Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.369

DRM 로그분석을 통한 퇴직 징후 탐지와 보안위협 사전 대응 방법

현 미 분,† 이 상 진‡
고려대학교 정보보호대학원

The Proactive Threat Protection Method from Predicting Resignation Throughout DRM Log Analysis and Monitor

Miboon Hyun,† Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

기업 대부분은 사업 연속성을 위협하는 기밀정보 유출을 방지하기 위해 DRM, 메일 필터링, DLP, USB 보안 등 다양한 보안 시스템 구축에 투자를 아끼지 않고 있다. 그러나, 기업이 기밀정보의 유출 및 관련 사건을 인지한 시점에는 해당 직원이 이미 '퇴직'해 인사적 조치가 어렵고 관련 증거도 퇴직과 함께 사라져 버리는 경우가 많다. 그런 측면에서 퇴직 징후를 미리 탐지하고 사전 조치를 하는 것은 매우 중요하다. 데이터의 최소 단위인 파일을 대상으로 이루어지는 사용자 행위를 기록하는 DRM 로그를 활용하면, 퇴직 예측이 장·단기적으로 가능하므로 유출 행위를 예방하고 사후 증적으로도 활용할 수 있다. 이 연구는 직원의 퇴직 징후를 예측해 사전에 모니터링하는 프로세스를 수립함으로써, 퇴직자의 기밀 유출로 인한 기업 손실을 최대한 방지할 수 있는 방안을 제시한다.

ABSTRACT

Most companies are willing to spend money on security systems such as DRM, Mail filtering, DLP, USB blocking, etc., for data leakage prevention. However, in many cases, it is difficult that legal team take action for data case because usually the company recognized that after the employee had left. Therefore perceiving one's resignation before the action and building up adequate response process are very important. Throughout analyzing DRM log which records every single file's changes related with user's behavior, the company can predict one's resignation and prevent data leakage before those happen. This study suggests how to prevent for the damage from leaked confidential information throughout building the DRM monitoring process which can predict employee's resignation.

Keywords: DRM, Log Analysis, Outlier Detection, Prediction, Monitoring Process, Proactive Threat Detection

I. 서 론

최근 IT 기술 발전으로 기업이 소유하고 있는 주요 기밀은 종이 같은 물리적인 형태에서 벗어나 전자파일, 이진 데이터 등의 논리적 형태로 변모했다. 이로 인해 기업의 기밀 유출을 육안으로 즉시 확인할 수 없는 경우가 많다. 법무부 통계 자료에 따르면, 검찰이 처리한 기술 유출 범죄 사건은 99년 총 39건(95명)에서 09년 292건(807명)으로 꾸준히 증가했다[1]. 또한, 산업기술보호센터의 발표에 따르면 국내 기술의 해외 불법 유출 사례가 04년 26건에서 10년 41건을 기록한 이후 2013년까지 급증하고 있

Received(01. 11. 2016), Modified(03. 03. 2016), Accepted(03. 03. 2016)
† 주저자, miboonhyun@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

다. 발표 기관에 따른 편차가 있긴 하나 지난해 산업 기술 유출에 따른 피해액은 수조 원에 이르고 있다.

이와 같은 기밀 유출 사건이 꾸준히 증가함에 따라 관련 법률(부정경쟁방지법, 산업기술보호법)의 보호를 받기 위한 효율적인 수단으로 많은 기업들이 DRM(Digital Right Management)을 사용하고 있다. 이는 재판의 쟁점이 되는 '영업비밀'의 성립에 중요한 요건인 '상당한 노력에 의하여 비밀로 유지'라는 항목을 충족시킬 수 있기 때문이다[2].

기업망에 구축된 네트워크 보안장비, 서버와 달리 PC는 정보 유출의 직접적인 창구로써 역할한다. DRM이 설치된 PC는 정보 유출 시도 시 로그에 그 행위가 기록될 가능성이 매우 높다. 결국 DRM 로그 분석은 정보 유출 시도를 탐지·증명하는데 매우 큰 역할을 한다. 하지만, PC에 DRM 설치 사실을 인지한 정보 유출자는 이를 우회하고자 하므로 사용자의 행위를 통계적으로 분석·패턴화해 유출 가능성이 높은 사용자를 사전에 선별·모니터링하는 방법이 필요하다. 이 연구는 DRM 로그를 분석함으로써 기밀 유출 가능성이 높은 사용자, 특히 퇴직 예정자를 사전에 판별해 조치함으로써 유출 가능성 및 유출 리스크를 현저히 낮추는데 목적이 있다.

II. 퇴직자에 대한 설문조사

중소기업청의 중소기업 산업기밀관리 실태조사 보고서에 따르면, 퇴직사원(62.9%)과 현직사원(23.5%)이 주요 기밀을 유출한 것으로 조사되었다[3]. 직원 대부분은 평소 대량의 중요 데이터를 백업하거나 외부매체에 별도 저장하지 않다가 데이터를 활용하고자 하는 목적이 생겼을 경우(예를 들면, 퇴직 3개월 전 퇴직을 결심하게 된 상황) 이와 같이 행동함을 이직 경험자(20명)의 설문조사를 통해 Fig. 1과 Fig. 2와 같이 확인할 수 있다.

Fig. 1과 Fig. 2와 같이 기밀 유출은 재직 중 매체, 웹 스토리지, 인쇄물을 통해 데이터를 저장 후 퇴직 시 가지고 나가는 경우가 대부분이며, 퇴직 시 데이터의 대량 '저장'과 '삭제'를 하지 않는 경우는 매우 적었다. 또한 데이터 유출 여부와 상관없이 퇴직 시에는 개인 자료를 삭제하는 일이 빈번하게(33%) 발생하였다.

여기서 주의해야 할 또 다른 활동은 '종이 출력(Fig. 2의 14%)'으로 직원 대부분은 회사의 네트워크를 통해 송수신하는 데이터와 PC 작업 내용이 모

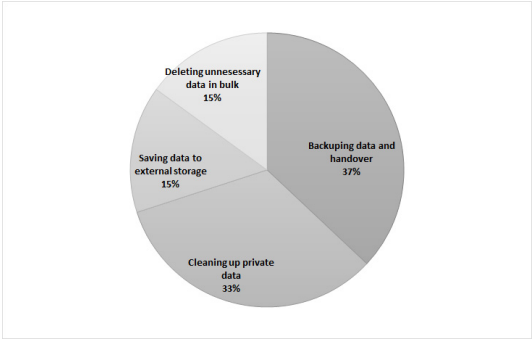

Fig. 1. Survey result of "Behavior of data cleanup before resignation" (Multiple answer available)

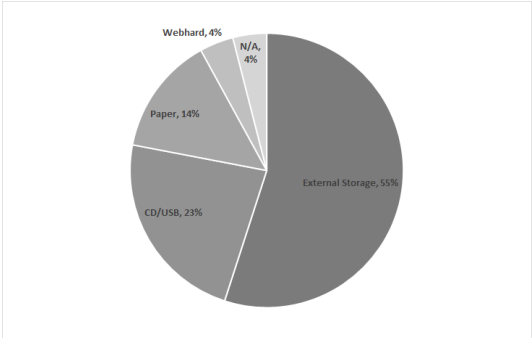

Fig. 2. Survey result of "Method of data cleanup before resignation" (Multiple answer available)

니터링되고 있다는 사실을 사전에 인지하고 있기 때문에, 모니터링을 우회하기 위해 인쇄를 택하는 경우가 종종 있다. 여기서 중요한 것은 핵심이 되는 기밀이 A4 용지 한 장만으로도 충분히 담길 수 있으므로, '인쇄' 이벤트는 출력 매수, 데이터 양보다는 발생 사실 자체에 의미가 있다는 점이다.

III. DRM 로그를 활용한 퇴직징후 분석기법

3.1 DRM 로그 형태

DRM 제조사별로 로그 포맷이 상이하지만, '생성/편집/해제/인쇄/삭제/해제실패'와 같은 행위가 일반적으로 기록된다. 본 연구에서는 퇴직의 핵심 징후인 '삭제'와 '인쇄' 행위만을 분석 대상으로 한다.

3.2 분석 대상

본 연구는 기밀 유출의 민감도가 가장 높은 기술

Table 1. DRM log sample (vender A)

Column	Details
date	date log created
name	DRM user account name
ID	DRM user account ID
PC IP Address	PC IP user logged on
PC MAC Address	MAC address of PC which user logged on
department	department of user
log type	created/edited/decrypted /printed/deleted/failed to decrypt
source IP	system IP which source file existed on
source file path and name	source file path and name handled with
destination IP	destination system IP which file saved on
destination file path and name	file path and name which has been saved or copied or moved

연구소를 대상으로 하고 있지만, DRM 솔루션을 사용하고 있는 조직이라면 어디든지 적용할 수 있는 일반성이 있다. 앞서 설명한 바와 같이 퇴직 예정자는 데이터를 저장한 후 '삭제'를 실시하며, 각종 보안 통제와 DRM 우회를 위해 '인쇄'를 실시한다는 점을 바탕으로 '삭제'와 '인쇄' 행위를 분석 대상으로 한다.

3.3 퇴직자 이상 징후 분석

이상행위 탐지 분석 기법은 표준 편차(Standard Deviation)를 이용한 탐지 기법과 MAD(Median Absolute Deviation) 기법을 적용했다. 실험 과정에서 표준 편차를 이용한 이상행위 탐지는 오탐율이 높아 민감도(sensitivity)가 낮은 MAD 기법을 채택했다. 정규분포를 이용한 이상탐지기법은 이상값이 평균과 정규분포에 큰 영향을 미쳐 적합하지 않았다.[4] 본 논문에서는 [5][6]에서 설명하고 있는 MAD의 우수성(붕괴점(Breakdown point)[7]이 표준 편차, Interquartile Range보다 높음)과 탐지 비교 결과를 바탕으로 MAD 기법을 이용한다.

MAD를 구하는 방법은 아래 수식(1)과 같이 표본 데이터에서 중간값(Median)을 구한 후, 각 데이터에서 중간값을 뺀 다음 절대값으로 바꾼 결과값에 대해 다시 중간값을 구함으로써 MAD 값을 얻을 수 있다[8]. MAD 값을 이용해 산출한 Modified Z-score의 절대값이 3.5 이상인 경우 이상값(outlier)에 해당한다[9,10].

$$MAD = median\,|x_i - \bar{x}| \quad (1)$$
$$M_i = \frac{0.6745(x_i - \bar{x})}{MAD}$$
$$|M_i| > 3.5$$

본 연구에서는 임직원의 평소 삭제/출력 활동을 수용하기 위해 최초 6개월 동안의 DRM 로그를 학습한다. 이후 지속적으로 6개월 구간을 슬라이딩하는 방식으로 당일 발생한 이벤트 로그가 최근 6개월간의 활동과 비교해 특이했는지를 확인한다. 학습과 모니터링 기간을 6개월로 설정한 이유는 최소한 반기(6개월)를 모니터링해야만 업무의 특성을 파악할 수 있기 때문이다. 기업의 업무 순환 주기가 분기(3개월), 반기(6개월), 연간(1년)을 기준으로 순환하는데, 반기를 학습하면 두 번의 분기를 반영할 수 있을 뿐만 아니라 한 번의 반기 업무를 반영할 수 있어 학습의 효과성을 높일 수 있다. 연간으로 설정하는 것이 나을 수 있으나, 이 경우 적용에 너무 오랜 기간이 소요된다는 단점이 있다. 이상값이 탐지되면 연관 분석(출력 분석) 단계로 넘어가며, 해당 값은 이후 데이터 분석에 미치는 영향을 최소화하기 위해 완화(중간값으로 대체)한다[11].

'삭제' 이벤트가 이상값으로 탐지된 경우 최근 2주일(14일) 이내에 '출력' 이벤트에서 최근 6개월 동안의 로그에 기반해 이상값이 탐지되는지를 확인한다. '삭제'와 '탐지'에서 이상값이 모두 탐지된 경우에만 '퇴직 징후'로써 유효한 탐지라는 가설을 수립했다.

IV. 퇴직 징후에 대한 모니터링 기법

퇴직 징후가 탐지된 임직원에 대한 조치를 할 때의 핵심 고려사항은 언제까지 모니터링을 해야 하는냐이다. 퇴직 징후가 발생하더라도 해당 임직원이 다양한 원인(상사의 회유, 가정사, 이직할 회사의 사정 등)으로 인해 퇴직을 번복할 수 있다는 점과 해당 임직원의 업무상 이유(조직 이동, 감사 대비), 회사의 캠페인(자료 정리, PC 교체) 등의 이유로 오탐일 수 있다는 점에서 효과적인 모니터링 기간을 설정하는 것이 무엇보다 중요하다.

4.1 퇴직자 및 재직자 분석

본 연구에서는 임직원 약 200명 규모의 연구소에서 발생한 2년 6개월의 DRM 로그를 활용해 퇴직 징후 탐지와 모니터링 기간을 분석했다. 해당 기간동안 실제 퇴사한 16명과 나머지 임직원을 대상으로 했으며, 이중에서 학습 기간 및 로그가 충분하지 않은 대상자를 제외해 퇴직자 14명과 재직자 170명을 분석했다.

Table 2에서 볼 수 있듯이 14명의 퇴직자에 대해 MAD 기법을 이용해 퇴직 징후를 분석한 결과, 14명 모두 다수의 퇴직 이벤트가 검출되었다.

합리적인 탐지 기준일을 도출하기 위해 퇴직 이전 100일을 기준일로 그 기간 안에 탐지된 마지막 이벤트를 찾고 직전 이벤트가 10일 이내에 발생했을 경우 이를 추가 수용했으며, 수용된 이벤트의 직전 이벤트도 동일한 방식으로 포함해 퇴직 징후를 파악할 수 있는 최초 시기를 분석했다. 퇴직자 14명의 데이터를 분석한 결과, Fig. 3과 같이 평균 약 95일 이전에 이상 행위가 탐지되었으며, 100일 동안 평균 8회(최소 2회에서 최대 21회)의 이상행위가 탐지되었다. 즉, 퇴직 징후가 발견된 후 기본적으로 100일간의 모니터링을 실시하면 퇴직자의 정보 유출을 사전에 탐지해 대응할 수 있을 것으로 기대할 수 있다.

재직자 170명에 대한 이상행위를 탐지한 결과, Fig. 4와 같이 86%(147명)의 재직자가 1회 이상 이상행위를 한 것으로 탐지되었다. 재직자의 탐지가 다수 있다는 점으로 인해 퇴직 징후 탐지에 오탐이

Table 2. Result of resigned employees

Name	Monitor Duration	# of Detection
Emp.1	818	31
Emp.2	700	23
Emp.3	805	14
Emp.4	481	12
Emp.5	887	49
Emp.6	865	20
Emp.7	912	67
Emp.8	702	33
Emp.9	818	28
Emp.10	631	22
Emp.11	864	19
Emp.12	742	19
Emp.13	651	9
Emp.14	708	11

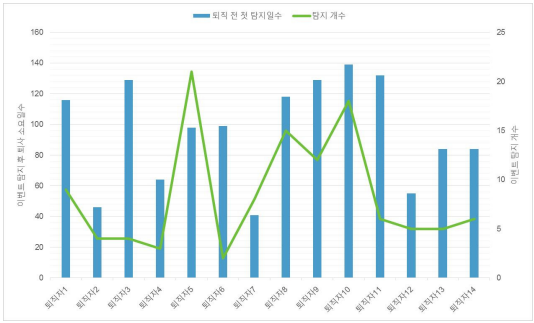

Fig. 3. monitoring period and detection count for 14 retired employees

잦다고 문제를 제기할 수 있다. 그러나, 재직자에 대해 재직 기간 대비 탐지 횟수를 비교한 결과 72%(111명)가 미미한 수준의 탐지비율(1~4%)을 보였다. 앞서도 언급한 퇴직 번복, 업무 환경 등의 이유로 인해 모니터링 기간 동안 재직을 했음에도 불구하고 퇴직 징후가 탐지될 수 있다.

무엇보다 본 연구가 실무 환경을 고려하지 않은 단순 데이터 분석인 점으로 인해 재직자의 심경 및 업무 환경 변화에 따른 당시 환경을 반영하지 못하는 제약사항이 있다. 또한, 본 연구의 주제는 실무 환경에서 모니터링을 실시한다는 가정 하에 이루어지는 것으로 실무 환경에서는 퇴직 징후 발생 시 퇴직자의 주변 상황을 모니터링해 이벤트의 유효성을 검증할 수 있다는 점도 고려되어야 한다. 재직자 개인별로 탐지 횟수가 비교적 적다는 점과 실무 환경에서의 예외 처리를 고려한다면 오탐으로 규정하기 어렵다.

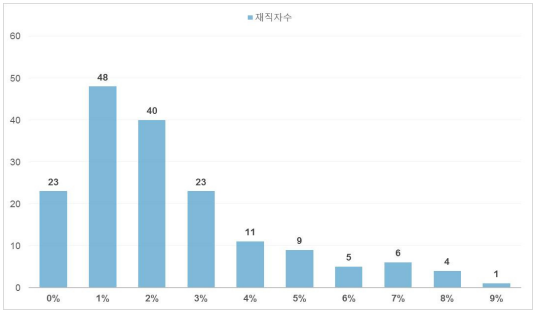

Fig. 4. Detection rate for working employees

4.2 퇴직 징후 탐지 및 대응법

MAD 기법을 이용한 이상행위 탐지는 퇴직 징후를 탐지할 수 있는 정보 원천으로써 큰 가치가 있다.

이 정보를 실무 환경에서 보다 가치 있게 사용하기 위해서는 Fig. 5와 같은 모니터링 기법을 활용해 퇴직 징후자를 사전에 탐지해 정보 유출에 대한 모니터링을 강화할 수 있다.

1. 평소 임직원의 업무 및 행동 패턴을 정립하기 위해 6개월(180일)동안 DRM 로그를 학습한다.

2. 6개월 후 부터 '삭제' 이벤트에서 이상 행위가 탐지되는지를 최근 6개월간의 데이터를 대상으로 일일 모니터링한다.

3. '삭제'에 대한 이상 행위가 탐지되면 최근 2주(14일) 이내 '출력' 이벤트 이상 행위가 탐지되는지를 확인한다. 이때 '출력' 이벤트 역시 6개월간의 데이터를 기반으로 이상 행위를 탐지한다.

4. '삭제'와 '출력' 모두에서 이상 행위가 탐지된 경우 비정기적인 업무 또는 특수상황에서 발생한 '예외'인지를 확인한다. 확인이 어려운 경우에는 간접적인 방법(채용 사이트 접근 여부, 메신저 대화 내용, 상사와의 면담 등)을 통해 상황을 확인한다. 직접적인 확인을 할 경우 모니터링 사실에 대해 경각심을 가질 수 있으므로 주의해야 한다.

5. '예외'가 아닌 경우로 판단되면 해당 임직원에 대한 강화모니터링을 100일 동안 진행한다. 회사에 존재하는 다양한 보안 통제(DLP, 웹 프록시, DNS, 방화벽 등)을 통해 접근 사이트(예. 이직 관련 사이트), 이메일 또는 메신저, 저장매체 등을 통해 정보 유출 시도가 있는지를 모니터링한다. 이 때 수집된 다양한 출처의 로그는 추후 혹시 발생할지 모를 정보 유출 사고(법정 소송)에 대응할 수 있도록 일정기간 동안 별도로 보존한다.

6. 강화모니터링으로 전환된 이후 추가적인 이상 행위 탐지 이벤트가 10일 이내(a) 발생할 경우 모니터링 기간을 추가 이벤트가 탐지된 기간(a)만큼 연장한다. 그 이후에 탐지된 이벤트 역시 10일 이내일 경우 동일한 방식으로 모니터링 기간을 연장하며, 10일을 초과한 이벤트가 발생한 경우 그 이후는 더 이상 모니터링 기간을 연장하지 않는다. (예로, 모니터링이 강화된 이후 3일 내에 첫 번째 추가 이벤트가 탐지된 경우 3일의 모니터링 기간을 더하며, 두 번째 추가 이벤트가 이후 4일 내에 발생한 경우에도 4일을 연장한다. 세 번째 추가 이벤트가 11일 이후 발생한 경우에는 더 이상 모니터링 기간을 연장하지 않는다.)

7. 강화 모니터링 기간이 만료된 이후에는 평시 모니터링으로 전환한다.

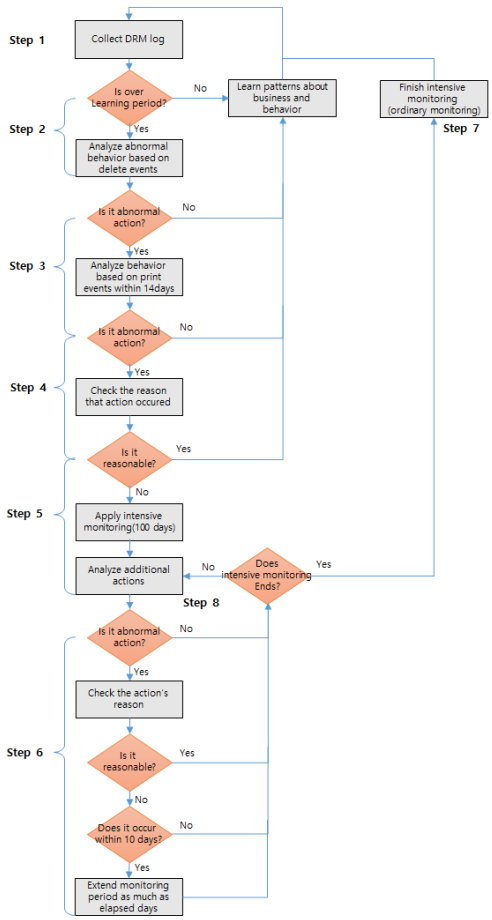

Fig. 5. Monitoring process for detecting sign of employees' resignation

8. 강화 모니터링 기간 내에 퇴직하는 경우에는 DRM 인쇄로그 상의 파일명을 대조하여 해당리스트의 파일을 모두 제출받는다.

이와 같은 방법을 활용해 퇴직자 14명에 대해 모니터링 프로세스를 시뮬레이션한 결과는 Table 3.과 같다. 퇴직자는 퇴직 징후가 탐지되었으며, 퇴직 이전까지 모두 모니터링 대상에 포함되었다. 재직 기간 중 평균 4회의 강화 모니터링 기간이 발생했으며, 퇴직 직전 모니터링 일수는 평균 69일이었다.

특이사항은 두 가지가 발생되었다. 첫 번째는 퇴직자 4의 경우 퇴직 8일 전에서야 강화 모니터링으로 전환되었단 점이다. 이는 실제 유효한 탐지일(2011.04.26)이 이전 탐지 및 모니터링 기간 안에 포함됨에 따라서 시뮬레이션 상에서는 너무 늦은 탐

Table 3. Simulation result of retired employees

Name	# of Monitoring	Last monitoring duration(day)	Start date of last monitoring	Resignation date	etc,
Emp.1	5	103	2010-12-21	2011-04-03	
Emp.2	4	45	2010-10-21	2010-12-06	
Emp.3	4	93	2011-02-16	2011-05-20	
Emp.4	3	8	2011-06-21	2011-06-29	Detects in 2011-04-26 (64days before)
Emp.5	6	37	2011-05-23	2011-06-29	
Emp.6	4	37	2011-04-13	2011-05-20	
Emp.7	3	41	2011-05-26	2011-07-06	
Emp.8	3	181	2010-10-15	2011-02-10	
Emp.9	2	122	2010-12-03	2011-04-04	Ends monitoring before 15 days of resignation
Emp.10	3	71	2010-07-19	2010-09-28	
Emp.11	4	115	2011-01-24	2011-05-19	Ends monitoring before 15 days of resignation
Emp.12	4	55	2010-11-23	2011-01-17	
Emp.13	2	33	2010-09-15	2010-10-18	
Emp.14	3	84	2010-12-17	2011-03-11	

지로 나타나게 된 것이다. 두 번째는 퇴직자 9, 11의 경우 퇴직 15일 전에 모니터링 기간이 종료된다는 것이다. 하지만, 이 두 가지 경우 정상적인 모니터링이 실시된다면, 퇴직자의 활동으로 퇴직 징후를 명확히 인지할 수 있다는 점과 본 연구가 퇴직일 예측이 아닌 사전 예방과 관련 증빙 수집이란 차원에서 약간의 오차는 수용 범위 내에 있다고 할 수 있다.

재직자의 시뮬레이션은 탐지율이 높았던 재직자 1과 재직자 2를 대상으로 했으며, 2명 모두 6회의 모니터링 전환이 발생했다. 즉, 앞서 언급한 바와 같이 실무 환경에서는 모니터링과 즉각적인 현황 파악을 통해 예외 처리가 가능하다는 점과 오탐이 되더라도 1인당 최대 6회(2년 6개월간) 발생한다는 점에서 실무 환경에서 감내할 수 있는 예외 수준으로 판단된다. 참고적으로 재직자 1의 경우 업무 특성상 예외(회계, 비품 등 주기적 관리업무로 인한 잦은 인쇄 및 데이터 삭제) 가 잦았던 임직원으로 실무 환경에서 충분히 예외 처리를 실시할 수 있었으며, 이로 인해 모니터링 횟수를 줄일 수 있는 상황이었다.

V. 결 론

DRM 로그는 정보 유출 탐지 관점에서 여러 보안 통제 로그 중에서 중요도가 높은 정보 원천이다. 사람의 행위를 한 가지 패턴만으로 파악하기 어려운 점이 존재하지만, DRM 로그를 이용한 이상행위 탐지는 퇴직자를 예측하는데 충분한 정보를 제공한다. 본 논문의 연구는 일반적인 상황 하에서 퇴직자를 사전에 예측할 수 있음을 밝혔다.

실무 환경에서 보다 효과적으로 퇴직자를 예측하고 오탐을 줄이기 위해서는 업무 환경에 대한 이해와 더불어 회사에 존재하는 다양한 보안 통제 로그(출근 기록, 방화벽 로그, 웹 접근 및 파일 전송 기록 등)를 활용하는 환경 구축이 무엇보다 중요하다.

References

[1] Youngwoo Lee, "Trade secrets, keep it using the electronic fingerprint!," http://www.ytn.co.kr/_ln/0103_201009090008502441, YTN, 9, Aug. 2010.

[2] "Unfair Competition Prevention and Trade Secret Protection Act", http://www.law.go.kr/lsInfoP.do?lsiSeq=142374, The National Law Information Center, 30, Jul. 2013

[3] "Report on the Current Status of SMEs' Management of Industrial Confidential Information," Small & Medium Company Administration, pp.15, Jun. 2007.

〔4〕 Christophe Leys and Christophe Ley, etc., "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," Journal of Experimental Social Psychology, pp. 1, Mar. 2013.
〔5〕 Christophe Leys and Christophe Ley, etc., "Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median," Journal of Experimental Social Psychology, pp.2, Mar. 2013.
〔6〕 Manish B Dave, Mitesh B Nakrani, "Malicious User Detection in Spectrum Sensing for WRAN Using Different Outliers Techniques," IJETT, Vol.9, Mar. 2014.
〔7〕 Songwon Seo, "A Review and Comparison of Methods for Detecting Outliers in Univariate Data Sets", University of Pittsburgh, pp. 47, 2006
〔8〕 "Median absolute deviation,"https://en.wikipedia.org/wiki/Median_absolute_deviation
〔9〕 Francisco Augusto Alcaraz Gracia. "Tests to identify Outliers in Data Series," MATLAB 7.8, 18, Aug. 2010
〔10〕 Sagar S. Sabade, Duncan M. Walker, "Evaluation of Effectiveness of Median of Absolute Deviations Outlier Rejection-based IDDQ Testing for Burn-in Reduction",
〔11〕 "A Comprehensive guide to Data Exploration," http://www.analyticsvid hya.com/blog/2015/02/outliers-detection-treatment-dataset/, Analytics Vidhya, 10, Jan. 2016

〈저자소개〉

현 미 분 (Miboon Hyun) 정회원
1999년 2월: 숭실대학교 컴퓨터학과 졸업
2010년 3월~현재: 고려대학교 정보보호대학원 석사수료
〈관심분야〉 디지털 포렌식, 로그분석

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2015년 1월~현재: 고려대학교 정보보호대학원 부원장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수