情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

디지털 포렌식 도구를 활용한 기업의 대규모 정보감사 적용 방안

홍 정 민*, 김 종 현**

요 약

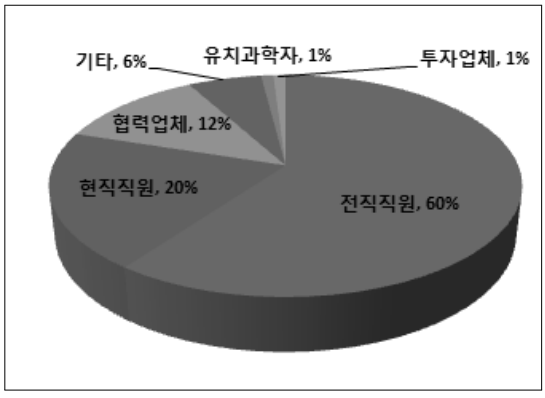
기업은 퇴직자, 외부용역, 협력업체 등의 감사, 내부고발 및 정보유출 등을 확인하기 위한 많은 노력을 기울이고 있다. 하지만 감사 대상 분석을 위한 인력 충원의 어려움, 비용 소모 및 소요 시간 증가, 업무 효용성 저하 등을 비롯하여, 지속적으로 늘어나는 정보량으로 인해 정보감사 수행에 어려움을 겪고 있다. 본 연구의 목적은 정보감사 수행시간의 단축 및 협업 등을 위하여 디지털 포렌식 분석도구인 AccessData社의 AD LAB을 활용하여 효율적인 정보감사를 수행할 수 있는 적용 방안을 제시한다.

Ⅰ. 서 론

최근 기업 내 기밀유출 사례의 80%는 해킹이나 산업 스파이 등의 원인으로 발생하는 외부적 원인보다 퇴직 또는 이직을 하였거나 계획하고 있는 사내 임직원을 통해 이뤄지는 내부적 원인의 경우가 많다. [그림 1]은 2008년부터 2012년까지 산업기밀보호센터에서 조사된 총 202건의 기술유출사례를 보여준다. 이 중에서 기술유출 주체의 60%가 전직직원으로 가장 높았으며, 현직 직원 20%, 협력업체 12% 등의 순으로 집계된 것 확인할 수 있다.[1]

내부 정보 유출은 USB, 외장 하드디스크 등의 외부 저장매체를 사용하여 복사 및 이동될 수 있으며, 온라인 메신저나 이메일 등으로 발생될 수 있다. 더욱이 외부 인터넷이 가능하며, 외장형 저장장치로 활용할 수 있는 스마트 폰의 급격한 보급으로 본 매체를 통한 정보유출에 대한 대응이 시급히 필요하다. 이와 같은 정보 유출 방지를 위해서는 다양한 매체에 대한 통제가 가능하도록 로그 기반 정보 유출 판별 또는 업무와 불필요한 사이트의 접근 확인에 대한 모니터링 등을 통해 정보의 유통 흐름과 직원의 행위에 대한 흐름을 파악할 수 있어야 한다. 더불어 정보감사를 실시하여 내부자가 정보를 어떻게 취급하고 있는지를 관리하고, 단순히 정보 유출을 통제하는 것이 아니라 정보의 수집 및 저장 등에 대한 전반적인 흐름을 관리할 수 있는 정보보안 강화에 힘써야 한다.

하지만 기업 내 모든 임직원에 대한 정보감사를 수행하기 위해서는 많은 시간이 소요되며, 분석을 위한 인력 충원 문제를 비롯하여 정보감사 진행으로 인해 직원들의 업무 효용성도 저하될 수 있다. 그러므로 분석 주체를 신속히 파악하여 정보감사를 진행할 수 있도록 감사



〔그림 1〕 국내 기술유출 주체

* 더존정보보호서비스 포렌식센터 (brentkorea@duzon.com)
** 더존정보보호서비스 포렌식센터 (joseph@duzon.com)

계획 단계부터 감사대상에 대한 정의, 수행기간 등을 명확히 수립하고, 대상 매체를 수집 및 분석하여 보고하는 일련의 과정을 통해 효율적인 감사 수행이 가능하도록 해야 한다. 이에, 대상 매체에 대한 수집과 내부적인 분석을 수행하는 과정에서 소요되는 시간을 단축하고, 다양한 분야의 전문가와 협업을 수행할 수 있도록 디지털 포렌식 분석 도구인 AccessData社의 AD LAB을 활용하는 방안을 제안한다.

Ⅱ. 디지털 포렌식 및 활용분야

2.1 디지털 포렌식(Digital Forensics)

디지털 포렌식은 컴퓨터 범죄와 관련하여 디지털 기기에 있는 전자적 정보를 과학적 절차와 기법을 사용하여 복구 및 조사하는 제반 행위를 포괄하는 법 과학이다. 이는 디지털 데이터를 저장할 수 있는 모든 장치를 대상으로 디지털 증거의 수집, 보존, 분석에 대한 보고서를 작성하여 형사 또는 민사 소송에 대한 범죄의 직접적인 증거로 제출되거나 특정 알리바이 및 진술에 대한 확인, 식별, 인증 등을 위해 사용될 수 있다.

디지털 포렌식은 디지털 장치의 유형에 따라 컴퓨터 포렌식, 네트워크 포렌식, 포렌식 데이터 분석, 모바일 포렌식 등으로 나뉘어 분류하기도 하며, 일반적으로 사이버 범죄수사, 침해사고 대응 등에 활용되고 있다.[2]

2.2 포렌식 어카운팅(Forensic Accounting)

기업이 부정적인 목적으로 재정 상태나 경영실적을 부풀리려는 분식회계를 비롯하여, 비정상적인 자금 운용 등의 복잡하고 다양한 방법으로 재무 조작행위를 하는 것을 회계부정이라고 한다. 그러므로 회계부정에 대한 정보를 검증할 수 있는 회계증거를 찾는 기술이 필요하였으며, 해외에서는 회계 정보를 대상으로 사건의 조사, 감사 등과 융합하여 수행할 수 있는 연구가 활발히 진행되고 있다. 이와 같이, 법정에서 사용될 수 있는 증거와 회계 자료를 제출하는 과정을 모두 포함하며 회계 및 감사 기법에 대한 배경 지식이 필요한 분야를 의미한다.

포렌식 어카운팅을 위한 도구로는 해외에서 가장 높은 점유율을 가지고 있는 ACL(Audit Command Language)과 CASEWARE社에서 개발한 IDEA, 벤포드 법칙을 활용한 미국의 DATAS Software 등이 있다.[3]

2.3 정보감사(The Information audit)

조직의 정보 관리 시스템에 대한 회계 및 재무의 범위에서 총체적으로 감사의 개념을 확장한 것을 의미한다. Orna, Henczel, Wood 등의 학자들은 “조직 내부자와 문서에 대한 정보 자원의 사용 및 흐름에 대한 체계적인 조사를 의미한다고 하였다. 하지만 정보감사의 정의를 명확히 한정짓기에는 어려움이 있다.[4]

이를 통해 정보감사를 수행하는 목적은 조직의 정보 자원 확인을 비롯하여 정보 자원의 비용, 정보 활용에 대한 이점 파악, 비즈니스와의 통합, 정보 흐름 및 처리 등을 식별하여 정책 및 전략을 수립할 수 있도록 하는데 있으며, 정보 자원 관리(IRM, Information Resource Management)의 중요성을 인식할 수 있다.[5]

단순히 기업의 정보만 통제하는 것이 아니라 내부 직원을 통한 정보누수 사례에 대해 사람 관리에 초점을 맞추고, 시나리오 기반, 원시 로그 기반의 정보유출 여부에 대한 판단을 수행하기도 한다.[6]

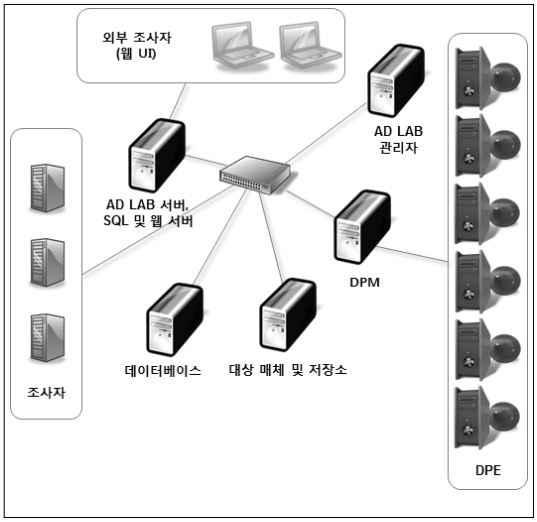
Ⅲ. 기업 정보감사를 위한 디지털 포렌식 도구

3.1 시스템 구성도

디지털 포렌식 분석을 위한 도구로는 Guidance社의 EnCase, AccessData社의 Forensic Toolkit 등이 사용되지만, 대부분 분석 매체에 대하여 단일 조사자가 조사를 수행할 수 있는 도구들이다. 그러므로 조사에는 많은 시간이 요구되며, 조사 매체의 내용이 조사자의 전문 분야가 아닌 경우, 해당 분야의 전문가를 필요로 할 수 있다.[7]

정보감사는 감사 매체에 대한 수집, 분석 등이 디지털 포렌식의 조사 방법과 유사하다. 이 때, 디지털 매체에 기록된 내용을 도구를 활용하여 사전 분석(수집)하는데 소요되는 시간을 비롯하여 다양한 분야의 전문가들과 조사자간의 협업을 통해 분석된 매체에 대한 증거 탐색 시간을 단축시키기 위해서 AD LAB을 구성하여 적용할 수 있으며, 시스템 구성은 [그림 2]와 같다.

대상 매체에 대한 사전 분석에 소요되는 시간을 단일



〔그림 2〕 AD LAB 구성도

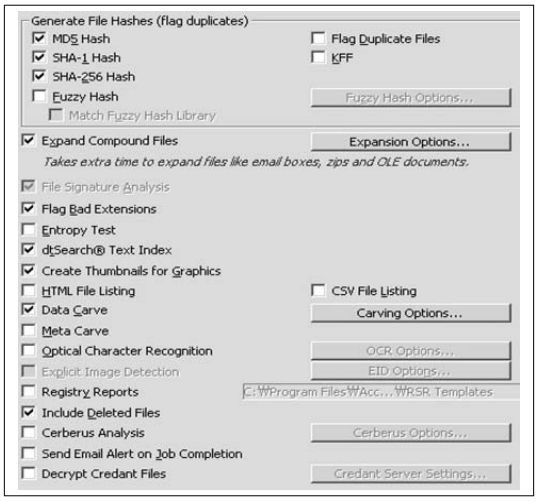
장비와 비교하기 위해 [그림 2]의 AD LAB 서버, SQL 및 웹서버, DPM(Distributed Processing Manager;분산 처리 매니저)과 DPE (Distributed Processing Engine; 분산 처리 엔진)의 총 8대에 대한 동일한 하드웨어(HP DL160 Gen8)를 구성하여 사전 분석 소요시간을 테스트 하였다. AD LAB 서버의 하드웨어 구성은 [표 1]을 통해 확인할 수 있으며, 나머지 7대는 HDD a 유닛 1개(HDD b 제외)로 동일하게 구성되었다. 또한, 운영체제는 모두 Windows Server 2008 R2 Standard SP1 x64 한글버전에서 AD LAB 4.0.2를 기준으로 결과를 산출하였다.

〔표 1〕 하드웨어 구성

Item	Type	Unit
CPU	Intel Xeon Quad-Core E5-2603	1
RAM	8GB PC3-10600(LRDIMM)	1
HDD a	HP 500GB 7.2K SATA 3.5"	2
HDD b	Seagate 1TB SATA 3.5"	1
Network	1Gigabit	1

3.2 구동 소요시간 측정

대상 매체에 대한 사전 분석을 위하여 [그림 3]과 같이 AD LAB에서 기본적으로 제공되는 파일의 해쉬 생성, dtSearch, 그래픽 썸네일 생성 등의 옵션과 함께 Data Carve를 추가로 선택하였다. 그리고 분석에 소요



〔그림 3〕 프로세싱 옵션 선택 창

되는 시간을 비교하기 위해서 DPE의 구성 수를 변화시켜 사전 분석에 소요되는 총 작업 시간을 확인하였다.

사전 분석 대상이 되는 데이터 셋은 [표 2]와 같이, 가상의 수집된 PC매체(120GB HDD의 이미지 파일;E01)를 대상으로 하였다.

[표 2] 사전 분석 대상 데이터 셋의 항목 및 개체 수

항목	개체 수
Archives	1,237
Databases	99
Documents	55,840
Email	604
Executable	170
Folders	7,823
Graphics	437,564
Multimedia	2,092
OS/File System Files	3,360
Other Encryption Files	48
Other Known Types	188,749
Presentations	5,683
Slack/Free Space	64,362
Spreadsheets	13,019
Unknown Types	15,835

[표 3]은 120GB HDD의 이미지에 대한 사전 분석 소요 시간을 비교한 것으로 단일 환경에서 사전 분석에 소요되는 시간은 약 10시간 42분이지만, DPE의 개수를 증가시켜 분산 처리를 수행하게 되면 약 1/3가량의 시간을 단축시킬 수 있다는 사실을 확인할 수 있다. 하지만 결과에서 확인할 수 있듯이 DPE의 개수를 지속적으

〔표 3〕 사전 분석 소요 시간 비교

DPE 구성	A	B	C	D
0	10:42:11	09:41:37	00:40:11	10:41:00
2	06:57:56	06:33:41	00:20:38	06:57:14
3	05:43:38	03:25:18	00:21:18	05:42:40
4	04:33:30	02:17:45	00:20:44	04:32:41
5	03:46:16	02:07:24	00:20:12	03:45:28
6	03:33:55	02:03:03	00:12:43	03:33:06

* A:Total Job Time, B:Processing Time, C:Postprocessing Time, D:Indexing Time

로 증가시키는 만큼 시간이 단축되지 않는 다는 것을 알 수 있으며, 합리적인 구성을 위해서는 DPE의 개수를 4~5개로 할 수 있다.

이와 같은 테스트 결과를 통해 사전 분석에 소요되는 시간을 줄일 수 있으므로 감사 대상 매체에 대한 총 분석 시간을 감소시킬 수 있다.

3.3 정보감사의 활용 및 효과

감사 수행자는 감사 대상 매체에 대하여 3.2장에서와 같은 사전 분석을 수행한 후, 분석을 수행할 수 있다. 먼저 대상 매체에 대한 감사 증거 수집을 위한, 사전 분석을 위해서 DPM 및 DPE를 사용하여 단일 조사도구에 비해 사전 분석시간을 단축시킬 수 있다.

수집된 대상 매체는 저장소에 저장되어 관리할 수 있으며, 해당 매체에 대한 조사는 AD LAB 서버를 통해 다수의 조사자가 직접 접근하여 분석할 수 있다. 이 경우, 단일 매체에 대하여 역할을 맡은 조사자들이 분산된 분석을 수행하여 데이터베이스에 저장할 수 있다. 게다가 다양한 분야의 전문가들이 웹 UI환경을 사용하여 의견을 제시하거나 조사를 수행할 수 있도록 구성되어 있기 때문에 전 과정에 대한 동시 조사가 가능하여 조사 시간을 단축시킬 수 있다는 장점도 있다.

이와 같은 시스템을 구성하기 위해서는 초기 구축을 위한 높은 비용을 감수해야 할 수 있다. 하지만, 이는 단기적인 관점에서 일시적인 소비가 증가할 수 있는 부분이며, 장기적인 관점에서는 비용 절감과 더불어 데이터 관리, 분석 등이 효율적이다. 영국 헌병대(RMP;The Royal Military Police)의 사례를 살펴보면, 사이버 범죄 센터에 분산 처리 기술을 활용할 수 있는 AD LAB을 도입/구성하였고, 케이스 백 로그의 42%를 줄이고 초기 케이스 비용을 약 1/3감소시키는 결과를 얻었다.[8]

Ⅳ. 결 론

기업 내부의 정보 유출 사례에 대한 주체가 전직 또는 현직 직원과 같은 내부 임직원에 의한 발생율이 대다수이므로 이를 방지하기 위한 기업 내부자에 대한 정보감사가 필요하다. 하지만 기업의 규모, 감사 대상자 선택, 감사 대상 매체 확보, 분석 등에 대한 시간 소모가 많으며, 동일한 감사 매체에 대한 분석을 위한 전문가와의 협업도 어렵다.

본 연구에서는 정보감사에 대한 총 수행 시간을 단축시킬 수 있도록 디지털 포렌식 분석 도구를 활용하는 방안을 제안하여, 다양한 분야의 전문가와 협업이 가능하도록 하고, 사전 분석에 대한 시간을 단축시킬 수 있다는 것을 확인하였다.

총 8대의 하드웨어 장비에 대한 동일한 설정으로, 사전 분석을 위한 시간 비교를 위하여 120GB의 데이터 셋에 대한 테스트 결과, 단일 장비에 대하여 5개 DPE 이상 사용할 경우 약 1/3의 시간을 단축할 수 있다는 결과를 얻었다. 더불어 여러 대상 매체에 대한 사전 분석을 동시에 처리할 수 있고, 사전 분석을 위한 서버를 사용하여 데이터 관리를 유용하게 할 수 있으며, 웹 UI를 제공함으로써 다양한 분야의 전문가들과 협업을 가능하게 한다.

향후 본 도구를 활용하여 비용 대비 효과적인 하드웨어 구성을 통해, 동시다발적인 감사 대상 매체에 대한 사전 분석에 대한 검증을 수행한다면, 더욱 효율적인 대규모 정보감사를 수행하는데 기여할 수 있을 것이다.

참고문헌

[1] NIS 산업기밀보호센터, “기술유출 통계”, *http://service4.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00*,2012년

[2] Wikipedia, "Digital Forensics", http://en.wikipedia.org/wiki/Digital_forensics, last modified July 2013

[3] 최재민, 이상진, 임종인, “포렌식 어카운팅 기술 동향”, *정보보호학회지*, 18(1), 2008년 2월

[4] Buchanan, S. and Gibb, F., “The information audit: Methodology selection”, *International Journal of Information Management*, 28(1), 2008

[5] Buchanan, S. and Gibb, F., “The information audit: Role and scope”, *International Journal of Information Management*, 27(3), 2007

[6] 전상덕, 홍동숙, 한기준, “디지털 포렌식의 기술 동향과 전망”, *정보화정책*, 13(4), 2006년

[7] ZDNetKorea, “LG전자 정보감사...‘사람관리’에 무게”, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20121009100504, 2012년

[8] ComputerWeekly, "Royal Military Police cuts digital forensics costs with distributed processing", *http://www.computerweekly.com/news/2240181162/Royal-Military-Police-cuts-digital-forensics-costs-with-distributed-processing*, April 2013

〈著者紹介〉

홍 정 민 (Jeongmin Hong)
정회원

2011년 2월 : 인제대학교 컴퓨터공학과 졸업
2011년 2월~2013년 2월 : 고려대학교 정보보호대학원 금융보안학과 석사
현 : 더존정보보호서비스 포렌식센터 연구원
<관심분야> 금융보안, 디지털 포렌식, 정보보호

김 종 현 (Jonghyun Kim)
정회원

2000년 2월 : 아주대학교 정보컴퓨터공학 졸업
2009년 9월~현재 : 고려대학교 정보보호대학원 석사과정
현 : 더존정보보호서비스 포렌식센터 센터장
<관심분야> 디지털포렌식, eDiscovery, 침해사고대응