을 설계하고 구현하는 과정이 필요하다. 그리고 시스템 포렌식 분야뿐만 아니라 네트워크 포렌식 분야까지 확장된 포렌식 데이터 수집 체계에 대한 연구가 요구되며, 또한 포렌식 데이터 수집에서 포렌식 데이터 분석까지 새로운 모델의 수립과 감사대상의 정보 축약 등 확대된 연구가 필요하다.

참고문헌

[1] Palmer, Gary L., "A Road Map for Digital Forensics Research – Report from the First Digital Forensics Research Workshop (DFRWS)," 2003
[2] N. L. Beebe, J. G. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," Digital Forensics Research Workshop (DFRWS), 2004.
[3] DoJ, "Electronic Crime Scene Investigation – A Guide for First Responders," U.S. Department of Justice, pp. 1-82. 2001
[4] Kevin Mandia & Chris Prosise, "*Incident Response : Investigating Computer Crime*" Osborne/McGraw-Hill, 2001.
[5] Kevin Mandia, Chris Prosise and Matt Pepe, "*Incident Response & Computer Forensics, (Second ed.)*," McGraw-Hill/Osborne, Emeryville, 2003.
[6] "침해사고 분석 절차 가이드," 한국정보보호진흥원, 2006년 11월
[7] 오세민, "*컴퓨터 포렌식스를 위한 휘발성 정보 수집 분석 시스템 설계 및 구현*" 대전대학교 박사학위논문, 2007년 2월.
[8] Ieong R. S. C. (2006), "FORZA – Digital forensics investigation framework that incorporate legal issues", Digital Forensics Research Workshop (DFRWS), 2006.
[9] Ieong R. S. C. and Chau H. C. (2007), "Deriving case specific live forensics investigation procedures

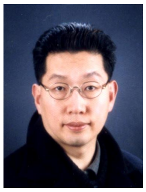
from FORZA," ACM SAC 2007.
〔10〕 이형우, "컴퓨터 포렌식스 기술," 한국정보보호학회 제12권 제5호, 8-16쪽, 2001년 10월.
〔11〕 정익래, 홍도원, 정교일, "디지털 포렌식 기술 및 동향," 전자 통신 동향분석 제22권 제1호, 2007년 2월.

저 자 소 개

김 태 훈
1997 - 현재 : 주성대학 교수
1990 : 경북대학교 전자공학과 공학석사
1990 - 1997 :
하이닉스 반도체 선임연구원
2008 : 충북대학교 컴퓨터공학과 공학박사
관심분야 : 유비쿼터스 , 홈네트워크, 서버보안

박 남 규
2000 - 현재 :
충북대학교 전산정보원 조교
2007 - 현재 :
충북대학교 컴퓨터공학과박사과정
2004 :
충북대학교 전기전산공학과 공학석사
관심분야 : 디지털방송, 모바일컴퓨팅, 유비쿼터스

최 한 나
2009 :
충북대학교 컴퓨터공학과 박사수료
2006 - 현재 :
우송대학교 컴퓨터공학과 겸임교수
관심분야 : 디지털 음향, 게임사운드 디자인, 유비쿼터스



이 대 윤
2007 - 현재 : 충북대학교 컴퓨터공학과 박사수료
2004 - 2006 : 계명대학교 애니메이션과 교수
1985 : 미국, NYIT Graduate School, Computer Graphics Dept.
관심분야 : 디지털방송, 3D Animation, 유비쿼터스

안 종 득
1998 - 현재 :
주성대학 e스포츠게임과 부교수
1995 :
청주대학교 컴퓨터공학과 공학석사
2003 :
충북대학교 컴퓨터공학과 박사수료
관심분야 : ERP, CRM, 기업정보화 등

조 용 환
1982 - 현재:
충북대학교 전자정보대학 교수
현재 : (사)한국엔터테인먼트산업학회 수석부회장
1989 : 고려대학교 이학박사
관심분야 : U-healthcare, 유비쿼터스컴퓨팅, 멀티미디어통신