*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1435

# 보안문서와 트랜잭션ID 연계기반 개인정보유통경로 탐지기법 연구

신 재 호,† 김 인 석‡
고려대학교 정보보호대학원

# Study on Detection Technique of Privacy Distribution Route based on Interconnection of Security Documents and Transaction ID

Jae-ho Shin,† In-seok Kim‡
Center for Information Security Technologies(CIST), Korea University

## 요 약

금융회사에서는 내부자에 의한 개인정보유출 방지 및 내부통제 강화를 위하여 E-DRM(Enterprise-Digital Right Management), 개인정보검색, DLP(Data Loss Prevention), 출력물보안, 인터넷 망 분리시스템, 개인정보모니터링 시스템 등의 보안 솔루션을 도입 운영하고 있다. 하지만 개인정보유출 사고는 계속해서 발생하고 있으며, 이 기종 보안 솔루션간의 독립적인 로그 체계로 인하여 개인정보문서의 회사 내부유통 및 외부반출 관련한 정합성 있는 유통경로의 연관 분석이 어렵다. 본 논문은 보안문서를 기반으로 하여 업무시스템 및 이 기종 보안 솔루션간의 로그를 유기적으로 정합성 있게 연관 분석할 수 있는 연결고리 체계 방안을 제시하고, 업무시스템을 통하여 개인PC에 생성되는 보안문서나 개인이 작성한 보안문서에 대한 Life-Cycle 관리방안 및 개인정보가 포함된 보안문서에 대한 유통경로 추적을 위한 효율적인 탐지 방안을 제안하고자 한다.

## ABSTRACT

Finance Companies are operating a security solution such as E-DRM(Enterprise-Digital Right Management), Personal information search, DLP(Data Loss Prevention), Security of printed paper, Internet network separation system, Privacy monitoring system for privacy leakage prevention by insiders. However, privacy leakages are occurring continuously and it is difficult to the association analysis about relating to the company's internal and external distribution of private document. Because log system operated in the separate and independent security solutions. This paper propose a systematic chains that can correlatively analyze business systems and log among heterogeneous security solutions organically and consistently based on security documents. Also, we suggest methods of efficient detection for Life-Cycle management plan about security documents that are created in the personal computer or by individual through the business system and distribution channel tracking about security documents contained privacy.

**Keywords:** Personal Information, DRM, Distribution channel, Systematic chains, Life-Cycle management

Received(08. 24. 2015), Modified(1st: 10. 12. 2015 2nd: 10. 19. 2015), Accepted(10. 20. 2015)

† 주저자, mycall7230@gmail.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

## I. 서 론

개인정보유출사고는 최근에도 지속적으로 증가하고 있으며, 유출된 개인정보를 이용한 다양한 형태의 보안사고가 발생하고 있다. 2014년 1월 카드 3사 1억여건의 대량 고객정보유출 사고[1]에 이어 2015년 3월에는 아이핀 75만 건의 부정 발급[2] 등 크고 작은 정보유출 사건이 발생하고 있다. 금융위원회 및 금융감독원은 2014년 3월 발표한 '금융분야 개인정보 유출 재발방지 종합대책[3]'대한 이행 점검을 강화하고 있으며[4], 금융회사 개인정보유출 사고에 대한 제재 수준을 강화하고 있다. 이에 금융회사에서는 개인정보 유출 방지 및 내부통제 강화를 위하여 E-DRM(Enterprise-Digital Right Management)을 통한 문서 강제(자동) 암호화 적용, 매체통제 솔루션을 통한 보조매체(USB/CD-ROM) 사용 통제 적용, 개인정보검색차단솔루션(Data Loss Prevention, DLP)을 통한 사용자 단말(PC)내 개인정보 실시간 자동검색 및 문서 별 개인정보등급 적용, 출력물보안 솔루션을 통한 개인정보파일 출력 통제 및 출력물에 대한 워터마킹(WaterMarking) 적용, 인터넷 망 분리를 통한 내부 업무용 PC 인터넷 통제 정책 적용 등 강화된 보안정책을 수립하여 운영하고 있다. 하지만 개인정보유출 사고는 계속해서 발생하고 있고, 금융회사에서는 최근 보안시스템 로그를 실시간으로 수집분석을 위한 개인정보모니터링시스템 및 내부 이상거래 모니터링(Fraud Detection System, FDS) 시스템을 구축하여 내부직원의 비인가 · 비정상 행위 탐지 및 개인정보유출 사전 예방을 위한 노력을 기울이고 있다. 이러한 고도화된 보안시스템을 통한 개인정보유출 사전 예방 활동에도 불구하고 현재 금융회사에서 운영 중인 업무시스템 및 내부통제 보안 솔루션간의 독립적인 로그(Log) 체계로 인하여 개인정보문서의 내부유통 및 외부반출에 대한 정합성 있는 연관분석을 하는데 한계가 존재한다.

이러한 관점에서 본 논문은 금융회사 내에서 DRM을 통하여 95% 이상 생성 및 사용되는 보안문서를 기반으로 하여 업무시스템 및 이 기종 보안솔루션간의 로그를 유기적으로 정합성 있게 분석할 수 있는 연결고리 체계 방안을 제안하고, 업무시스템(Application, DB접속, FTP전송 등)을 통하여 개인 PC에 생성(저장)되는 보안문서나 개인이 작성한 보안문서에 대한 Life-Cycle(생성-유통-폐기) 관리방안 및 개인정보가 포함된 보안문서에 대한 유통경로 추적을 위한 효율적인 탐지방안을 제안하고자 한다. 본 논문에서 제시된 방안을 A 금융회사에 실제 적용하여 적용 전·후, 개인정보포함 보안문서의 정합성 있는 유통경로 추적이 가능함을 빅데이터 시스템(Splunk)을 이용하여 효과성 검증을 하였다.

논문의 구성은 총 6장으로 구성되었다. 2장에서는 본 연구와 관련한 앞서 선행된 기존연구와 주요 특징에 대하여 살펴보고, 본 연구의 차별성을 밝힌다. 다음으로 3장에서는 보안문서 헤더정보 내 변하지 않는 유일한(Unique)한 일련번호 색인(Index) 및 보안문서 파일단위 암호화 해제 정책 등을 제시한다. 다음으로, 4장에서는 보안문서 헤더정보의 일련번호 참조 기반 이 기종 보안 솔루션간의 보안 로그 연결고리 체계 구현을 통한 개인정보가 포함된 보안문서의 효율적인 유통경로 탐지기법을 제시한다. 다음으로, 5장에서는 실제 적용된 데이터를 빅 데이터 시스템을 이용하여 시나리오기반 효과성을 검증하였다. 마지막으로, 6장에서는 본 연구에 대한 결론을 맺고, 향후 연구에 대한 방향을 제시하고자 한다.

## II. 관련 연구

### 2.1 E-DRM (Enterprise Digital Right Management)

E-DRM 기술은 전자문서의 저장 및 관리의 주체를 기준으로 하여 PC DRM과 Server DRM으로 정의하여 사용한다[5]. PC DRM은 PC 내에서 사용자가 문서를 처음 생성하여 저장하거나 기존 문서를 수정하여 저장하거나, 또는 Application에서 사용자 PC로 문서 저장 시 암호화된 보안문서를 생성하며 생성된 보안문서에 대한 열람, 편집, 출력, 유효기간 등의 사용권한을 제어하거나 보안문서 내의 복사&붙여넣기차단, 화면 캡쳐차단 등의 컨텐츠 보호를 위한 보안 기능을 제공한다. Server DRM은 업무시스템 내에서 보안문서 생성, 열람, 출력, 저장 등 사용권한을 통제하는데 사용하며, PC DRM과 연계하여 생성된 보안문서의 사용권한 제어 및 컨텐츠 보호 기능을 제공한다.

Fig. 1. 과 같이 E-DRM에서 암호화된 보안문서를 생성 시에는 '헤더정보'를 생성한다[6]. 보안문서 헤더정보에는 보안문서의 효과적인 이력 관리를 위하여 문서이름, 생성자정보, 생성일자, 문서범주 등의 기본적인 정보가 포함되어 있다.

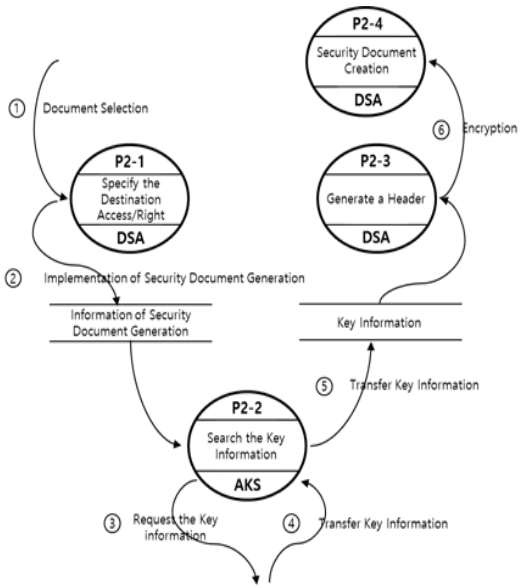


Fig. 1. Process of Creating Security Documents

최초 생성된 헤더정보의 내용은 해당 보안문서가 '해제' 되기 전까지는 그대로 유지되는 특성을 가지고 있어 보안문서를 열람, 편집, 출력 등의 행위가 발생할 때마다 E-DRM 시스템에서는 헤더정보를 로깅(Logging) 하여 보안문서의 Life-Cycle을 관리하고 있다.

하지만 보안문서 헤더정보(문서이름, 생성자정보, 생성일자)를 조합하여 문서의 Life-Cycle 관리를 수행하다 보니 특정 보안문서에 대한 유통 경로를 추적할 시에는 검색 속도에 대한 이슈가 발생하며 문서이름이 동일한 경우에는 정합성 있는 유통 경로를 추적하는데 어려움이 발생하고 있다.

### 2.2 DRM 및 보안시스템 로그 연계 기존 연구동향

최종욱의 연구[7]는 개인정보유출을 방지하기 위하여 E-DRM 기술에 DLP에서 사용하고 있는 내용 검색 기능을 통합한 PPS(Privacy Protection Safer)시스템을 제안하였다. 해당 연구는 사내 유통되는 민감한 정보를 DLP에서 검색하고 E-DRM을 기능을 이용하여 암호화하기 때문에 문서를 복호화하여 읽을 수 있는 사용자 수가 제한적이라는 점에서 DLP 기술에 비해 스마트기기의 카메라에 의한 유출에서 비교적 안전한 기술이라 제한하였다.

박성주의 연구[8]는 개인정보유출 방지를 위한 보안위험지표(Security Risk Indicator, SRI)기반 모니터링 시스템 개발을 제안하였다. 해당 연구는 금융회사의 개인정보보호 목표달성을 위한 기준을 설정하고 목표달성을 방해하는 위험과 금융회사에서 보유하고 있는 보안솔루션 기반으로 개발/유지보수(Application), 접근통제(System, Database), 통신/운영보안(Network, PC)에 해당하는 3개 부문에 보안위험지표(SRI)를 선정하였고, DRM 관련해서는 DRM 설치율을 SRI 기준으로 정의하는 등 선정된 SRI 기반으로 하여 개인정보 유출 위험을 사전에 파악하고 자동으로 측정하여 사고 징후를 조기에 포착, 대응하여 사고를 사전에 예방하며 사후 감사가 가능할 수 있는 방안을 제시하였다.

조성규의 연구[9]는 조직의 업무 연속성을 해할 수 있는 개인정보유출이라는 위험을 정의하고, 개인정보유출이 발생할 수 있는 근본 요소들인 핵심위험요인을 정의하였다. 또한 핵심위험요인들을 수치적으로 정량화하여 처리할 수 있는 핵심위험지표(Key Risk Indicator, KRI)를 활용한 개인정보 유출 모니터링 시스템의 설계 방안을 제시하였다. 해당 연구는 기업 내 환경에 맞는 개인정보유출관련 보안시스템 로그를 자동으로 수집하고 수집된 로그를 분석 알고리즘을 이용하여 분석을 수행하고 다양한 통계치를 산출한다. 관리자가 기 정의한 핵심위험지표에 대한 보안 임계치와 통계치를 비교하여 위험의 정도를 분류하며, 개인정보유출과 관련된 다양한 지표들에 대한 정보를 관리자에게 제공함으로서 실제 조직에서 개인정보유출과 관련된 위험요소들은 무엇이 있으며, 어느 정도인지 직관적으로 파악할 수 있는 방안을 제시 하였다.

채현탁의 연구[10]는 다양한 PC보안솔루션 중 개인정보유출 방지를 위해 PC에 필수 설치되는 보안솔루션을 정의하고, 해당 PC보안솔루션의 로그분석을 통해 개인정보유출 사고 방지를 위한 보안정책을 제안하였다. DRM 관련해서는 문서에 대한 접근정책보다는 DRM 해제 시 통제 정책을 강화하는 방법을 제시하였고, DRM 해제 정책을 강화하기 위해서는 기업 내 업무시스템이 DRM을 인식할 수 있도록 변경되어야 함을 강조하였다. 예를 들어 DRM 파일을 업무시스템 내 업로드 시 자동 복호화 처리를 해야 사용자의 불필요한 해제 신청을 통제할 수 있음을 제안하였다.

### 2.3 연구의 차별성

선행 연구를 종합해 보면 기존에는 DRM 기술을 이용하여 주요문서를 단순 암호화하여 데이터를 보호하는데 연구가 수행되었으나, 최근 연구에는 개인정보유출관련 기업 내 보안위험지표(SRI)나 핵심위험지표(KRI)를 선정하고 개인정보유출 방지를 위해 운영하는 DRM 및 각 종 보안시스템 로그를 수집/분석하여 기 정의된 보안 임계치와 비교하여 사고 징후를 사전에 파악하기 위한 연구가 수행되거나 보안시스템 로그를 분석하여 기업 내 환경에 적합한 보안정책을 제시하는 연구가 진행 되었다.

본 연구는 기존 연구에 비해 다음과 같은 차별성을 갖는다. 첫째, 보안문서 최초 생성 시 보안문서 헤더정보에 유일한 일련번호 색인 방법과 보안문서 파일단위 암호화 해제 방안을 제안하여 기존보다 효율적인 보안문서 Life-Cycle 관리를 수행하였다. 둘째, 보안문서의 일련번호 참조기반 이 기종 보안솔루션 간 유기적인 로그 연결고리 체계를 제안하여 개인정보문서 내부유통 및 외부반출에 대한 정합성 있는 유통경로 추적이 가능하게 하였다. 이를 위해서, A은행에 제안한 내용을 실제 적용하여 효과성을 검증하였다.

## III. 보안문서 정책 강화

외부로 유출된 개인정보문서의 내부 유통과정을 확인하기 위해서는 Table 1. 과 같이 문서의 생성부터 폐기까지 관리가 될 수 있도록 기업 내부의 프로세스를 수립해야 한다.

이를 위해 본 논문에서는 대다수의 기업에서 사용하는 DRM이 적용된 보안문서를 대상으로 문서가 생성되는 시점에는 문서의 고유성을 식별할 수 있는 일련번호를 헤더정보에 삽입하고, 외부로 반출되기 위해 보안문서에서 일반문서로 변환되는 시점까지 통제함으로써 기업 내부에서의 보안문서 유통과정을 탐지 할 수 있는 방법론을 제안하고자 한다.

### 3.1 보안문서 헤더정보에 일련번호 색인

보안문서(개인정보포함)의 Life-Cycle(생성-유통-폐기) 관리 및 효율적인 문서 추적을 위해서는 문서를 식별할 수 있는 정보가 필요하며, 보안문서의 경우 문서 생성자, 생성일시, 문서범주 등 보안문서의 정보를 담고 있는 헤더(Header)라는 공간에 고유의 일련번호 색인(Index)이 가능하다.

Table 1. Proposal methodology for detect distribution processes of security documents

| Division | Scope | Proposal Methodology |
|---|---|---|
| Creation of security documents | - Downloading documents from business system in companies importing via external media such as USB/CD<br>- Downloading documents from corporate web mail and internet site via internet data link<br>- Creating personal documents directly | - Inserting serial number when security documents create |
| Distribution of security documents | - Reading/Editing security documents<br>- Printing out security documents<br>- Detecting personal information | - Logging serial number about the security documents in DRM system, Printed matter security system and Personal information search system |
| Discard security documents | - Exporting via external media such as USB/CD<br>- Unlocking security documents for uploading internal business system<br>- Exporting documents from corporate web mail and internet site via internet data link | - Decryption of security document of file unit<br>- Logging serial number and approval number of Media control system and E-mail(Data link) system |

보안문서 생성은 사용자가 직접 문서를 생성하거나 외부의 문서를 반입하는 일반적인 경우와 기업 내의 업무시스템에서 조회한 내용을 문서로 추출하는 경우로 크게 분류할 수 있으며, 일련번호는 각 경우에 따라 다른 형태로 부여할 수 있다. 전자의 경우 유일한(Unique) 일련번호 체계를 구성하도록 일련번호를 색인하며 본 논문에서는 RID(Random Identification)로 명명한다. 후자의 경우에는 유일성뿐만 아니라, 업무시스템의 조회 내용까지 추적 가능하도록 트랜잭션ID를 이용하여 색인하며, 본 논문에서는 TID(Transaction Identification)로 명명한다.

예를 들면, Table 2. 와 같이 RID는 DRM에서 PC의 MAC값과 보안문서 생성일시(YYYYMMDDHHMMSS)를 조합한 값을 해쉬(Hash) 함수로 단 방향 암호화하여 생성한 값을 이용할 수 있으며, TID는 업무시스템에서 내용 조회 시마다 생성되는 트랜잭션ID를 보안문서의 일련번호로 색인 한다. 업무시스템을 통해 생성된 문서가 일련번호 RID로 사용한다면, 해당 문서가 사고로 유출 됐을 시 문서의 최초 생성자 추적은 가능하나, 해당 문서의 최초 생성자와 업무시스템을 조회한 사용자와의 일치 여부를 파악하기 위해 많은 노력 및 시간이 필요하다. Table 2. 는 보안문서 일련번호 생성규칙 TID 와 RID의 예시를 보여주며, Fig. 2. 는 보안문서 헤더정보의 예시를 보여준다.

DRM을 통하여 보안문서 생성, 읽기, 편집, 출력 등의 행위마다 일련번호를 포함한 보안문서의 헤더정보 내용을 로깅 및 관리하는 것이 중요하다.

Table 2. Creation rule for serial number of security document (Example)

| Division | Creation rule | Example |
|---|---|---|
| Transaction ID (TID) | Date of authoring full text: 8 digits | 20150601998 1Y1541813501504033 0 |
| | Name of system creating full text: 8 digits | |
| | Standard serial number of full text: 14 digits | |
| Random ID (RID) | Hash(MAC + Date of creation) | mDqMhLl1gUt9D FcmhwoPy7aE370 |

[ Business system ]

**Document name** : ₩Data₩Business₩information.xls
**Writer** : 011110984(Hong)
**Date** : 2015-06-02 10:34:56
**Document category** : CRM document
**Serial number** :201506029981Y1541813501504033 0

[ Personal ]

**Document name** : ₩Data₩Study₩Writing.ppt
**Writer** : 011110984(Hong)
**Date** : 2015-06-01 10:11:10
**Document category** : Personal document
**Serial number** : mDqMhLl1gUt9DFcmhwoPy7aE370

Fig. 2. Security document header information (example)

### 3.2 보안문서 파일단위 암호화 해제

금융회사 내에서는 암호화된 보안문서를 업무상 필요 시 해제를 수행하는데 있어 일반적으로 문서범주에 대한 사용자 단위의 보안문서 해제 권한 방식을 사용하여 불필요하게 보안문서를 해제 하는 경향이 있다. 이러한 불필요한 해제 행위는 본 논문이 제안하는 일련번호 기반 보안문서 추적성 확보에 미흡 하거나 보안상 취약한 부분을 노출하고 있어, 사용자 단위의 보안문서 해제 방식을 파일단위 암호화 해제

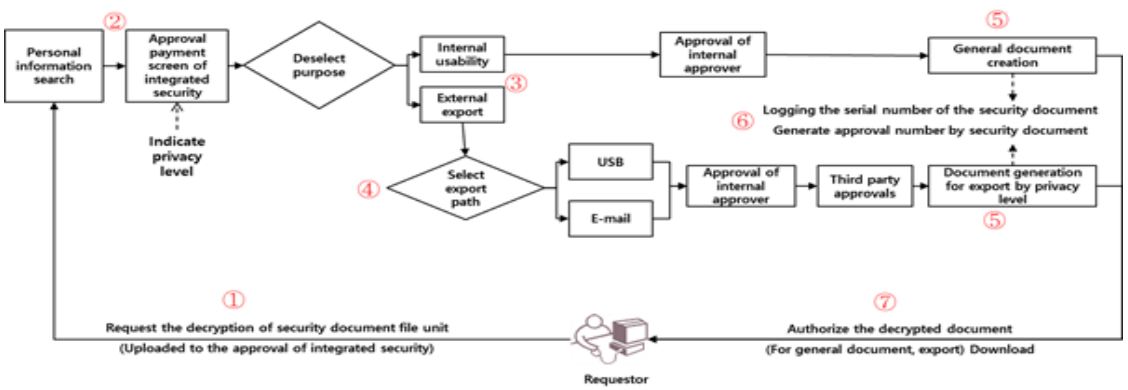


Fig. 3. Decryption Process of Security Document of File Unit

방식의 보안정책 적용을 제안한다. 파일단위 암호화 해제 프로세스는 Fig. 3. 과 같이 7단계의 과정을 구분하여 수행한다.

1단계, 해제 요청자가 통합보안결재승인시스템을 통하여 해제 요청할 보안문서를 업로드(Upload)하여 신청한다. 2단계, 업로드 한 보안문서를 개인정보 검색솔루션(DLP)와 연계하여 개인정보등급을 자동으로 화면에 표시한다. 개인정보등급은 Table 3. 과 같은 기준으로 5개 등급으로 구분하여 사용할 수 있다. 3단계, 암호화 해제목적(내부사용, 외부반출)에 따라 최종 승인권 자를 구분하여 적용한다. 내부사용 시에는 요청자의 부서장이 최종 승인을 하며, 외부반출 시에는 요청자의 부서장 승인 후 제3자에 의한 이중 승인을 통하여 보안을 강화할 수 있다. 4단계, 해제목적이 외부반출인 경우는 반출경로(USB, E-mail)를 추가로 선택한다. 5단계, 해제 요청에 대한 최종 승인이 완료되면 내부사용은 일반문서로 생성되고, 외부반출은 외부반출용 문서로 생성된다. 외부반출용 문서에는 반출경로(USB, E-mail)정보, 요청자정보, 승인번호, 승인일자, 개인정보등급을 헤더정보에 색인하여 개인정보유출경로를 탐지하는데 활용 할 수 있다. 외부반출용 문서는 Table 4. 와 같이 실행파일 형태로 생성되며 개인정보등급에 따라 문서의 권한이 다르게 부여되어 외부에서 DRM 솔루션 없이도 권한(읽기 횟수, 출력 횟수, 유효기간 등)에 따라 문서를 볼 수 있는 기능이 포함되어 있다. 6단계, 통합보안결재승인시스템에서는 해제 요청한 보안문서의 일련번호(TID, RID)를 로깅 및 관리하고 요청 문서 별 승인번호를 매핑(Mapping)하여 생성한다. 7단계, 요청자는 승인이 완료 된 '일반문서' 나 '외부반출용 문서'를 PC로 다운로드 한다.

외부반출용 문서 헤더정보의 반출경로정보와 요청자정보를 이용하여 USB 및 E-mail(자료연계)을 통하여 파일 반출 시 해제 요청자와 반출 요청자가 일치 하는 지와 반출 하고자 하는 경로가 일치 하는 지를 검증할 수 있어 개인정보유출차단에 효과적이라 할 수 있다. 물론 매체통제(USB)솔루션과 E-mail(자료연계)시스템에서 외부반출용 문서에 대한 검증을 위한 연동작업이 필요하며, 정상반출 시에는 매체통제 솔루션과 E-mail(자료연계)시스템에서 외부반출용 문서 헤더정보 내 승인번호를 로깅 및 관리하는 것이 중요하다. Fig. 4. 와 같이 외부반출용 문서 반출 검증 프로세스를 도식화 할 수 있다.

Table 3. Standards for privacy level (Example)

| Privacy level | Standards for privacy level |
|---|---|
| Level A | - More than 100 cases of four major detection targets<br>- Document file size of Level B is more than 1MB |
| Level B | - 50~90 cases of four major detection target |
| Level C | - 1~49 cases of Social security number, Credit card number and Account number<br>- 10~49 cases of four targets of major detection target |
| Level D | - Any information that include privacy under threshold<br>- Any information that was not including privacy |
| Level E | - Any personal information was not detecting |

- Detection target: Social security number, Phone number, Account number, E-Mail address, Credit card number, Foreign registration number, Passport number, Driver license number
- Major detection target: Social security number, Phone number, Account number, E-Mail address

Table 4. Privacy level of document for exporting specific right information (Example)

| Privacy level | Reading | Save | Printing | Validity |
|---|---|---|---|---|
| Level A | 20 times | Impossibility | Impossibility | 7 days |
| Level B | 50 times | Impossibility | Impossibility | 14 days |
| Level C | 100 times | Impossibility | 1 time | 30 days |
| Level D | Unlimited | Unlimited | Unlimited | Unlimited |
| Level E | Unlimited | Unlimited | Unlimited | Unlimited |

## IV. 보안로그 연계 및 분석

### 4.1 보안문서 일련번호 참조기반 이 기종 보안솔루션 간 보안로그 연결고리 체계 구축

일반기업들 중 특히 금융회사에서 개인정보가 포함된 문서가 외부로 반출 될 수 있는 경우는 정상 승인 하에 USB, CD, E-Mail, 문서출력, 전자FAX 등의 전달매체를 통하여 외부로 반출 될 수 있다.

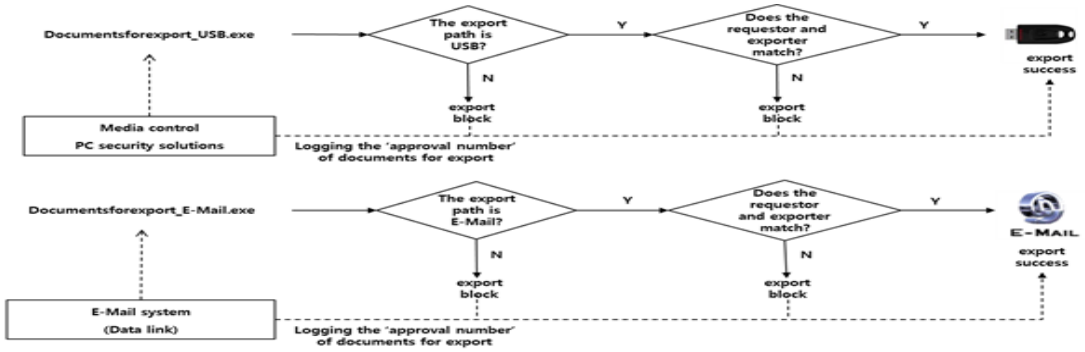


Fig. 4. Export verification process of documents

최근 금융회사 대부분은 DRM을 사용하고 있으며 생성되는 문서에 대하여 강제(자동) 암호화 정책을 적용하고 있어 개인 PC에서 사용되는 문서의 95% 이상이 보안문서 임을 알 수 있다. Fig. 5. 와 같이 개인정보가 포함된 문서의 유통경로 추적을 원활히 처리하기 위해서는 보안문서의 헤더정보 중 고유 식별자인 일련번호(TID, RID)를 참조하여 내부통제 보안솔루션마다 문서보안 일련번호를 로깅 하여 이 기종 내부통제 보안솔루션 간의 보안로그를 분석할 수 있는 연결고리 체계 수립이 필요하다. 예를 들면, DRM시스템에서는 보안문서를 생성/편집/출력 행위 시마다 일련번호(TID, RID) 로깅, 개인정보 검색솔루션에서는 보안문서를 개인정보검색 시마다 일련번호(TID, RID)와 보안등급 로깅, 출력물보안 솔루션에서는 보안문서를 출력 시마다 일련번호(TID, RID)와 보안등급 로깅, 통합보안결재시스템에서는 보안문서를 암호화 해제 요청 시마다 일련번호(TID, RID)와 보안등급, 승인번호를 로깅, 매체통제 솔루션에서는 외부반출용 문서를 반출 시마다 승인번호와 보안등급 로깅, E-mail(자료연계)시스템에서는 외부반출용 문서를 반출 시마다 승인번호와 보안등급을 로깅하여 관리한다. 이처럼 보안문서의 생성-유통-폐기 과정마다 일련번호 체계를 적용한다면 각 파일 로그마다 통일된 검색단위를 갖고 있기 때문에 일련번호 체계가 없는 경우보다 추적시간을 단축할 수 있을 뿐 아니라 결과에 대한 정확성 또한 높다는 것을 예측 할 수 있다. 이를테면, 반출된 보안문서에 대한 기업 내부의 유통과정을 추적하기 위한 총 추적시간은 다음과 같이 정의할 수 있다. 총 추적시간($Total_{time}$) = (A 시스템의 최대 검색빈도수 X A 로그 검색시간) + (B 시스템의 최대 검색빈도수 X B 로그 검색시간) + + (N 시스템의 최대 검색빈도수 X N 로그 검색시간) $= \sum_{n=A}^{n} count(n)$ X time(n)

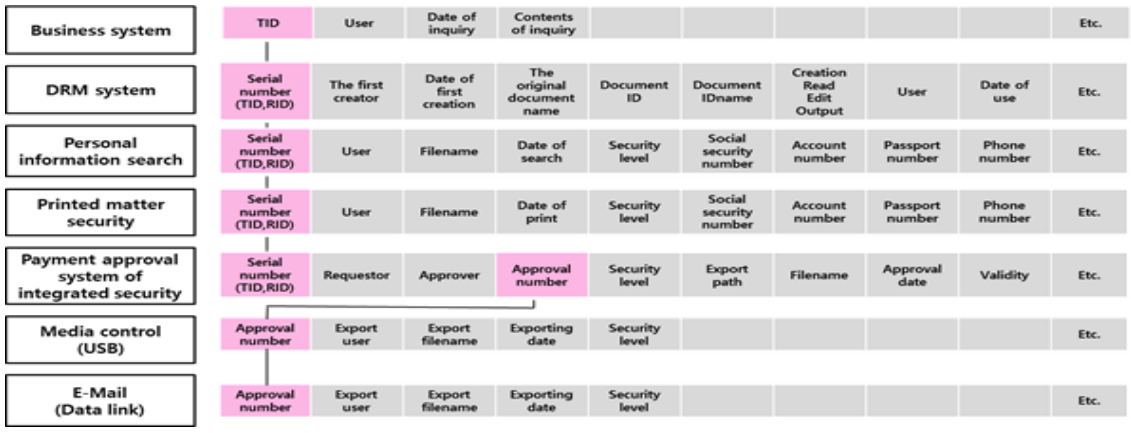


Fig. 5. Systematic chains of security log among heterogeneous security solutions based on the serial number

Table 5. Arithmetic expression of total time to track distribution channels of export security document

| Division | Total track time |
|---|---|
| No Serial number system | $Total_{time} = \sum_{n=A}^{n} count(n)$ X time(n) |
| Serial number system | $Total_{time} = \sum_{n=A}^{n} time(n)\,(Analysis\ system\ unused)$<br>$Total_{time}$ = time(S) (Analysis system used, S = Analysis system) |

최대 검색빈도수는 보안문서 추적을 하기 위해 필요한 각 단위 보안시스템 별 검색횟수의 합을 의미하며, 검색 시간은 각 단위 보안시스템의 로그 크기 별 걸리는 검색시간을 의미한다. Table 5. 와 같이 일련번호 체계가 없는 경우에는 각 보안시스템 별 최대 검색빈도수는 최소 1번 이상이며, 최대 해당 로그의 컬럼(Column) 수까지 추정 가능하다. 반면에 일련번호 체계가 있는 경우에는 검색빈도수는 검색단위가 일련번호로 통일되어 있기 때문에 각 보안시스템 별 1로 고정되어 있으며, 더 나아가 통합로그분석시스템을 이용하는 경우 총 보안시스템 별 1회 검색으로 추적이 가능하다는 것을 확인할 수 있다.

### 4.2 분석시스템 활용 개인정보유통경로 추적성 확보

보안문서 일련번호 참조기반 이 기종 보안솔루션 간의 보안로그 연결고리 체계를 수립한 후에는 기 운영 중인 개인정보모니터링시스템, 통합로그분석관리시스템(ESM) 등 분석시스템을 이용하여 Fig. 6. 과 같이 업무시스템, DRM시스템, 개인정보검색시스템, 출력물보안, 통합보안결재시스템, 매체통제시스템, E-mail(자료연계)시스템 등 내부통제 보안솔루션의 로그를 실시간으로 수집하여 보안문서 '일련번호' 기반 개인정보유통경로 추적성을 확보할 수 있다.

Table 6. Number of log by security solution

| Division | Number of log(Case) |
|---|---|
| Business system | 4,994,560,380 |
| DRM system | 43,128,149 |
| Media control solutions | 33,736,503 |
| Personal information search | 128,529,526 |
| Approval system of integrated security | 9,818,493 |

## V. 적용 사례 및 검증

보안문서 일련번호(TID, RID) 기반 이 기종 보안솔루션 간 보안로그 연결고리 체계를 통한 개인정보유통경로 탐지 방안의 효과성을 검증하기 위하여 본 논문에서 제안한 내용을 A은행의 실제 운영 환경에 적용하였다. 약 6개월(2015.01.01 ~ 06.30)간의 업무시스템 및 내부통제 보안솔루션(DRM시스템, 매체통제솔루션, 개인정보검색, 통합보안결재승인시스템)의 로그를 빅 데이터 시스템(Splunk)에서 수집하여 분석을 진행 하였다. Table 6. 은 빅 데이터 시스템에서 수집하여 분석한 업무시스템 및 보안솔루션 별 발생 로그 수를 보여준다.

보안문서 일련번호(TID, RID) 기반 개인정보유통경로 탐지 방안 효과성 검증을 위하여 Table 7. 과 같이 1가지 시나리오에 대하여 2가지 조건(Case1, Case2)으로 구분하여 각 Case 별 비교분석을 진행 하였다.

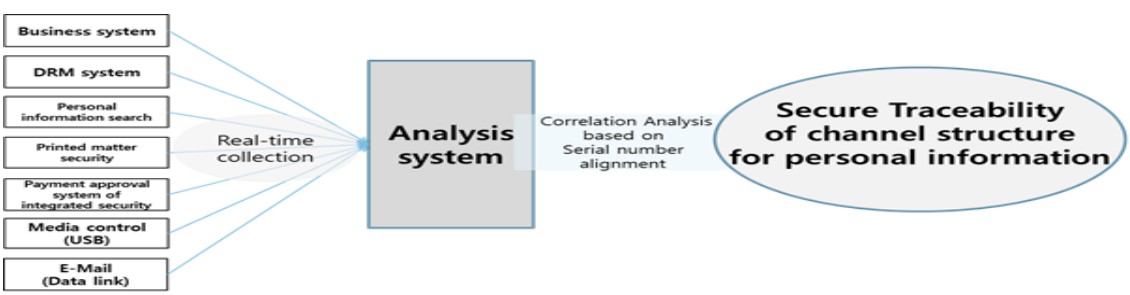


Fig. 6. Tracing process of channel structure for personal information based on serial number alignment by using analysis system

Table 7. Verification scenarios and conditions

| Scenario | Condition | Contents |
|---|---|---|
| Tracking internal Life-Cycle(Create-Distribute-Discard) about exported privacy 'Level C' documents from USB in approval export documents on June 24, 2015<br>- Source of document creation (Business system)<br>- First time of viewing business system by first creator<br>- First creator of document<br>- First time of created document<br>- Number of internal distribution user<br>- Total Number of edited document<br>- Number of printed document by users<br>- Total number of printed document<br>- Privacy level change of document<br>- Number of user who export document<br>- Number of exported document<br>- Total tracking time | Case1 | There is no serial number system in header information of security document |
| | Case2 | There are serial number(TID, RID) systems in header information of security document and systematic chains of security log among heterogeneous security solutions based on the serial number |

### 5.1 Case 별 시나리오 검증단계

Case1인 보안문서 일련번호 체계가 없는 경우의 시나리오 내용을 검증하기 위하여 Fig. 7. 과 같이 7단계 과정으로 검증을 진행 하였으며, Case2인 보안문서 일련번호 체계가 있는 경우의 시나리오 내용을 검증하기 위하여 Fig. 8. 과 같이 4단계 과정으로 검증을 진행 하였다. Case1인 경우는 보안솔루션 별 특별한 연결고리가 없으므로 반출된 '파일명'을 참조하여 분석을 진행 하였다.

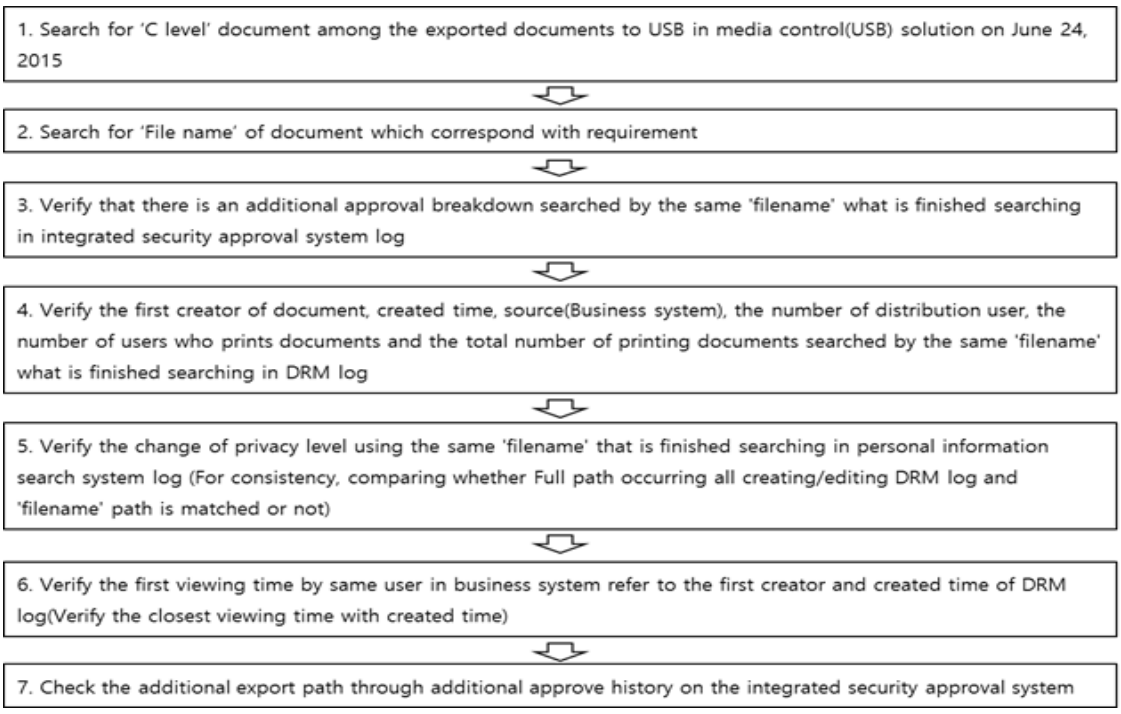


Fig. 7. Verification process of scenario about case 1

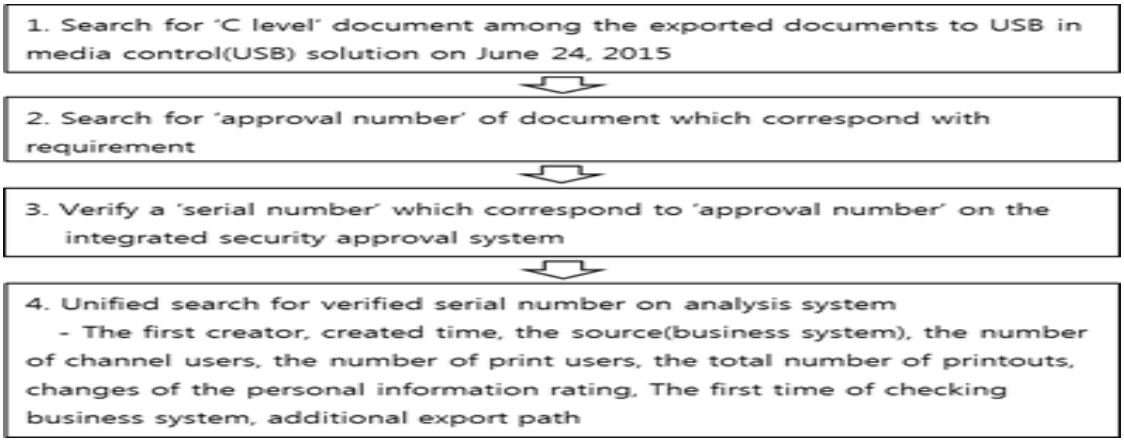


Fig. 8. Verification process of scenario about case 2

### 5.2 Case 별 시나리오 검증결과

빅 데이터 시스템에서 분석한 결과 6월 24일 USB로 반출된 문서 중 'C등급' 인 문서로 반출된 경우는 '윤*빈' 직원에 의하여 1개의 문서가 반출 되었으며, 반출된 외부반출용 문서의 '파일명'은 '담보현황요약_(2015_0331)' 이며, '승인번호' 는 '77*97ZuA77*9C**_vSjropXsjpkYEmVG' 이며, 해당 '승인번호'에 Mapping 되는 '일련번호'를 통합보안결재승인시스템 로그에서 확인한 결과 '20150331W1021699100844183200070O' 임을 확인 할 수 있었다. Case1 인 경우는 '파일명'으로 각 단계별 검증을 수행 하였으며, Case2 인 경우는 확인된 '일련번호'로 통합검색을 수행하여, Table 8. 과 같이 각 Case 별 시나리오 결과를 산출 하였다.

Table 8. Calculation results by scenario each case

| Division | Case1 | Case2 |
|---|---|---|
| Source of document creation (Business system) | Personal document Information terminal system Personal document | Information terminal system |
| First time of viewing business system | 20150331101012 | 20150331101012 |
| First creator of document | Cho, Rae, Rae, | Rae |
| First time of created document | 20150312102110, 20150331101229, 20150416113002, | 20150331101229 |
| Number of internal distribution user(Persons) | 6 | 8 |
| Total Number of edited document (Case) | 60 | 71 |
| Number of printed document by users(Persons) | 3 | 5 |
| Total number of printed document(Case) | 3 | 6 |
| Privacy level change of document | Yes | Yes |
| Number of user who export document(Persons) | 1 | 2 |
| Number of exported document(Case) | 2 | 3 |
| Total tracking time(sec) | 3,560 | 396 |

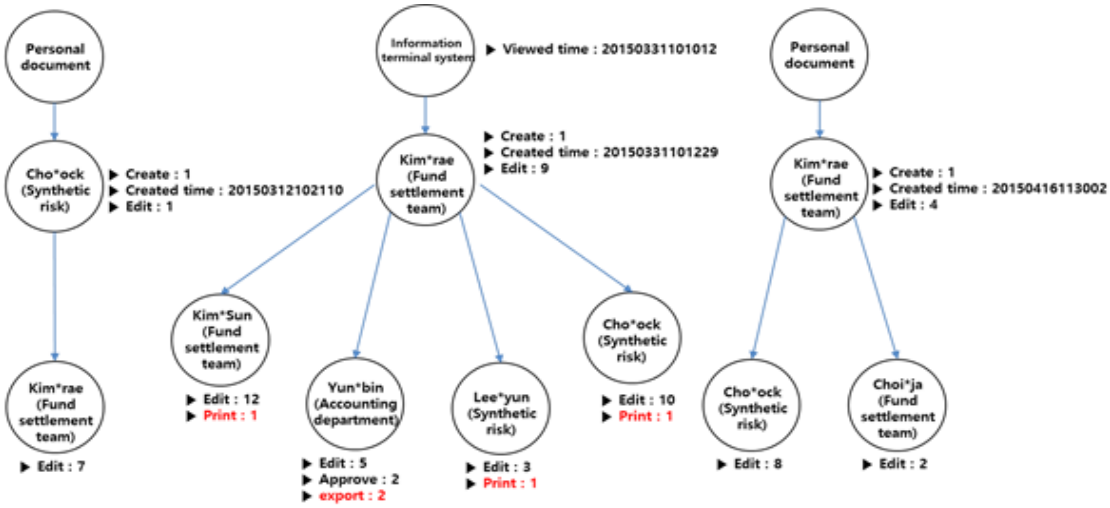


Fig. 9. Schematized for document distribution channels of Case1

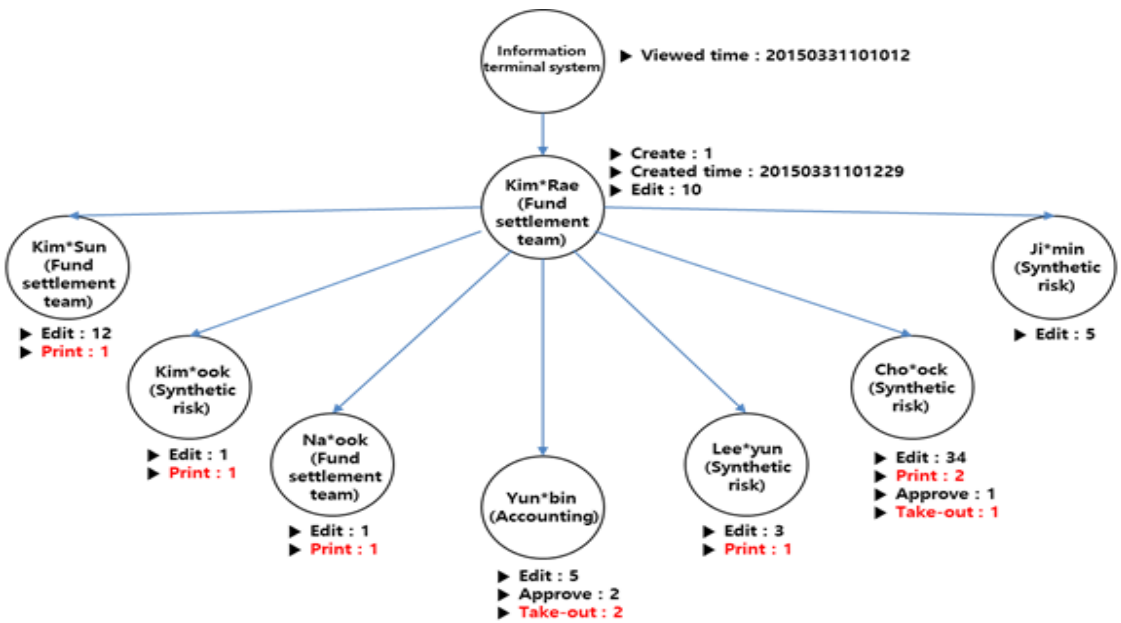


Fig. 10. Schematized for document distribution channels of Case2

또한 Case 별 보안로그를 분석한 결과 Fig. 9. 와 Fig. 10. 과 같이 문서유통경로를 각 Case 별 도식화하여 표현할 수 있다.

해당 결과에서 주목해야 하는 사항은 해당 문서의 반출부터 생성과정까지의 역 추적에 대한 정확성, 그리고 추적에 걸리는 시간이다. Table 8. 을 보듯이 Case1의 경우 반출 문서에 대한 생성 문서로 추정되는 문서가 3개인 것으로 추정되며, 이로 인해 해당문서 출력, 편집, 개인정보에 대한 정보들이 반출된 문서와 동일한 문서에 대한 정보인지 판단이 모호하다. 반면에 Case2의 경우 생성 문서를 정확히 추적할 수 있었으며, 편집과 관련된 로그 또한 동일문서에 대한 정보라는 것을 확인할 수 있었다. 또한 문서의 Life-Cycle(생성-유통-폐기)를 총 추적하는데

걸리는 시간이 Case1(3,560초) 보다 Case2(396초)가 약 9배 단축하여 추적이 가능하다는 결과를 얻을 수 있었다.

결과적으로 Case2 와 같이 본 논문에서 제안하는 보안문서 일련번호 체계가 있는 경우에는 없는 경우 Case1 보다 문서의 사내 유통경로 추적 및 실제 문서의 폐기(반출) 상태를 정확하게 확인 가능했으며, 추적 시간 또한 단축됨을 확인할 수 있었다.

## VI. 결론 및 향후 연구과제

금융회사는 개인정보유출 방지를 위해 지속적으로 지능화되고 고도화된 내부통제 보안솔루션을 설치운영하고 있으며, DRM을 이용하여 생성되는 모든 문서를 강제(자동) 암호화하는 보안정책을 적용하고 있다. 본 논문에서는 금융회사 사용자 PC에서 생성되는 대부분의 문서가 보안문서임을 감안하여 보안문서 헤더정보 내 변하지 않는 일련번호(TID, RID)를 색인하는 방안을 제안하였고, 일련번호 참조기반 이기종 보안솔루션 간 보안로그 연결고리 체계 방안을 제시하여 개인정보가 포함된 보안문서에 대한 정합성 있는 개인정보 유통경로 추적이 가능함을 A 금융회사에 실제 적용하여 효과성을 검증하였다.

하지만 기 운영 중인 보안솔루션들에 보안문서 일련번호를 참조하기 위한 프로그램 수정 작업이 필요하며 적지 않은 시간이 소요됨을 확인 할 수 있었다.

일반기업에서도 내부 주요정보 보호를 위하여 생성되는 모든 문서를 강제 암호화하는 정책을 추진하고 있어 본 논문이 제안한 보안문서 일련번호 참조기반 보안로그 연결고리 체계를 수립하여 운영한다면, 보다 더 효율적인 내부통제 강화에 도움이 될 수 있을 것으로 예상된다.

향후에는 DRM으로 암호화 되지 않는 일반문서에 대해서도 문서 추적성을 확보할 수 있는 방안을 연구하여 제시하고자 한다.

## References


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

〔2〕 Yonhapnews, http://www.yonhapnews.cokr/bulletin/2015/03/05/0200000000AKR20150305081700004.HTML

〔3〕 Financial Supervisory Service, http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp? url=&seqno=17681

〔4〕 Financial Supervisory Service, http://www.fss.or.kr/fss/kr/promo/bodobbs_view.jsp? url=&seqno=18293

〔5〕 Jingue Moon, "A Design of DRM solution for Prevention of Proprietary Information Leakage," Korea Computer Congress , pp. 7-10, Jun. 2007

〔6〕 Hangbae Chang, Sang-Soo Yeo, Gilcheol Park, and Changhoon Lee, "The Study on Development of Document Security Components," Journal of Security Engineering, 5(1), pp. 57-66, Feb. 2008.

〔7〕 Jong-Uk Choi, Yong-Jin Lee, and Ju-Mi Park, "E-DRM-based Privacy Protection Technology for Overcoming Technical Limitations of DLP-based Solutions," Journal of The Korea Institute of Information Security & Cryptology, 22(5), pp. 1103-1113, Oct. 2014.

〔8〕 Chae, Eun Ji, "A study on the PIMS based methodology for monitoring to prevent leakage of personal information in the banking industry," Graduate School of Dongguk University, Feb 2015.

〔9〕 Sung-Kyu Cho and Moon-Seog Jun, "Privacy Leakage Monitoring System Design for Privacy Protection," Journal of The Korea Institute of Information Security & Cryptology, 22(1), pp. 99-106, Feb. 2012.

〔10〕 Hyun tak Chae and Sang-jin Lee "Security Policy Proposals through PC Security Solution Log Analysis (Prevention Leakage of Personal Information)," Journal of The Korea Institute of Information Security & Cryptology, 24(5), pp. 961-968, Oct. 2014.

## 〈저자소개〉

신 재 호 (Jae-ho Shin) 정회원
1998년 2월: 강원대학교 정보통신공학과 졸업
2001년 5월~현재: KEB하나은행 IT보안부
2014년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 개인정보보호, 전자금융보안, 빅 데이터, 포렌식

김 인 석 (In-seok Kim) 종신회원
1973년: 홍익대학교 전자계산학과(학사)
2003년: 동국대학교 정보보호학과(석사)
2008년: 고려대학교 정보경영공학과(박사)
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규