JANT 한국항행학회논문지 Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 18(5): 494-500, Oct. 2014

디지털 포렌식 기법을 활용한 효율적인 개인정보 감사 대상 선정 방안 연구

A study on the Effective Selection of the Personal Information Audit Subject Using Digital Forensic

전 준 영 · 이 상 진*
고려대학교 정보보호대학원

Jun-young Cheon[1] · Sang-jin Lee[2*]
[1]Center for Information Security Technologies (CIST), Korea University, Seoul 136-713, Korea

[요 약]

최근 대량의 개인정보 유출 사고가 잇따라 발생하고 있으며, 외부 해킹과 더불어 내부직원 및 외주업체 직원에 의한 개인정보 유출 사고가 증가하고 있다. 이에 따라 기업에서는 내부 보안을 강화하고, 개인정보 처리 업무를 위탁한 수탁사를 대상으로 개인정보의 분실, 도난, 유출 위험을 최소화하기 위해 정기적인 조사 및 점검을 통한 개인정보 감사를 진행하고 있다. 그러나 수탁사의 다양한 업무 환경으로 인해 한정된 시간 동안 모든 개인정보 취급 PC를 정밀 조사하는데 어려움이 있다. 따라서 개인정보의 유출 위험성이 높은 고위험군을 식별하여 점검 대상을 효과적으로 선정하는 것이 필요하다. 본 논문에서는 디지털 포렌식 기법을 활용하여 사용자 행위 기반의 고위험군 선정 방안을 제안한다. 또한, 이를 활용하기 위한 도구를 설계 및 구현하였고, 실험 결과를 통해 효과를 입증한다.

[Abstract]

Recently the leak of personal information from in-house and contract-managed companies has been continually increasing, which leads a regular observation on outsourcing companies that perform the personal information management system to prevent dangers from the leakage, stolen and loss of personal information. However, analyzing many numbers of computers in limited time has found few difficulties in some circumstances- such as outsourcing companies that own computers that have personal information system or task continuities that being related to company`s profits. For the reason, it is necessary to select an object of examination through identifying a high-risk of personal data leak. In this paper, this study will formulate a proposal for the selection of high-risk subjects, which is based on the user interface, by digital forensic. The study designs the integrated analysis tool and demonstrates the effects of the tool through the test results.

Key word : Digital forensics, Personal Information audit, Selection of high-risk subjects, Information leakage prevention, High-risk subjects selection system.

http://dx.doi.org/10.12673/jant.2014.18.5.494

Received 18 September 2014; **Revised** 22 October 2014
Accepted (Publication) 6 October 2014 (30 October 2014)

***Corresponding Author; Sang-jin Lee**

Tel: +82-2-2209-3671
E-mail: sangjin@korea.ac.kr

Ⅰ. 서 론

개인정보가 마케팅 및 기타 불법적인 영리수단으로 활용됨에 따라 개인정보의 수요가 증가하고, 이로 인해 개인정보침해 사고가 증가하고 있다. 이에 따라 개인정보의 무단수집, 무단이용 및 제공, 외부 유출 등 개인정보를 침해할 수 있는 다양한 요소로부터 사생활을 보호하고 개인의 권리 및 가치를 구현하기 위해 2011년 9월 개인정보보호법이 시행되었다. 그러나 2012년 개인정보 침해신고 상담건수는 166,801건, 2013년에는 총 177,736건으로 전년에 비해 증가하였다 [1]. 감사원의 금융회사 개인정보 유출 관련 검사·감독 실태 감사 결과 보고서에 따르면 최근 5년간(2009~2013년) 20개의 금융회사에서 약 1억 1,000만 건의 개인정보가 유출되었다[2]. 이처럼 카드사, 은행, 보험사, 통신사 등 대량의 개인정보를 취급하는 기업으로부터 매년 개인정보 유출 사고가 지속적으로 발생하고 있다.

최근 국내 개인정보 유출 사례를 종합해 본 결과 전문적인 해커에 의한 개인정보 유출 사고보다 개인정보를 처리하는 협력업체 직원 및 외주직원, 그리고 권한이 있는 내부 임직원에 의한 개인정보 유출 사고가 더욱 빈번하게 발생하고 있다. 업무 특성 상 일상적으로 개인정보를 취급하는 내·외부 직원은 개인정보에 대한 접근성이 높고, 기업에서는 완벽한 내부 통제가 힘들기 때문에 내·외부 직원에 의한 개인정보의 유출 사고는 항상 잠재적인 위험 요소로 남아있다. 이에 따라 기업은 개인정보를 취급 및 처리하는 내·외부 직원 관리에 대한 중요성을 인지하고, 개인정보 유출 사고를 방지하기 위해 DRM (digital rights management), DLP (data loss prevention), 개인정보검출 솔루션, DB 접근통제 및 암호화 솔루션, 하드디스크 암호화 솔루션, 완전삭제 솔루션 등 다양한 보안 솔루션을 적극적으로 도입하고 있다.

하지만 개인정보 처리 업무를 위탁받은 수탁사의 경우 각종 보안 솔루션 도입에 따른 비용 부담 및 운영·관리를 위한 인력 부족 등의 이유로 기업과 동일한 보안 수준을 갖추기가 어렵다. 따라서 기업에서는 관련 조직을 구성하고 수탁사를 대상으로 정기적인 개인정보 감사를 진행하고 있다.

개인정보 감사는 조직에서 취급하는 개인 정보가 라이프사이클 각 처리 단계별로 올바르게 처리되고 있음을 판단하기 위해 관리 및 점검하는 것을 의미한다. 개인정보 감사를 진행하는 경우 디지털 포렌식 기법을 통해 개인정보 취급 PC로부터 개인정보 유출 또는 유출 시도, 정보 은닉, 내부 보안 규정에 위배되는 행위 여부 등을 분석하여, 보다 정밀한 개인정보의 유출 위험성 조사가 가능하다. 하지만 모든 PC에 대해 정밀 점검을 수행하기 위해서는 많은 시간이 소요된다. 따라서 한정된 시간 동안 효과적인 점검을 수행하기 위해 개인정보의 유출 위험성이 높은 고위험군을 식별하여 점검 대상을 효과적으로 선정하는 것이 필요하다.

본 논문에서는 다수의 개인정보취급 PC로부터 점검 대상을 보다 효과적으로 선정하기 위한 사용자 행위 기반의 감사 대상 선정 방안을 제안하고, 이를 활용하기 위한 도구를 설계 및 결과물을 보여준다.

Ⅱ. 개인정보 감사 대상 선정 방안

2-1 샘플링을 통한 점검 방법의 한계

개인정보 감사를 수행하는 경우 감사 절차와 방법은 기업 정책 및 수탁사 환경에 따라 차이가 존재하지만, 개인정보 라이프사이클 처리 단계별로 개인정보 침해 및 유출 위험성을 조사하고 이를 보완하여, 개인정보 유출 사고를 예방하고자 하는 목적은 동일하다. 즉, 개인정보 감사의 목적은 수탁사에서 취급하는 개인정보가 수집·이용, 저장·관리, 제공·위탁, 파기 각 단계별로 개인정보보호법령 규정에 명시된 바와 같이 올바르게 처리되는지를 재확인하여 개인정보 유출 위험성을 최소화 시키는데 있다.

개인정보를 취급하는 PC에서 개인정보 검출 솔루션을 통해 개인정보가 저장된 문서의 보관 여부 및 암호화 여부를 판단할 수 있고, 수집된 개인정보 파일의 삭제 여부 등을 확인할 수 있다. 하지만 실제 사용자가 개인정보 취급 PC에서 비 인가된 응용프로그램의 설치 및 실행 흔적, 외부저장매체의 사용 및 개인정보 취급 흔적, 수집된 개인정보의 완전 삭제 수행 여부, 보유기간이 만료된 개인정보 파일 보유 여부, 의도적인 정보 은닉 등은 일반적인 방법으로 점검하기 어렵다.

디지털 포렌식 기법을 활용한 개인정보 감사는 개인정보 취급 PC에서 수행한 흔적들을 분석하여 사용자 행위를 파악할 수 있으며 앞서 언급한 점검하기 어려운 항목들에 대해 확인이 가능하다. 또한, 정보보안 관련 시스템(DLP, DRM, F/W 등)이 구축되어 있는 수탁사의 경우 해당 로그와 사용자 행위 분석 결과를 비교하여 보안솔루션의 정상 동작 여부 및 보안정책 반영 여부, 모니터링 여부 등을 함께 파악할 수 있다. 이처럼 개인정보 감사에 포렌식 기법을 적용하는 경우 다양한 장점이 존재하는 반면 많은 시간이 소요된다는 단점이 존재한다.

TM (tele marketing), DM (direct mail) 발송 업무와 같이 대량의 개인정보를 처리하는 수탁사의 경우, 업무 연속성이 이윤과 직결되거나, 다수의 개인정보 취급 PC를 운영하기 때문에 한정된 시간 동안 모든 개인정보 취급 PC를 정밀 조사하는 것은 현실적으로 어렵다.

따라서 회계감사에서 통상적으로 사용되는 샘플링 조사 방법과 같이 한정된 시간 내 효과적인 점검을 수행하기 위해 개인정보 감사도 일반적으로 샘플링 점검을 수행한다. 수탁사의 일부 PC만 점검할 경우, 점검 대상의 선정 기준이 별도로 존재하지 않기 때문에 조사자는 개인정보 취급자의 직급, 권한, 근속기간 등 다양한 고위험군 식별 기준을 만들고, 해당 기준에 적합한 대상자 중 일부를 선정하여 정밀 점검을 수행한다. 하지만 위와 같은 고위험군 식별 기준을 통한 샘플링 조사 결과는 전수조사를 통해 얻은 결과와 차이가 발생할 수 있는 샘플링 위험이 존재한다. 또한 고위험군을 식별하기 위한 기준이 객관적이지

않으며 개인의 컴퓨터 사용 능력에 대한 수준 평가가 이루어지지 않아 식별 기준에 대한 정확도가 떨어질 가능성이 존재한다.

2-2 PC 사용 행위 기반 고위험군 식별 방안

개인정보를 취급하는 수탁사를 대상으로 효과적인 관리·감독을 위해 개인정보 유출 위험성을 지닌 분석 주체를 신속하고 정확하게 파악하는 것이 중요하다. 따라서 샘플링 방법의 고위험군 선정 방법의 한계점을 보완하기 위해 개인정보 취급 PC 내부에 설치된 응용 프로그램과 사용자의 프로그램 사용 패턴을 수치화하여 고위험군을 식별할 필요가 있다.

PC사용 행위 기반 고위험군 식별 방법은 표 1과 같이 PC사용 흔적 중 정보 유출 위험성이 높은 행위를 선별하고, 수탁사의 개인정보 취급PC로부터 유출 위험성이 있는 사용 패턴을 가진 PC를 파악하여 고위험군으로 식별하는 것이다. 즉, 조사 우선순위를 샘플링이 아닌 사용자의 PC 사용 패턴(행위)에 기반하여 점검 대상을 선정하는 것이다.

모든 개인정보취급 PC를 대상으로 심층 분석을 수행한다면 많은 시간이 소요되어 전수 조사가 어려우며, 내부 직원들의 업무 효용성이 저하될 수 있다. 따라서 정보 유출 위험성이 높은 행위들을 신속하게 파악할 수 있는 윈도우 아티팩트를 선별 수집하고 분석함으로써 점검 시간을 단축시키고, 모든 개인정보취급 PC를 대상으로 1차적 점검이 가능하므로 샘플링 점검의 한계점을 보완할 수 있다.

또한 수탁사의 업무 특성에 따라 USB 메모리 또는 상용 메일 등의 사용이 필요한 경우가 있으므로 수탁사 내부 보안 정책을 고려할 필요가 있다. 따라서 각 유출 위험성 존재 행위(P_0) 중 수탁사의 내부 보안 정책(W_0)을 반영하여 이를 위반한 내부 직원이 발견되는 경우, 고위험군 식별을 위한 위험도 평가 시 추가 가중치 부여가 가능하다.

표 1. 개인정보 유출 관련 위험 행위
Table 1. Risk activities that leak of personal information.

도메인	유출 위험성 존재 행위 (Pi)
외부저장매체	USB메모리, CD/DVD
응용 프로그램	원격 접속 관련 프로그램
	온라인 메신저
	FTP 프로그램
	P2P 프로그램
	파일 및 폴더 은닉 프로그램
무선 네트워크	무선 공유기, 무선 렌카드, 스마트폰 테더링
공유폴더	공유폴더, 네트워크드라이브
웹 사이트	상용 메일
	클라우드 서비스
	개인블로그, SNS, 카페 등 데이터 업로드가 가능한 웹 사이트

위험도 평가 방법은 다음과 같다. 사전에 선별 수집한 PC사용 흔적에서 기존에 설정한 유출 위험성이 존재하는 행위(P_0)가 발견되는 경우를 1 (P_0=1), 발견되지 않는 경우 0 (P_0=0)으로 설정한다. 내부 보안 정책(W_0)은 위배 여부에 따라 위배되는 경우 2 (W_0=2), 위배되지 않는 경우 1 (W_0=1) 값을 부여한다.

유출 위험성이 존재하는 행위 발견 여부(P_i)와 사내 보안 정책 위배 여부(W_i)를 아래 식과 같이 계산하여 PC사용 행위 기반의 유출 위험성(T)를 도출할 수 있으며, 이 결과를 바탕으로 개인정보 감사 대상을 선정할 수 있다.

$$T = \sum_{i=1}^{11} (P_i \times W_i) \quad (1)$$

Ⅲ. 개인정보 감사 관점 포렌식 기법 활용

3-1 개인정보 유출 가능 경로

개인정보 유출 사고 원인은 다양하지만 주로 개인정보를 악의적인 목적으로 활용하기 위한 외부 해킹이나 내부자에 의한 고의적인 유출로 인해 발생한다.

표 2는 내부직원 또는 외주업체 직원에 의한 개인정보 유출 사례 및 유출 경로를 정리한 것이다. 위 사례에서 알 수 있듯이 개인정보 취급자가 개인정보를 고의적으로 유출하는 경우 USB 메모리가 가장 많이 사용되었으며, DVD, 이메일, 프린터, 불법 프로그램 또한 개인정보 유출 경로로 사용되었음을 알 수 있다.

위 사례에서 소개된 유출 경로 외에도 표 3과 같이 팩스, 메신저, P2P, 웹 하드, 클라우드, FTP, 원격 프로그램 등 다양한 경로를 통해 개인정보 유출이 가능하다. 개인정보 감사 관점에서 정보 유출 가능 경로는 개인정보의 유출 여부 판단 및 잠재적인 위험성을 파악하는데 중요한 점검 요소로 사용된다.

표 2. 내부 또는 외부 직원을 통한 개인정보 유출 사례
Table 2. The examples of leaked personal informations by internal and external company staff.

업체명 (날짜)	유출 건수	유출 경로
OO 칼텍스 (‘08.09)	1,150만	DVD 복사
OO 카드('11.08)	80만	프린터 출력
OO 카드('11.10)	9만 7,000	이메일 전송
OOO 캐피탈 (‘11.12)	5,800	프린터 출력
OOO, OO 통신사 (‘12.03)	20만	불법프로그램 사용
OOO화재 (‘12.05)	16만 4,000	USB 복사
OO은행 (‘13.12)	10만	USB 복사
OO은행 ('13.12)	3만	프린터 출력
OOOO카드 (‘14.01)	5,300만	USB 복사
OOOO카드 ('14.01)	2,500만	USB 복사
OO카드 ('14.01)	2,600만	USB 복사

표 3. 개인정보 유출 가능 경로
Table 3. The route which personal informations are leaked.

개인정보 외부 유출 가능 경로
○ 외부저장매체 (USB 메모리, CD, DVD 등)
○ 하드디스크 (하드디스크 복제)
○ 공유폴더 / 네트워크 드라이브
○ 온라인 메신저 및 이메일
○ 파일 공유 사이트 (웹하드, P2P, 클라우드 등)
○ 응용 프로그램 (FTP, 원격 프로그램 등)
○ 무선 네트워크, 스마트 폰 테더링
○ 복합기 (프린터, 팩스, e-팩스)

3-2 포렌식 기법을 통해 획득 가능한 PC사용 정보

기업으로부터 개인정보 데이터를 전달받는 일부 서버를 제외하고 개인정보를 처리하는 PC에는 대부분 윈도우 운영체제가 설치되어 있다. 따라서 표 4와 같이 포렌식 기법을 이용하여 레지스트리, Index.dat, 링크 파일, 프리패치, 이벤트 로그 등 다양한 윈도우 아티팩트를 함께 분석함으로써 개인정보 취급PC의 사용 패턴을 파악할 수 있다.

1) 외부저장매체 사용 흔적

USB 메모리와 같은 이동식 저장장치는 크기는 작지만 대용량의 데이터 저장이 가능하여 반입자체를 차단하기 어렵고, 개인정보취급 PC에서 물리적인 차단 또는 보안솔루션을 통한 통제가 되지 않는 한 개인정보 유출 위험의 가장 큰 위협 요소 중 하나이다. 외부저장매체 연결과 관련된 정보는 레지스트리와 SetupAPI.log에서 확인 가능하며, 외부저장매체로부터 데이터를 취급했던 흔적은 레지스트리와 링크 파일, 프리패치 파일 등에서 확인할 수 있다[3],[4].

따라서 레지스트리로부터 개인정보 취급 PC에 연결되었던 외부저장매체의 디바이스 정보, 연결 시각, 시리얼 번호 등을 수집하고, 링크 파일로부터 참조 대상 파일의 드라이브 유형 및 시리얼 번호, 프리패치 파일로부터 참조 목록 및 응용 프로그램이 실행되었던 드라이브 시리얼 번호 등을 함께 분석하여 비인가 저장매체의 사용흔적과 개인정보 취급·유출 흔적 여부를 조사한다.

2) 응용프로그램 사용 흔적

온라인 메신저, FTP, 원격, 파일·폴더 은닉 프로그램 등 개인정보를 외부로 유출시킬 수 있는 프로그램을 사용하거나, PC에 개인정보를 은닉하여 개인정보 보유 여부를 탐지하지 못하도록 숨기는 경우가 존재한다. 사용자의 응용프로그램 설치 및 실행 흔적은 레지스트리와 링크 파일, 프리패치, 점프 목록에서 확인할 수 있다. 따라서 이러한 아티팩트들로부터 응용 프로그램의 설치 및 사용 시각, 실행 횟수 등의 정보를 수집하고 각 응용프로그램에서 PC에 남기는 로그 및 설정 파일이 존재하는지 확인 후 함께 분석하여 사용자가 해당 응용프로그램을 통해 어떠한 행위를 수행하였는지를 조사한다[4].

하지만 각각의 응용프로그램의 종류 및 개수가 매우 많고, 응용프로그램에 따라 사용 로그 및 설정 파일을 저장하지 않는 경우가 있어 분석하는데 어려움이 따른다. 이에 따라 외부로 정보를 유출시킬 수 있거나 그와 관련된 응용프로그램들을 목록화하고, 분석 과정에서 비슷한 동작을 수행하는 새로운 응용프로그램 발견 시 지속적인 목록 업데이트 수행이 필요하다.

표 4. 개인정보 감사 관점에서 디지털 포렌식을 통해 획득 가능한 사용자 행위 정보
Table 4. In terms of monitoring personal information audit, the possible way to find a history of the users activity by digital forensic.

항 목	Registry	Link File	Spool Data	Prefetch / Superfetch	Event Log	Jump List	Setup API Log	Index.dat	File System
계정 정보 / OS 설치 정보	○								
외부저장 매체 사용 흔적	○	○		○			○		
응용프로그램 설치 및 사용흔적	○	○		○	○	○			
공유폴더 사용흔적	○	○							
실행 명령 흔적	○								
프린트 설치 및 사용흔적	○		○						
웹 사이트 접근 및 검색 흔적	○							○	
무선 네트워크 사용 흔적	○								
최근 사용한 문서 흔적	○	○							
개인정보 파일 암호화 여부 (DRM, 파일자체암호화)									○
개인정보 파일 완전삭제 여부 (보유기간 만료된 개인정보 보유 여부)									○

3) 무선 네트워크 사용 흔적

에그(Egg)나 와이브로(WiBro)와 같이 통신사 커버리지 구역 안에선 언제든지 와이파이 서비스가 가능한 개인 휴대용 와이파이 기기 또는 스마트폰, 태블릿 PC를 모뎀 역할로 만들어 인터넷 사용을 가능하게 만드는 테더링(tethering) 기능 등 최근 스마트 기기 보급이 확대됨에 따라 무선 네트워크를 통한 개인정보 유출 위험성 또한 높아지고 있다.

수탁업체에서 개인정보 취급 PC에 망 분리를 수행하였다고 하더라도 무선 네트워크가 통제되지 않았다면, 개인정보 취급자가 내부망에서 무선 네트워크를 사용이 가능하며 이러한 경우 사내 네트워크를 이용하지 않기 때문에 정보보호 장비를 거치지 않고 자료 전송 등의 행위가 가능하게 된다. 또한 유출 사실에 대한 확인이 어렵기 때문에 무선 네트워크의 사용 흔적은 개인정보 감사 관점에서 매우 의미 있는 정보이다.

따라서 레지스트리로부터 무선 네트워크어댑터, SSID, 연결·사용 시간 정보 등을 수집하고 분석하여 개인정보 취급 PC에서 무선 네트워크의 사용 여부를 조사할 수 있다.

4) 공유폴더/네트워크 드라이브 사용 흔적

기업에서 업무 관련 자료의 공유 목적으로 네트워크 공유폴더를 많이 사용한다. 공유폴더에 대한 접근 권한을 설정하여 사용할 수 있으나 관리가 제대로 이루어지지 않아 일부 업체에서는 보안 정책 상 공유 폴더 사용 자체를 통제하는 경우가 있다. 공유폴더 사용 흔적은 개인정보 취급자가 직접 공유폴더를 생성한 경우와 타 사용자가 만든 공유폴더에 접근한 흔적으로 나눌 수 있다. 레지스트리로부터 개인정보 취급자가 직접 생성한 공유폴더 목록을 확인할 수 있으며, 링크 파일 및 레지스트리의 실행 명령 등으로부터 해당 사용자가 접근했던 타인의 공유 폴더 및 접근한 파일명 등을 확인할 수 있다.

따라서 개인정보 감사 관점에서 공유폴더의 존재 여부 및 접근 권한 미설정으로 인한 비인가자의 접근 가능 여부, 비인가자의 공유폴더 내 개인정보 저장 여부 등을 파악하여 개인정보 유출 위험성 점검한다.

5) 비인가된 웹 사이트 접속 및 메일 사용 흔적

방화벽 또는 웹 사이트 접속을 통제할 수 있는 DLP 솔루션을 운영하는 수탁사의 경우, 개인정보 취급 PC에서 업무 목적상 필요한 웹 사이트만 접속 할 수 있는 화이트 리스트 기반의 정책을 사용하여 인터넷 사용을 통제 할 수 있다. 그러나 보안 장비가 존재할지라도 관리·운영이 미흡하거나, 보안 장비 및 솔루션을 운영하지 않는 수탁사가 존재한다. 이러한 경우 파일 업로드가 가능한 웹 사이트 접속 및 메일 사용 등 개인정보의 유출 위험성이 존재한다. 따라서 웹 접속 기록 및 파일 열람 기록, 사용 시각, 메일 아카이브 파일 등을 수집하여 개인정보의 유출 여부 및 유출 위험성을 판단한다.

Ⅳ. 개인정보 감사대상 선정 시스템 구현 및 실험

4-1 시스템 구성

본 고위험군 선정 시스템은 그림 1과 같이 클라이언트, 중앙 서버, 그리고 사용자 행위 분석 agent와 통합 분석 도구로 구성되어 있다. 클라이언트는 수탁사에서 개인정보를 처리·취급하는 PC이며, 중앙 서버는 클라이언트와 사용자 행위 분석 agent 및 분석 결과 DB 파일을 서로 주고받을 수 있도록 네트워크가 연결되어 있으며, 통합 분석 도구가 실행되는 서버 또는 일반 PC를 의미한다.

시스템 동작 과정은 다음과 같다. ① 사내 중앙 서버에서 개인정보취급이 허가된 개인 또는 부서의 모든 PC를 대상으로 사용자 행위 분석 agent를 배포한다. 개인정보에 대한 취급 권한이 없는 직원 PC 또는 비 인가된 PC는 agent 배포 대상에서 제

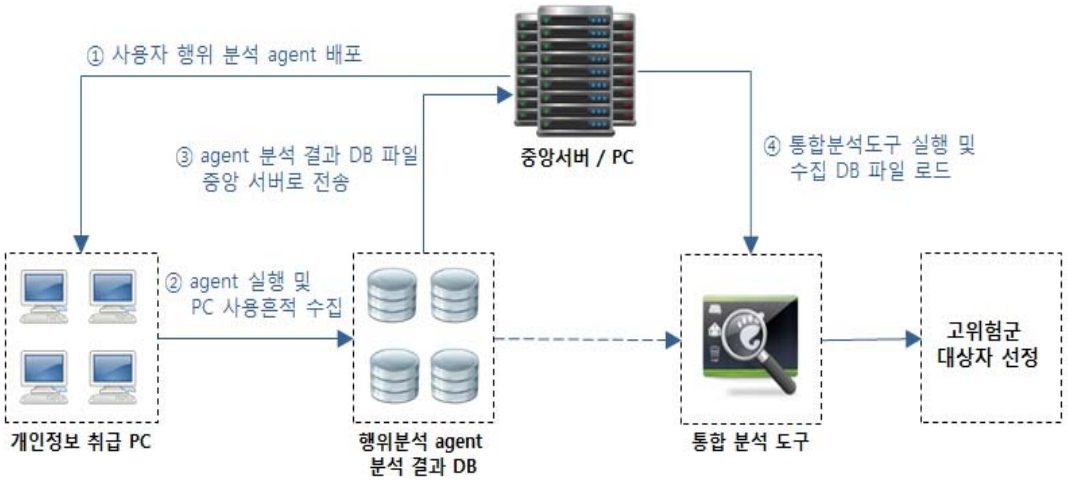

그림 1. 고위험군 선정 시스템
Fig. 1. High-risk subjects selection system.

외한다. ② 각각의 개인정보 취급 대상자 PC에서 agent를 실행하여 정보 유출 또는 정보 유출 위험성을 판단할 수 있는 포렌식 아티팩트를 수집한다. 수집된 데이터를 분석하고 정제하여 DB 파일로 저장한다. ③ 분석 결과 DB 파일을 중앙 서버로 전송한다. ④ 중앙 서버에서 통합 분석 도구를 실행하고, 각 클라이언트로부터 전달받은 DB 파일들을 일괄적으로 로드한다. 통합 분석 도구에서는 개인정보취급 대상자의 PC 사용 행위 정보를 통합하여 조사관이 모든 대상자로부터 수집된 데이터를 한눈에 볼 수 있으며, 각 대상자 결과에 대한 비교 및 외부저장매체와 공유폴더 사용에 관한 상관 관계 분석이 가능하다. 통합 분석 도구에서 각각의 포렌식 분석 항목으로부터 유출 위험성이 존재하는 행위 여부를 파악하고, 위험도 평가를 적용한 결과를 통해 고위험군을 선정할 수 있다.

4-2 실험 환경

샘플링 방법을 이용한 고위험군 선정 및 점검 결과와 PC사용 행위 기반의 고위험군 선정 및 점검 결과를 통해 고위험군 선정 대상의 유효성 및 정확성을 비교하기 위한 실험을 수행하였다. 결과 측정 방법은 각각의 방법을 통해 선정한 고위험군 대상으로부터 실제 유출 위험성이 존재하는 대상의 비율로 정확성을 비교하였다.

실험 환경은 TM업체, DM발송 업체, SMS/MMS발송 업체, 여행사, 홈페이지 운영대행 업체, 신용평가 업체 등 개인정보를 취급하는 다양한 수탁업체를 대상으로 진행하였으며, 두 가지 방법의 실험을 진행하는 동안 서로 다른 위탁업체로부터 동일한 개인정보 처리 업무를 위탁받은 중복된 수탁업체 또한 결과에 포함시켜 점검하였다.

샘플링 기반 고위험군 선정 대상은 58개의 수탁사로부터 182대의 PC를 선정하였고, PC사용 행위 기반 고위험군 선정 대상은 31개의 수탁사로부터 94대의 PC를 선정하였으며 PC사용 행위를 파악하기 위해 선별 수집 작업이 포함된 PC는 약 290대이다.

4-3 실험 결과

표 5는 샘플링 방법을 통해 고위험군 선정 방법과 PC사용 행위 기반 고위험군 선정 방법을 통해 각각의 유출 위험성이 존재하는 PC 개수 및 정확도 결과이다.

실험 결과와 같이 선별 수집한 데이터를 기반으로 모든 개인정보 취급자 PC의 사용 패턴 분석 후 고위험군을 선정하였던 방법이 상대적으로 더 높은 정확도를 보이는 것을 확인할 수 있다.

Ⅳ. 결 론

개인정보 유출 사고가 지속적으로 발생함에 따라 개인정보 처리 업무를 위탁받은 수탁업체의 개인정보 관리·감독의 중요성이 증가하고 있다. 한정된 시간동안 수탁업체에 있는 모든 PC를 대상으로 점검하는 것은 현실적으로 어렵기 때문에, 일반적으로 내부 직원 중 정보 유출 위험성이 높은 대상자를 고위험군으로 식별하고 해당되는 대상 그룹 중 일부를 샘플링하여 개인정보 감사를 진행하였다. 그러나 고위험군 선정 시 이러한 주관적인 기준에 의한 샘플링 방법을 적용하는 경우 샘플링 위험성이 따르며, 조사자에 따라 고위험군 대상자가 바뀌게 된다.

표 5. 실험 결과 정확도 비교
Table 5. Experimental results compare the accuracy.

도메인	유출 위험성 존재 행위 (Pi)	샘플링 기반 점검 결과			PC사용 행위 기반 점검 결과		
		고위험 선정 PC 개수	유출 위험성 존재 PC 개수	정확도	고위험 선정 PC 개수	유출 위험성 존재 PC 개수	정확도
외부저장매체	USB메모리, CD/DVD	163	70	42.94 %	35	22	62.85 %
응용 프로그램	원격 접속 관련 프로그램	32	5	15.62 %	7	1	14.28 %
	온라인 메신저	71	44	61.97 %	27	19	70.37 %
	FTP 프로그램	66	5	7.57 %	49	12	24.48 %
	P2P 프로그램	58	45	77.58 %	21	16	76.19 %
	파일 및 폴더 은닉 프로그램	19	4	21.05 %	8	6	75.00 %
무선 네트워크	무선 공유기, 무선 랜카드, 스마트폰 테더링	14	10	71.42 %	23	19	82.60 %
공유폴더	공유폴더, 네트워크드라이브	113	21	18.58 %	31	7	22.58 %
웹 사이트	상용 메일	75	63	84.00 %	47	41	87.23 %
	클라우드 서비스	11	8	72.72 %	14	12	85.71 %
	개인블로그, SNS, 카페 등 데이터 업로드 가능한 웹 사이트	65	24	36.92 %	19	10	52.63 %

따라서 객관적인 기준을 통한 효과적인 개인정보 대상자 선정 방법이 필요한 실정이다.

본 논문에서는 모든 개인정보취급 PC에서 신속하게 PC 사용 정보를 분석하여 실제 유출 위험성이 존재하는 행위가 있었는지를 판단하였고, 내부 직원의 PC 사용 정보와 내부 보안 정책을 반영하여 위험도를 수치화 하였다. 실험을 통해 확인하였듯이 사용자 행위 기반의 개인정보 감사 대상 선정 방법은 기존의 샘플링 방법에 비해 정확도가 높게 측정되었다. 이러한 연구 결과를 토대로 개인정보 감사를 수행하는 조사관은 보다 정확한 유출 위험 대상자를 선별하여 개인정보 유출 사고 예방에 많은 도움을 줄 수 있을 것이다.

참고문헌

[1] Korea Internet Security Agency (KISA), Information Security Statistics [Internet]. Available: http://isis.kisa.or.kr/sub07/?pageId=070500

[2] The Board of Audit and Inspection of Korea (BAI) [Internet]. Available: http://www.bai.go.kr/HPBKAudResultOpenAction.do?method=detailData&SEQ_NO=1642&PAGE=1&CYBER_PUHE_YN=Y&AUD_YEAR_NO=2014081&TASK_TYPE=KP1

[3] Microsoft.[MS-SHLLIK] Shell Link (.LNK) Binary File Format. [Internet]. Available: http://msdn.microsoft.com/en-us/library/dd871305.aspx

[4] H. Carvey, *Windows Registry Forensics: Advanced Digital Foernsic Analysis of the Windows Registry*, Burlington, NJ: Syngressmedia, 2011

[5] T. H. Kang and J. I, Lim “A study on consigned party management system enhancement for personal information protection,” *Journal of The Korea Institute of Information Security & Cryptology*, Vol 23, No. 4, pp. 781-797, Aug. 2013.

[6] C. H. Lee, “Study on digital investigation model for privacy acts in Korea”, *Journal of the Korea Navigation Institute*, Vol. 15, No. 6, pp. 1212-1219, Dec. 2011.

[7] C. S. Jung and Y. C. Kim, “A study on system tracing user activities in the windows operating system”, *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 21, No. 8, pp. 101-114, Aug. 2011.

전 준 영 (Jun-Young Cheon)
2010년 2월 : 세종대학교 (공학사)
2010년 9월 ~ 현재 : 고려대학교 정보보호대학원 석사과정
※관심분야 : 디지털 포렌식, 정보보호

이 상 진 (Sang-Jin Lee)
1987년 2월 :고려대학교 수학과 (이학사), 1989년 2월 :고려대학교 수학과 (이학석사)
1994년 8월 :고려대학교 수학과 (이학박사), 1989년 10월 ~1999년 2월 :한국전자통신 연구회 선임 연구원
1999년 3월 ~ 2001년 8월 : 고려대학교 자연과학대학 조교수, 2001년 9월 ~ 현재 : 고려대학교 정보보호대학원 교수
2008년 3월 ~ 현재 : 고려대학교 디지털포렌식 연구센터 센터장
※관심분야 : 디지털 포렌식, 심층암호, 해쉬함수