Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.961

PC보안솔루션 로그분석을 통한 보안정책 제안 (개인정보유출 방지)

채 현 탁,† 이 상 진‡
고려대학교 정보보호대학원

Security Policy Proposals through PC Security Solution Log Analysis (Prevention Leakage of Personal Information)

Hyun tak Chae,† Sang-jin Lee‡
Korea Graduate School of Information Security

요 약

내부자에 의한 개인정보유출 사고를 방지하기 위하여 다수의 기업은 문서 DRM(Digital Right Management), DLP(Data Loss Prevention), 개인정보 검색시스템 등과 같은 PC보안솔루션을 지속적으로 도입하여 운영하고 있다. 하지만 이러한 투자에도 불구하고 개인정보유출 사건들은 지속적으로 발생하고 있다. PC보안솔루션의 단순 구축이 아닌 기업에 적합한 보안 정책을 사전에 수립하고 정책에 맞는 시스템을 운영한다면 개인정보유출 사고를 미연에 방지할 수 있을 것이다. 또한 로그분석을 통하여 수립한 보안정책의 효과성을 검증할 수 있으며 로그분석결과를 바탕으로 보안정책의 수정 보완이 가능할 것이다. 본 논문은 다양한 PC보안솔루션 중 개인정보유출 방지를 위해 PC에 필수 설치되는 보안솔루션을 정의하고, 필수보안 솔루션을 개인정보보호 관점에서 통합 운영하는 방안, 그리고 로그분석을 통해 개인정보유출 사고 방지를 위한 효과적인 보안정책을 제안하고자 한다.

ABSTRACT

In order to prevent leakage of personal information by insiders a large number of companies install pc security solutions like DRM(Digital Right Management), DLP(Data Loss Prevention), Personal information filtering software steadily. However, despite these investments anomalies personal information occurred. To establish proper security policy before implementing pc security solutions, companies can prevent personal information leakage. Furthermore by analyzing the log from the solutions, companies verify the policies implemented effectively and modify security policies. In this paper, we define the required security solutions installed on PC to prevent disclosure of personal information in a variety of PC security solution, plan to integrate operations of the solutions in the blocking personal information leakage point of view and propose security policies through PC security solution log analysis.

Keywords: Personal information, PC security solution, log analysis

I. 서 론

우리나라 인구의 대부분이라고 할 수 있을 정도의 개인정보유출 사고가 지속적으로 발생하고 있다. 2013년 12월 시중은행에서 고객 개인정보 13만 여

접수일(2014년 8월19일), 수정일(2014년 9월 29일), 게제확정일(2014년 9월29일)
† 주저자, katc237@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

건이 유출되는 사건이 발생하였고[1], 2014년 4월 시중 카드사에서도 1억여건의 정보가 유출 되었다[2].

국가정보원 산업기밀센터에서 발표한 통계자료에 따르면, 최근 5년간 발생한 국내 핵심기술 유출 사건은 209건이며 이중 60.8%가 전직직원, 19.6%가 현직원원에 의해서 발생되었다. 유출 경로로는 카드형 USB, 외장하드, 스마트폰 등이 사용되었다[3]. 통계자료에서 알 수 있듯이 현재 국내 기업의 보안시스템은 외부 위협(해킹 등)을 방어하는데 적합하나 내부자의 정보유출로부터 개인정보를 보호하는 데는 한계가 있다고 보인다.

기업 특히 금융회사에서는 개인정보 유출을 차단하기 위하여 PKI 기반 인증 및 권한관리, 통합계정 권한관리(IAM), 문서DRM, 보조기억매체 통제 시스템, 출력물 통제 시스템, 개인정보 검색시스템, 네트워크 접근제어 시스템 등 다양한 보안시스템을 구축 및 운영하여 개인정보에 접근할 수 있는 사용자를 제한할 뿐만 아니라 오용을 방지하기 위한 2차 방안을 수립하여 운영하고 있다.

하지만 개인정보유출 사고가 지속적으로 발생하고 있고, 사건 발생 후 피의자를 기점으로 보안시스템 로그를 분석하여 원인을 파악하고 유출경로에 해당하는 시스템을 수정 보완하고 있다. 이러한 PC보안솔루션의 단순 구축 후 사후 점검보다는 각 기업에 적합한 보안정책을 사전에 수립하고 정책에 맞는 시스템을 운영한다면 개인정보유출 사고를 미연에 방지할 수 있을 것이다. 또한 로그분석을 통하여 보안정책이 효과적으로 시행되고 있는지 검증함으로써 로그분석 결과를 바탕으로 보안정책의 수정 보완이 가능할 것이다.

이러한 관점에서 본 논문은 다양한 PC보안솔루션 중 개인정보유출 방지를 위해 PC에 필수 설치되는 보안솔루션을 정의하고, 필수보안 솔루션을 개인정보 보호 관점에서 통합 운영하는 방안, 그리고 로그분석을 통해 개인정보유출 사고 방지를 위한 효과적인 보안정책을 제안하고자 한다.

II. 관련 연구

2.1 로그분석의 필요성

대부분의 회사에서는 시스템에서 생성되는 방대한 양의 로그를 정기적으로 백업하고 있지만 양도 많을 뿐만 아니라, 무슨 내용이 담겨 있는지 모르며, 막상 사용하려면 분석하기도 쉽지 않다.

그렇지만 사고가 발생했을 경우 추적할 수 있는 유일한 자료가 로그이기 때문에 로그 보존은 필수적이다. 또한 로그 파일은 법적증거자료로 활용하는 것도 가능하다. 더욱이 보안사고가 발생하기 전에 이상증후 여부와 외부에서의 해킹시도 여부를 감시하여 알아낼 수 있는 유일한 자료가 바로 로그이다.

정기적인 취약점 진단과 함께 정기적으로 로그를 분석할 수 있다면 Proactive한 보안 대응체계를 구축하는 것이 가능해진다. 특히 방화벽(Firewall)이나 침입탐지시스템(IDS)이 설치되지 않은 기관에서는 침입시도 여부를 감지할 수 있는 유일한 판단자료가 시스템 내부의 로그파일이기 때문에 더욱 로그분석이 필요하다[4].

금융회사 정보기술(IT)부문 보호업무 모범규준에 따르면 “금융회사 등은 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 주기적으로 전자금융기반시설에 대한 취약점 분석 평가를 실시하여야 한다.”라고 규정하고 있다[5]. 따라서 로그분석이 필요하지 않은 기관은 없지만, 특히 금융회사에서는 로그분석이 반드시 필요하다.

2.2 로그분석 대상 흐름

최근 보안시스템 로그 관리 분야의 동향은 통합보안관리(ESM)에서 위험관리시스템(RMS), 보안 정보 및 이벤트 관리(SIEM)에 이르기까지 지속적으로 진화하고 있다. 이 가운데 로그 통합관리를 위해 등장한 SIEM은 이기종 환경의 인프라 및 보안로그를 효율적으로 통합 운영하고 리스크를 낮추기 위한 해결책으로 받아들여지고 있다[6].

SIEM은 방화벽, 침입방지시스템(IPS) 등의 네트워크 정보보호를 위한 보안솔루션들에서 쏟아내는 로그를 분석해 사고를 미연에 방지하는데 초점이 잡혀있다[7].

2.3 선행 연구와의 차이점

본 연구는 첫째, 기존의 연구에서 다루지 않았던 PC보안솔루션의 로그분석을 통한 개인정보유출 차단을 위한 효과적인 정책을 찾기 위해 수행되었으며, 둘째, 실 사례를 바탕으로 보안정책 수립 및 변경에 관한 효과적인 방향을 제시한다는 점에서 의의가 있다.

III. 로그 분석 대상 PC보안 솔루션

금융감독원은 금융회사 정보기술(IT)부문 보호업무 모범규준을 통하여 정보보호시스템을 컨텐츠 정보보호, 시스템 정보보호, 네트워크 정보보호, 정보보호관리 관점에서 분류하여 제시하였다[8]. 이중 개인정보 보호관점에서 PC내 개인정보유출을 방지하기 위해 반드시 설치되어 활용될 수 있는 3가지 솔루션은 개인정보필터링S/W(개인정보검색), 저작권관리(DRM), 자료유출방지(DLP)이다.

PC내 저장중인 개인정보를 보호하기 위해서는 개인정보 검색시스템으로 개인정보의 보유현황을 추출하고, 해당 문서를 삭제 또는 저작권관리(DRM)에 의해서 암호화하며, 자료유출방지(DLP)로 USB 등 보조기억매체 및 인쇄 등으로 유출되는 경로를 통제할 수 있기 때문이다.

개인정보 검색시스템은 PC내 저장되어 있는 개인정보 현황을 검색하여 사용자에게 개인정보 저장 현황을 알려주는 시스템이다. 개인정보 중 검색에 사용되는 항목으로는 주민등록번호, 신용카드번호, 계좌번호, 핸드폰번호, 전화번호, E-mail 주소, 여권번호, IP주소, 법인등록번호, 사업자등록번호, 운전면허번호, 건강보험증 번호 등이 있다.

저작권관리(DRM) 솔루션은 문서 저장과 동시에 자동으로 문서 암호화가 수행되므로 복호화하지 않은 이상 어떤 방법으로 외부로 무단유출이 된다하더라도 문서 읽기가 불가 하다. 또한 문서에 대한 열람/편집/인쇄 권한 제어가 가능하며 사용자별/업무별/부서별 권한관리가 가능하다. 암호화 된 문서 열람 시 PrtSc키 차단, 캡쳐툴 실행 차단 등 캡쳐 차단 기능, 출력 시 사용자의 소속 및 경고 문구를 삽입하는 워터마크 기능 등이 포함되어 있다.

DRM 솔루션이 문서를 암호화하여 외부로 유출되어도 읽을 수 없게 하는 방식인 반면, DLP 솔루션은 문서암호화는 적용 치 않고 유출 경로를 차단하여 문서 외부 유출을 통제하는 솔루션이다. DLP의 주요 기능은 보조기억매체 사용통제 및 출력물 통제로 보조기억매체의 통제는 USB, CD, 플로피디스크, 휴대폰 등으로 저장하는 것을 통제하고 업무상 필요시 관리자 승인을 받게 한다. 출력물 통제는 인쇄를 차단하고 필요시 마다 관리자 승인을 통해 인쇄를 하도록 허용한다.

IV. 보안정책

보안 정책은 보안 솔루션 자체 기능을 중심으로 한 보안정책, 보안 솔루션들을 통합 운영하여 하나의 툴로써 관리하는 보안정책, 그리고 마지막으로 보안솔루션에서 기술적으로 처리할 수 없는 부분에 대한 관리적인 보안정책 3가지로 구분할 수 있다.

4.1 솔루션 별 보안정책

4.1.1 개인정보 검색시스템

금융회사에서 수집하는 개인정보는 공통 필수정보, 상품별 필수정보, 선택정보로 구분되며 공통 필수정보에는 성명, 고유식별정보(주민번호, 여권번호 등), 집(직장) 주소, 연락처(집, 직장, 휴대폰 중 선택가능), 직업군, 국적 등이 있다. 상품별 필수 정보는 개별 상품의 체결 및 이행에 필수적인 정보로서 해당상품을 이용하는 고객에 대해서만 별도로 수집하는 정보이며, 선택정보는 계약체결에는 필수적이지 않지만 거래조건(금리, 한도 등)에 영향을 미치거나 무료상해보험가입 등 부가혜택을 제공하기 위해 필요로 하는 개인정보이다[9].

파일의 검색 대상 항목, 검색 주기 및 검색 결과 통지 방법에 따라 활용 방안을 분류할 수 있다. 검색 대상 항목은 공통 필수 개인정보 중 정형화된 패턴으로 추출할 수 있는 고유식별정보 중 금융거래에 가장 많이 사용되는 주민번호, 연락처정보 중 휴대폰으로 제한 한 후 필요 시 확대 적용한다. 주기는 사용자 수동검색방법, 시스템 자동검색(매일, 매주, 매달) 방법이 있으며 검색 결과를 통지 하는 방법에는 알림창(POP-UP)을 통한 사용자 즉시 제공, 소속 부서별 검색 결과 조회화면 제공, 소속 부서장에게 메일로 전송하는 방법 등이 있다. Table 1. 은 개인정보 검색 시스템에서 수립할 수 있는 보안 정책이다.

Level 1에서 Level 3까지는 수동적인 정책에서 적극적인 정책으로 강화되고 있다. 정책 강화에 따라 개인정보 검색 결과 조치가 향상될 거라 판단된다.

정책 운영 시 고려사항으로는 세 가지가 있다. 첫째, 검색 대상 항목을 추가 할수록 검색 속도는 길어지며, PC성능에 영향을 미친다.

Table 1. Policies of personal information filtering software

Level	Content
1	- Employees themselves delete after execution
2	- Execution by the software and real-time notification to the employees - Delete the detected file by employees
3	- Execution and delete by the software

근무시간(9:00~16:00) 및 PC성능을 고려하여 검색 대상을 제한할 필요가 있다. 둘째, Level 1 운영 시 사용자가 삭제하지 않을 경우 개인정보가 지속적으로 PC에 남아 있을 수 있는 한계가 존재한다. 셋째, 개인정보 검색시스템은 정의된 패턴에 의해 개인정보를 추출한다. 정의된 패턴과 동일한 자료가 존재할 경우 보안담당자가 의도하지 않은 결과를 초래할 수 있다. 예를 들어 Level 3 정책 운영 시 주민번호 패턴과 이클립스에서 생성된 로그 파일이 동일할 경우, 계좌번호 패턴과 핸드폰 번호 패턴이 동일한 경우 등 해당 파일들이 삭제되어 시스템 파일에 손상을 주거나 사용자가 보관해야하는 데이터가 삭제될 수 있다.

4.1.2 저작권관리(DRM, Digital Right Management)

DRM은 문서 접근 권한 등 다양한 정책을 구현할 수 있다. 연구소 등 인사이동 없이 지속적으로 근무하는 환경에서는 사용자 또는 부서별 정책을 구현할 수 있으나 금융회사는 정기/수시로 인사이동이 있으므로 사용자 또는 부서별 정책을 구현하는 데에는 한계가 존재한다. 그러므로 문서에 대한 접근 정책보다는 DRM 해제 시 통제 정책을 강화하는 것이 금융회사에 적합하다. Table 2. 는 DRM 해제 시 수립할 수 있는 보안 정책이다.

Level 1에서 Level 3까지는 수동적인 정책에서 적극적인 정책으로 강화되고 있다. 대외 기관 또는 고객에게 데이터 제공 시 처리 프로세스 강화에 따라 사용자의 불편함이 증가될 수 있다.

DRM 해제 정책을 강화화기 위해서는 기업 내 업무시스템이 DRM을 인식할 수 있도록 변경되어야 한다. 예를 들어 DRM 파일을 업무시스템 내 업로드 시 자동 복호화 처리를 하지 않을 경우 사용자의 불필요한 해제 신청이 많아 실제 통제하고자 하는 정책과 상이한 결과가 나올 수 있다.

Table 2. Policies of decoding DRM

Level	Content
1	- Employees decode by themselves without authorization
2	- Employees decode by themselves after getting authorization from officer within department
3	- Employees decode after check the source file by officer within department

4.1.3 자료유출방지(DLP, Data Loss Prevention)

보조기억매체 통제, 출력물 통제 방식 및 승인 절차 등을 변경하여 통제 정책을 적용할 수 있다. 예를 들어 보조기억매체 읽기 허용/쓰기 차단 정책, 필요 시 내부 승인 절차를 통하여 보조기억매체를 통한 정보유출을 방지할 수 있다. 또한 모든 문서에 워터마킹을 생성할 것인지, 문서 출력 시 마다 내부승인을 할 것인지, 모니터링 방식을 선택할 것인지에 대한 정책을 통해서 문서 유출을 관리할 수 있다. Table 3. 과 Table 4. 는 보조기억매체 통제 및 출력물 통제 시 수립할 수 있는 보안 정책이다.

Level 1에서 Level 3까지는 수동적인 정책에서 적극적인 정책으로 강화되고 있다. 정책 강화에 따라 사용자의 불편함이 증가될 수 있다.

Table 3. Policies of secondary storage control system

Level	Content
1	- Allow read and write - Monitoring usage
2	- Allow read/ block write - Write after getting authorization from officer within department
3	- Block read and write - Read and write after getting authorization from officer within department
4	- Block read and write - Write after check the source file by officer within department

Table 4. Policies of output control system

Level	Content
1	- Monitoring usage
2	- Watermark on output - Erase watermark after getting authorization from officer within department
3	- Block print - Print after getting authorization from officer within department

보조기억매체 통제 시 유의사항은 새로운 유형의 보조기억매체 도입 시 DLP 솔루션에서 인식하여 통제가 가능한 시점까지 보안의 허점이 생길 수밖에 없다는 것이다. 스마트폰을 저장매체로 사용할 수 있도록 하는 미디어 전송 프로토콜(MTP, Media Transfer Protocol)의 통제를 DLP솔루션에 반영되기까지는 약 2년 정도의 시간이 소요되었다.

출력물 통제의 경우 인쇄하는 파일의 정보(Spool에 저장된 정보)를 이용하여 통제 여부를 결정하나 화면캡쳐 파일 등 이미지 파일에 대한 스풀정보 분석할 수 있는 솔루션이 현재 국내 시장에는 미흡하다. 따라서 현재에는 이미지를 통한 개인정보 유출 사고를 DLP를 통해서만 차단하는 것이 미흡하여 사람에 의한 관리적인 절차가 필요한 상황이다.

4.2 솔루션 통합 보안정책

4.2.1 솔루션 기능 통합

보안솔루션간의 기능 통합을 이용하여 개인정보 유출차단을 위한 보안정책을 수립할 수 있다. 개인정보 검색시스템과 DRM을 연동하여 검색 결과를 자동 암호화하는 효과를 발생할 수 있다. 또한 개인정보 검색시스템과 DLP솔루션을 연동하여 USB에 파일를 저장 시 개인정보 포함 여부를 검사하는 추가 보안정책을 적용할 수 있으며, 인쇄 시 개인정보가 포함된 파일만 통제할 수 있게 되어 출력물 통제 정책을 펼치는데 사용자의 이해 가능성이 높아질 수 있다.

솔루션 기능 통합 시 유의사항으로는 두 가지가 있다. 첫째, 개인정보 검색시스템과 DRM 연동 시 압축된 파일에 대한 관리적 대안이 필요하다. 검색시스템은 압축된 파일(Zip 등)내 개인정보 포함여부를 검색하기 위해 압축된 파일과 동일한 파일을 추가로 생성하여 압축 해제 후 검색결과 정보를 수집한 후 압축 해제된 파일을 삭제한다. 압축된 파일 내 개인정보 파일 정보를 DRM에 이관 하더라도 DRM은 압축된 파일 내 개인정보 파일을 자동 암호화 할 수 있는 기술적 방안이 존재 하지 않는다. 둘째, 검색이 가능한 파일의 용량이 제한적이다. USB로 대용량의 파일을 이동할 경우, 예를 들어 시스템 메모리 덤프 파일 등은 검색이 불가하여 USB 저장이 불가하다.

4.2.2 결재시스템 통합

DRM, DLP 솔루션들은 정보 유출 통제를 위한 솔루션으로 통제적용을 위한 절차가 필요하고, 암호화문서 해제, USB 사용 권한 부여, 출력물 승인 등 통제 해제를 위한 절차도 있어야 한다. 이런 여러 가지 해제 절차를 하나의 승인시스템으로 일원화하면 사용자 편의성도 향상될 뿐만 아니라 보안담당자의 모니터링 부담도 줄일 수 있어, 보안의 효율성도 향상된다. 또한 정책이 변경될 경우 통합 승인시스템의 손쉬운 변경을 통해 신속한 정책 적용이 가능하므로 필수보안 솔루션간의 승인 프로세스와 시스템을 통합하는 것이 필요하다.

4.3 관리적 보안정책(제3자에 의한 통제 정책)

업무 수행을 위해 설정된 통제 정책을 해제할 필요가 있는 경우, 보통 책임자의 확인 과정을 거친다. 하지만 업무의 연속성에 관여하는 책임자에게 해제 권한을 주면 필요성 검증 보다는 업무의 신속성을 위해 의미 없이 승인하는 경우가 빈번하다. 그러므로 결재 시스템을 내부자 확인 후 제3자가 이차 확인하는 방식으로 구성한다면 불필요한 해제 과정은 줄게 될 것이다.

Fig 1.은 개인정보 문서의 USB 저장, 암호화해제 및 인쇄에 요구되는 각 승인프로세스를 하나로 통합하여, 해당 부서 관리자에 의한 1차승인과 본부통제 담당자에 의한 2차승인 프로세스를 보여준다.

USB에 파일을 저장할 경우 해당 파일에 개인정보 포함여부를 검색하고, 저장대상 문서에 개인정보가 포함되어 있으면, 부서관리자에게 시스템이 자동적으로 승인을 신청한다. 이때 자동 승인신청이 요구되는 개인정보 포함건수를 기준건수(임계치)로 설정하여 임계치 초과 승인 건은 본부통제 담당자의 2차 승인 절차를 진행한다. 해당 절차는 개인정보가 포함된 문서의 암호화 해제 또는 출력 시에도 동일하게

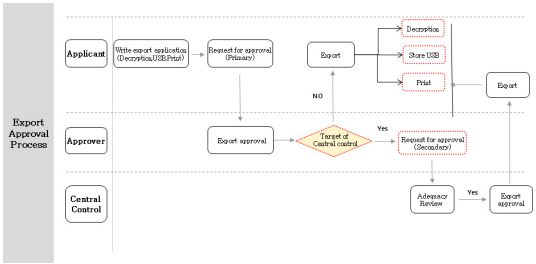

Fig. 1. The flow of the first approve by the administrator and the second approve by third party

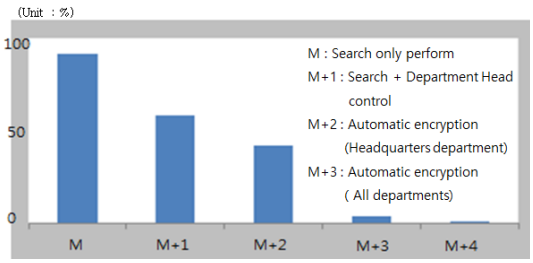

Fig. 2. Retention of personal information stored in the PC according to the security policy

적용된다.

V. 정책 적용 사례 및 로그분석을 통한 검증

솔루션 기능 및 결재시스템 통합, 관리적 보안정책의 효과성을 검정하기 위하여 A은행의 5개월간, 약 2만명 직원의 PC보안솔루션 로그를 분석하였다. A은행은 고유식별번호 중 주민번호 또는 연락처 정보 중 핸드폰 번호가 2개 이상 포함된 파일을 개인정보검색시스템 검출 대상으로 정의하였으며, 검색시스템 Level 2 정책과 DRM을 통합하였다. USB 통제는 Level 4 정책과 검색시스템을 통합하고, 제3자 승인을 운영하였으며, 출력물 통제는 Level 3 정책과 검색시스템 통합 및 제3자 승인을 운영하였다.

5.1 개인정보 검색시스템 정책 적용 및 분석

Fig.2는 보안정책이 PC에 저장된 개인정보 건수에 미치는 영향을 분석하기 위해 개인정보 검색시스템 단독운영, DRM과 연동한 자동 암호화 정책을 적용하면서 개인PC에 저장된 개인정보 건수를 보여준다. M월에는 매일 툴에 의한 검색을 하여 사용자에게 개인정보 저장 건수를 통지하는 방식을 사용하였다. M+1월에는 관리적인 차원에서 부서별 자체 점검을 부서장 차원에서 통제하였다. M+2월에는 전체직원의 20%인 본부부서에 개인정보를 포함하는 문서를 자동 암호화 방식을 적용하였다. M+3월에는 개인정보 포함 문서 자동암호화 방식을 전체 부서로 확산하였다. 또한 M+3월에는 관리적 차원을 강화하기 위하여 관리 부서에서 개인정보 과다보유자에게 전화 및 과다보유자의 관리자에게 시정 조치를 요구하였다.

단독운영 시 개인정보 보유현황을 기준으로 DRM과 연동 후 결과 비교 시 DRM 연동 후 개인정보 보유건수가 96% 감소함을 확인 할 수 있다.

5.2 USB 저장, DRM 해제, 출력물 통제 정책 적용 및 분석

Fig.3은 DRM, DLP 솔루션과 개인정보 검색시스템을 결합하여 개인정보 유출 차단 관점에서 시스템을 운영한 결과 추이를 보여준다. M월~M+1월에는 개인정보 포함 문서의 USB 저장, 출력 및 DRM 해제 시 업무 연관관계가 있는 책임자가 승인하게 하였다. M+2월부터 동일 업무 수행 시 개인정보 건수가 임계치를 초과하면 제3자 승인을 적용하였다. 제3자 승인 적용 이후 암호화해제 및 출력에 대한 추이가 하양하고 있음을 확인할 수 있다.

업무 연관성이 없는 제3자 승인 후 출력물 내 개인정보 건수는 62% 감소하였으며 USB 사용 건수 역시 70% 감소하였다. 관리적 활동으로 제3자에 의해 암호화 문서 해제 시 적정성 점검 강화 활동을 진행한 결과 해제 문서 내 개인정보 포함 건수가 69%의 감소 효과를 거둘 수 있었다.

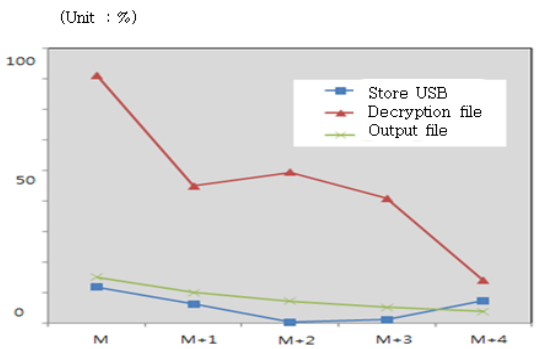

Fig. 3. Trend after the second approval number of USB storage, decryption file, output file

5.3 제 3자를 통한 개인정보 승인 요청 건수 추이

Fig.4는 제3자 승인을 통한 개인정보 승인 요청 건수의 감소 추이를 보여준다. M월 관리자 승인 건수는 일평균 61건, 제3자 승인 요청 문의 건수는 평균 24건, 승인 건수는 14건이다. M+1월에는 2차 승인 대상 임계치를 50건에서 30건으로 하양 조정하며 개인정보유출을 더 미세하게 통제하였다. 조정결과 대상 건수 일평균 194건, 문의건수 35건, 승인 건수는 26건으로 늘어났다. 그러나 1개월 뒤 지속적인 제3자 승인 통제로 전체 승인요청건수가 194건에서 171건으로 줄어들었다. 또한 제3자 승인을 통해 M월은 개인정보 노출 위험도를 77%, M+1월은 노출 위험도를 82% 낮추는 효과를 얻을 수 있었다. M월의 경우 1차승인 건은 61건이지만 제3자 승인 요청을 위한 전화 승인 요청건수는 24건으로 줄어들었고 제3자에 의해 실제 최종 승인된 건은 14건에 불과한 것으로 보아 꼭 필요치 않은 개인정보 반출 승인이 일어나고 있음을 알 수 있다.

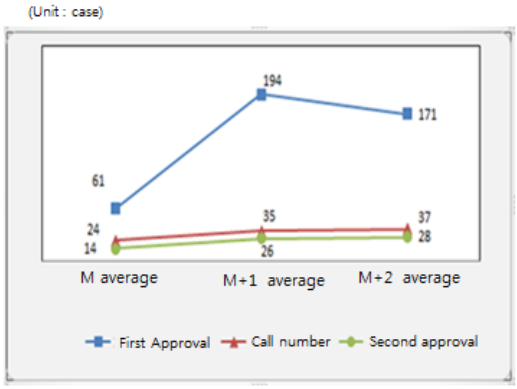

Fig. 4. Reduction Trend of Approval number of USB storage and output file

VI. 결론 및 향후 발전 방향

6.1 결론

금융회사는 감독규준 준수 및 개인정보 유출 방지를 위해 지속적으로 보안솔루션을 설치·운영하고 있으나, 개인정보 유출 사고는 끊임없이 발생하고 있다. 본 논문에서는 상용 PC보안솔루션 중 필수 설치 보안솔루션을 소개하고, PC보안 솔루션의 각 기능들을 개인정보 보호 관점에서 통합한 하나의 관리 툴로써 운영하는 방안을 적용하였다. PC보안 솔루션 통합 활용과 더불어 PC저장된 개인정보 과다 보유자에 대한 제3자에 의한 적극적인 개입과 1:1가이드를 제공하는 관리활동을 진행한 결과, PC에 저장된 개인정보 건수가 96% 감소하는 효과를 거두었다. 즉, PC내 많은 개인정보가 저장됨으로 인해 생기는 위험 노출 정도를 감소시키는 효과를 얻을 수 있었다. 또한 USB 저장 또는 문서 출력에 대해 부서관리자에 승인 요청되는 건수 대비 실제 제3자에 승인을 통해 최종 승인된 건수도 60% 이상 감소하는 결과를 볼 때, 제3자의 승인이 불필요한 개인정보의 외부 반출 시도를 현격히 줄일 수 있는 효과적인 수단이 됨을 알 수 있다.

본 연구에서 제3자의 의한 승인 내역 중 USB 저장 승인 건수와 문서출력 승인 건수 비중을 분석한 결과, USB 저장 승인 건수는 10% 이내 인 반면, 문서 출력에 의한 개인정보 반출 건수는 전체 건수에 90% 이상을 차지하고 있다. 카드사 개인정보 유출 사고 이후 직원들의 USB 사용에 대한 문제의식이 고조되고 있다는 영향도 있을 것이라고 판단되지만, 향후 개인정보유출을 보다 효과적으로 방지하기 위한 주요 모니터링을 개인정보 문서 출력물에 집중할 필요가 있음을 알 수 있었다.

6.2 향후 연구과제

본 연구에서는 정책의 검증을 위해 5개월간 생성된 PC보안 솔루션 각각이 가지고 있는 로그를 쿼리 작업 등을 통해 추이 분석한 바, 보안정책의 효과성을 검증할 수 있었다.

향후 연구에서는 이기종간의 PC보안 솔루션 로그를 실시간으로 수집하여, 로그분석을 통한 시나리오 패턴을 도출하고 시나리오 기반의 이상 징후 탐지 시스템 구축하는 것을 고려할 수 있다. 해당 시스템을 통해 학습된 사고 유형을 통해 사고유발 대상자를 지정하고 별도 관리함으로써 사전에 개인정보유출을 차단하는 시나리오를 구성해보고, 이 시나리오에 따라 개인정보를 통제한다면, 차후에 일어날 개인정보 유출을 예방하는 효과를 얻을 수 있을 것이다.

References

〔1〕 Yonhapnews, http://www.yonhapnews.co.kr/economy/2013/12/11/0301000000AKR20131211074400002.HTML

〔2〕 Yonhapnews, http://www.yonhapnews.co.kr/economy/2014/02/13/0301000000AKR20140213044400002.HTML

〔3〕 NIS, industry confidential protection center Industry and security information knowledge spill statistics, http://service4.nis.go.kr/servlet/page?cmd=preservation&menu=AAA00#.U4k8c3lZp9A

〔4〕 Huy Kang Kim, "Need for log analysis," Information Security 21C Contribution, pp.1, Feb. 2003.

〔5〕 Financial Supervisory Service, "Financial company information technology sector protection work best practices," pp.10, Oct. 2011.

〔6〕 Song-young Kim, Joseph Kim, Jong-in Lim, Kyung-ho Lee, "A study on the security policy improvement using the big data," journal of the korea institute of information security &Cryptology VOL.23, NO.5, Oct. 2013.

〔7〕 Digital Daily, http://www.ddaily.co.kr/news/article.html?no=120963

〔8〕 Financial Supervisory Service, "Financial company information technology sector protection work best practices," pp.51, Oct. 2011.

〔9〕 Korea Federation of Banks, "Comprehensive plan to prevent recurrence of personal financial information disclosure," pp.2, July. 2014.

〈저자소개〉

채 현 탁 (Hyun tak Chae) 정회원
2007년 2월: 전남대학교 전자컴퓨터정보통신공학부 학사
2007년 1월~현재: KB국민은행 정보보호본부
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 개인정보보호, 디지털포렌식, 빅데이터

이 상 진 (Sangjin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식