The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 6, pp.25-30, Dec. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.6.25
JIIBC 2015-6-4

금융기관 개인정보 자산 분석 자동화 시스템의 설계와 구현

Design and Implementation of Financial Security Automatic System for Privacy Information of Financial Institution

이정민*, 김인석**

Jeong-Min Lee*, In-Seok Kim**

요 약 금융기관 보안의 가장 큰 화두는 정보에 대한 유출이다. 시중 대형 은행을 비롯한 금융기관에서도 각종 해킹과 취약점을 통하여 빈번이 유출하려는 시도를 받고 있고, 이 정보의 중심은 금융기관이 보유하고 있는 고객의 개인정보 이다. 금융기관의 보안 담당자들이 개인정보 유출 방지를 위해 다각적으로 노력하고 있으나 실상은 어떤 개인정보가 어디에 있는지도 모르는 경우가 많음을 이번 논문을 준비하며 더욱 확실하게 알게 되었고, 어디에 있는지 알고 있다고 추정을 하여 검색하더라도 다른 곳에서의 발견이 빈번하며, 일일이 수동으로 검색하여 인적/시간적 낭비가 많아 IT컴플라이언스 대응이 어렵다. 본 논문은 개인정보의 주요 보관소인 PC 및 Server를 주기적으로 자동화된 시스템으로 점검 관리하여 개인정보 유출 방지 및 IT컴플라이언스 대응에 효율성을 극대화 하고자 함이다.

Abstract One of the hottest issues of security is information leakage of financial institution. Financial institutions including commercial banks are frequently threatened by attempts of leakage through hacking and vulnerability, and this information is centered on personal information of their clients. Through this study, I found out that security managers of financial institutions are trying to prevent the leaking of private information, but in fact most of them barely know where their personal information is. Even if they know where it is and trace the data, it is often found in unexpected places. Because there is a lot of waste in time and human resources as search is done manually, we have understood that responding to IT Compliance requires a lot of effort. This study is to improve IT Compliance response and protect information leakage through monitoring PC and servers, the main storage of personal information by automated system, periodically.

Key Words : IT Compliance, Personal Information, Financial Institution

Ⅰ. 서 론

개인정보 유출사고의 금융기관의 피해는 영업정지, 대표이사 해임, 담당자 형사 처벌에 이를 정도로 막대하다. 개인정보 거버넌스의 가장 첫 단계는 개인정보 자산의 식별이다. PC 및 Server의 개인정보 자산 분석은 개인정보보호법과 정보통신망법에 목적과 정의 등에서 규제에 대한 기본적인 사항을 제시하고 특히 최근에는 감독기관의 감사 항목이 PC외에 아래와 같은 법 규정에 의해 Server 쪽도 금융회사에서 추가되고 있다.[6] 또한 금융감

*준회원, 고려대학교 금융보안학과
**정회원, 고려대학교 정보보호학과(교신저자)
접수일자: 2015년 10월 29일, 수정완료: 2015년 11월 29일
게재확정일자: 2015년 12월 11일

Received: 29 October, 2015 / Revised: 29 November, 2015 / Accepted: 11 December, 2015
**Corresponding Author: iskim11@korea.ac.kr
Graduate School of Information Security, Korea University, Korea

표 1. 관련 법규 정리

Table 1. Regulations cleanup_ Personal Information Protection Act (rate), Privacy Act Notice "Ensure safety measures based on personal information", Promotion of Information and Communications Network Utilization and Information Protection Act satisfaction

조항	법 규정	해석(법규준수기능)
개인정보보호법(률)		
제 1조 (목적)	개인정보의 수집, 유출, 오용, 남용으로부터 사생활의 비밀 을 보호, 국민의 권리와 이익을 증진하기 위하여 개인정보처리에 관한 사항을 규정한다.	PC내 사전 정의된 개인정보패턴만을 인덱싱 하므로 내부직원의 프라이버시를 존중하고 보호 해줌
2조 (정의)	★처리 : 개인정보의 수집,생성,기록,저장,보유,가공,편집,검색, 출력,정정,복구,이용,제공,공개,파기	- 전사적으로 PC내 개인정보를 검출 - 주기적으로 개인정보검출, 주기적 관리 - 취급 도에 따라 부서별, 개인별 별도정책 적용
28조 (취급자에 대한 감독)	개인정보취급자(개인정보를 ★처리하는 자)에게 적절한 관리, 감독을 행하여야 한다.	
제 21조 (파기)	① 개인정보가 불필요하게 되었을 때에는 지체 없이 파기	- 개인정보유효기간 지정 - 유효기간만료 및 장기간 방치된 개인정보검출
제 34조 (유출통지)	유출 인지 시에는 지체 없이 해당정보주체에게 유출된 개인정보 항목, 유출시점 및 경위.	- 개인정보 보유현황관리, 흐름통제-
개인정보보호법고시 “개인정보의 안전성 확보조치 기준”		
7조 7항 (암호화)	인터넷구간과 내부망의 중간지점(DMZ)에 고유식별정보 저장 경우 위험도분석과 관계없이 암호화를 적용해야 한다. DMZ의 대표적 예는 웹Server, 메일Server	- PC뿐 아니라 Server내 개인정보 검출, 파기, 암호화 - DMZ의 대표적 예는 웹Server, 메일Server
7조 8항 (암호화)	업무용컴퓨터에 고유 식별 정보 저장 시 상용 암호화소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.	- PC내 암호화되지 않은 개인정보 검출
정보통신망 이용촉진 및 정보보호 등에 관한 법률 만족		
23조의2 (주민번호제한)	① 주민등록번호를 수집, 이용할 수 없다.	DB, Server, PC, USB내 전사적 주민번호 검출 및 파기
27조의3 (누출 통지신고)	① 누출 시 이용자에게 통지(개인정보 항목, 시점, 이용자가 취할 수 있는 조치, 서비스 제공자 대응조치 등) 및 방통위에 신고 상시적인 개인정보 현황분석 및 Flow Control필요	1. 전사적 개인정보 현황분석 2. PC에서 개인정보의 보조저장매체 이동 및 출력 시 내역기록
30조의2 (이용내역통지)	① 이용자에게 이용내역(3자 제공 및 위탁 포함) 주기적 통지 상시적인 개인정보현황분석 및 Flow Control필요	
29조의2 (파기)	② 3년 이상 휴면사용자 개인정보 파기 유효기간지정 및 만료된 개인정보 검출파기프로세스 필요	1. 개인정보유효기간 지정 2. 만료된 개인정보 검출 3. 복구재생 불가한 방법으로 파기

독원 금융감독법규 정보시스템 세칙제·개정예고 511번 게시물인 “2015년 금감원 정보보안 점검항목에는 “공개용 웹Server_DMZ구간 내 이용자 정보 등 주요정보를 저장, 관리하지 않는지 여부”를 매월 보안점검의 날에 CISO가 점검할 정보보안 점검항목으로 신설 하여 외부망에 주요정보를 저장하지 않도록 관리 지침을 예고하였다. 특히 이러한 웹 환경에 노출된 웹Server는 개인정보 유출에 많이 노출 되어 있다.[3],[4] Server 쪽 개인정보 자산분석 자동화 시스템이 없을 경우 서버 담당자가 일일이 확인하는 작업을 하며, 실제로 DMZ 구간의 100여대 서버(은행 기준)를 모두 분석 하려면 10명의 인원이 2~3주간 작업을 한 경우가 있다. 그러나 실제로 감사기간의 감사에는 서버 담당자가 보고한 내용보다 더 많은 개인정보가 발견하여 문제가 된 경우도 있고, 자동화 분석 시스템을 도입하였으나 없을 것이라 추측하여 분석하지 않았던 서버에서 개인정보가 나왔다.

본 논문은 개인정보 자산 식별을 위한 자동화 시스템 구현에 있어서 요구사항과 분석과 그 설계와 적용, 그리고 정책에 의하여 체계적으로 개인정보를 관리하는 내용에 대하여 다룬다.

금융기관 보안담당자 및 개인정보 보호담당자는 개인정보 자산 분석 자동화 시스템의 필요성은 많이 인정하

고 있었다.

개인정보 자산 분석 자동화 시스템은 안정성, 성능, 부하 우려, 오탐에 대한 정교함이 대표적 요구사항이었으며, 시스템 운영 책임에 대한 부담 회피도 높게 차지하였다. 해당되는 개인정보 자산 분석 자동화 시스템 적용으로 효율적이고 안정적으로 개인정보 자산을 분석하고 개인정보 유출의 잠재적인 위험 제거의 방법을 기술하고자 한다.

II. 관련 연구

1. 관련 법령

행안부 위험도 분석표 만족에 법규정“ 내부 망에 있는 고유 식별정보 파일 현황분석 후 각 파일별로 위험도분석표를 작성“ 을 법규준수 기능으로 해석하면 ”내부망 내 DB, Server, PC내 고유 식별 정보 검출 및 현황분석” 이며, 다음 표와 같이 개인정보보호법(률),개인정보보호법고시 “개인정보의 안전성 확보조치 기준”, 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 관련한 내용이 있다. [표1]

2. 설문 조사

금융기관 50여개 종사자 100여명 대상으로 20개 항목을 설문조사 하였다. 설문조사는 총 4개의 파트로 1part에는 개인정보 자산 분석의 필요성을 인지하고 있는지 즉, 분석의 필요성과 관련법규 숙지여부, 유출사고 유무,분석의 효과(기대성) 등을 조사하였고, 2part에는 개인정보 자산 분석 수준. 즉, 개인정보 자산의 파악도, 정확도, 분석 주기 등을 조사하였고, 3part에는 개인정보 자산 분석 시 문제점. 즉, 개인정보 자산 검출수단, 기술적/정책적/환경적 등을 조사하였으며, 마지막 4part에선 개인정보 자산 분석 후 보호 조치. 즉, 검출 후 처리 조치 내용을 분석하였다.

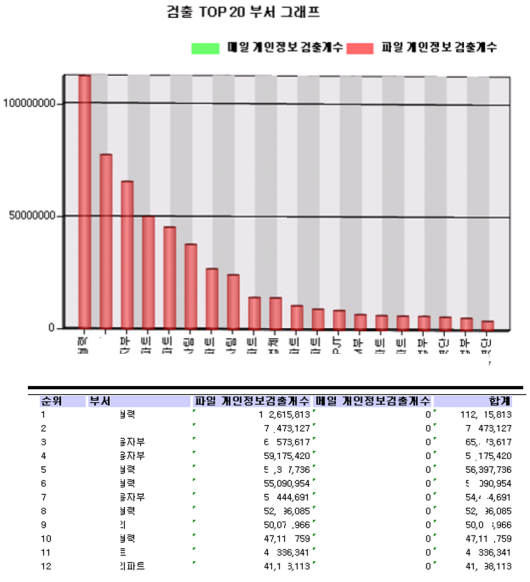
1part에는 개인정보 자산 분석의 필요성 및 유출사고가 있었는지에 대한 설문에 90%가 넘게 유출사고 경험이 있었고, 법규 숙지는 중간 수준이고, 분석도구를 도입함으로 잠재적인 위험을 제거 하는데 도움이 될 수 있다는 결과가 나왔다. 2part에는 개인정보 보유 현황에 대한 설문으로 보유 장소로는 PC와 파일Server 및 DB Server가 많았는데 DB Server의 자산분석은 DB암호화를 구현하기[5] 위하여도 필요하며. 취약 장소로는 스마트디바이스, PC, Server 순으로 결과가 나왔다. 스마트디바이스는 고객을 상대하는 업무를 하는 직원들 대상인데 아직 데이터 저장에 대한 금융회사 별 정책이 다르고 저장하고 있다고 하더라도 개인정보 자산 분석 후 중앙으로 데이터를 전달하는 이슈 등 아직 연구해야 될 부분이 많다. 그러나 설문과 같이 취약 장소를 스마트디바이스로 선택한 것은 한국 ICT추진협회에서의 조사 중 “본인의 정보가 유출될 것 같은 불안감이 있다“라고 응답한 사람이 전체의 23%에[2] 이를 만큼 불안감을 가지고 있으나 아직 보안에 대한 기술적 부족함이 많다. 3part에는 검출수단이 있으면 어떤 것인지와 검출수단을 도입 못했을 경우 이유 및 문제점에 대하여 설문한 결과로 PC쪽은 자동화 시스템을 사용한 경우는 39%에 불과하며 인터뷰와 설문 및 서류를 통한 분석이 주를 이루었고, Server쪽은 대부분 인터뷰와 설문을 통한 즉 수동으로 분석하는 경우가 대부분 이였다. 특이할 만한 사항은 자동화 도구를 도입 여부를 떠나 운용 인력이 부족함을 문제점으로 응답한 경우도 있었다. 4part에서는 개인정보 발생 시 어떤 조치를 하는지, 그리고 발생된 당사자의 반응을 설문하였는데, 발생 시 소유자나 부서장이 내부 보고 후 자율 처리되어 있고, 발생 당사자는 업무자료이니 업무 후 파기하겠다고 하거나 모르는 자료라고 하여 즉시 조치를 미루는 경우가 많았다고 응답 하였다. 자동화 구현으로 개인정보 검출내역을 리포트 형태로 팀장이나 부서장에게 자동으로 메일링하여 관리를 체계적으로 할 수 있는 시스템 구현이 필요함을 알 수 있다.

III. 개인정보 자산분석 자동화 시스템 구현

1. PC 내 개인정보 자산분석

PC 내 개인정보는 주로 PC에 agent를 설치해서 분석하며, PC에서 분석은 업무 부하를 우려해 스케줄링으로 업무 외 시간에 주기적인 분석을 하며 웹 형태의 대시보드로 개인정보의 개인별 부서별 보유 현황을 레포팅하여 관리 할 수 있으며[그림1] 부서별 개인별 등 업무의 특성에 따라 다양하게 정책을 적용할 수 있다. PC에 한번 저장된 개인정보는 끊임없이 복제가 되기 때문에 분석 정책으로는 개인정보 패턴명 및 반복횟수를 정하고, 검색

주기를 설정하며, 모든 파일을 분석할지 문서파일만 분석할지 여부, 파일크기 설정 및 압축파일 검사 여부, 검출결과 마스킹 및 암호화 여부, 검사 시 Windows 폴더와 같이 시스템 폴더들에 대한 예외처리 여부, 시작/종료 시 사용자PC에 알림 메세지 표시 여부, 검사 시 CPU할당량 조절 기능 및 유휴시간 설정 등을 정의 한다. 금융기관에서는 개인정보를 다수 취급하는 업무 특성상 개인정보 패턴 목록을 주민등록번호, 핸드폰번호, 신용카드번호, 계좌번호, 전화번호 등에 더 강력한 정책을 적용하며 업무의 특성상 법인등록번호나 사업자등록번호를 추가하기도 한다. 연구[1]에서는 금융회사에서 수집하는 개인정보에 대하여 실제 담당자가 소속회사에서 정의하고 정형화 된 패턴으로 분석 가능한 고유식별 정보에 대하여 검색 방법 및 결과를 통지하는 방법을 제시하고 개인정보 검색 시스템에서 수립할 수 있는 보안 정책을 제시 하였다.기본적으로는 자가진단을 통하여 자율분류를 하고 개인정보 유효기간을 지정하여 파일을 관리한다. 그리고 이 모든 정책설정 역시 웹 형태의 대쉬보드를 통해서 할 수 있다[그림1]



순위	부서	파일 개인정보검출계수	메일 개인정보검출계수	합계
1	남력	1 2,615,813	0	112, 15,813
2		7 .473,127	0	7 473,127
3	공자부	6 573,617	0	65, 73,617
4	공자부	59,175,420	0	5 ,175,420
5	남력	5 ,3 7,736	0	56,397,736
6	남력	55,090,954	0	5 390,954
7	공자부	5 444,691	0	54,4 4,691
8	남력	52, 36,085	0	52, 36,085
9	김	50,07 ,966	0	50,0 ,966
10	남력	47,11 759	0	47,11 ,759
11	트	4 336,341	0	4 336,341
12	김파트	41,1 3,113	0	41, 36,113

그림 1. PC 내 개인정보 보유추이
Fig. 1. Privacy retention trends in PC_Group part

2. Server 내 개인정보 자산분석

Server 내 개인정보 자산 분석은 크게 두 가지 방법으로 구현 가능하다. 첫 번째는 대상Server에 agent를 설치해서 분석하는 방식이며 관리Server로는 통계 데이터만 적재 되므로 개인정보 유출에 대한 우려가 없다. 두 번째는 directory 공유방식으로 NFS설치가 필요하며 개인정보 자산 데이터를 네트워크를 통해서 관리Server로 전송하여 중앙 집중적으로 분석하는 방식으로 순차적으로 분석하는 방식이다. 단 데이터 양이 많을 경우 네트웍에 부하가 생길 수 있으며, 관리Server가 또 하나의 개인정보 처리 시스템으로 Risk Point가 될 수 있다, 이런 FTP 방식은 SK컴즈의 2심 판결문 내용 중에서“FTP (FileTransfer Protocol)는 파일 전송을 위한 프로토콜로서 대량의 파일을 쉽게 송수신하는 역할을 하므로 개인정보를 보관하는 DBServer와 관련된 곳에서는 사용되어서는 안된다.”라고 의견이 나와 있다 [대구지방법원 3민사부 판결 2012나9865위자료 9page 내용] Server 내 개인정보 자산분석을 위해서 정책 부분은 PC 내 개인정보 자산분석과 큰 차이는 없으나 Server에 부하를 주지 않기 위해서 분석 인스턴스 개수나 CPU점유율, 검사 예외시간 등의 정책을 수립해야 하고[그림2], 이 모든 정책설정 및 분석 결과 확인은 웹 형태의 대쉬보드를 통해서 가능해야 한다.[그림3]

Discover 객체	세부사항	선택
기본구성	패턴	
	포멧	
	속성	기본설정
		파일
		폴더
	시간대	업무시간대
		비업무시간대
Detection Rules	검사패턴	주민등록번호
		외국인등록번호
		운전면허번호
		여권
		계좌번호
		신용카드번호
		핸드폰번호
		전화번호
		E-mail주소
		IP주소
	파일종류 자동탐지	사용 / 미사용
	압축파일검사	사용
		미사용
Discover 정책	검사 성능조절	인스턴스 개수
		CPU점유율
		검사 예외시간

그림 2. Server내 개인정보 자산분석 정책 샘플
Fig. 2. Privacy policy analysis sample of server assets

그림 3. Server 내 개인정보 보유추이
Fig. 3. Privacy retention trends in Server_Group part

Ⅳ. 기대효과 및 향후과제

본 논문에서 제안하는 금융기관 개인정보 자산분석의 자동화는 실제로 많이 구현되어 있지 않다. 비용적인 문제로 구현되어 있지 못한 곳도 있었고, 구현되어 있더라도 전문적인 인력 부족으로 제대로 운영 되어 있지 않았고 정책 설정도 조직별 업무별로 다양하고 특성 있게 수립하여야 하지만 그렇지 못한 경우가 많았다.

PC 내 개인정보 검색 같은 경우에는 개인의 프라이버시에 대한 대책과, 검색된 정보를 어떻게 관리 보관하여 업무에 안전하게 사용할지에 대한 연구, 파기 할 때 완전 파기를 어떻게 해야 할지, 또한 더 나아가서는 DLP(Data Loss Prevention) 정책도 세워 개인정보가 출력물, 매체 및 네트웍으로 유출되는 것도 보완해야 한다.

Server 내 개인정보 검색은 개인정보 자산분석을 자동화함으로써 Server 개인정보 보유현황에 대한 지속적 관리 효과성 제고(현황파악, 사내 개인정보 파일 보유 현황 종류, 장기중인 개인정보 파일 파악, Server별 부서별), 중앙검색을 통한 개인정보 보유실태 자율점검 기반 마련, DMZ 구간 고유 식별 정보 암호화 관련 컴플라이언스 사전 대응을 할 수 있으며 웹 형태의 대쉬보드를 구현하여 필요 시 언제나 개인정보 자산의 소유 위치를 확인 할 수 있어야 한다. 대쉬보드는 PC쪽과 통합하여 PC와 Server 의 개인정보 보유 현황을 한눈에 볼 수 있다.

Ⅴ. 결론

금융기관의 개인정보 자산분석 관리 자동화한 시스템을 통하여 PC 및 Server 쪽에 있는 개인정보에 대한 저장 위치와 내용을 파악하여 남용 및 악용될 수 있는 개인정보 유출 방지에 대한 기초적인 기반을 확립하고, 감사기관이 나왔을 때에 즉시 관련 자료를 제출하여 인적/시간적인 불필요한 요소를 최소화 할 수 있는 기준을 제시하였다.

References

[1] Hyun tak Chae, 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 VOL.24, NO.5, Oct. 2014.

[2] Korea Association for ICT Promotion "Perspective of the user and the smartphon Utilization Study analyzed after regulation", 2010.12.31

[3] Young-Duk Seo, Jae-Young Chang "A Retrieval Technique of Personal Information in a Web Environment" The Journal of The Institute of Internet, Broadcasting and Communication 2015

[4] SeungWon Han, Sangjin Lee, GangShin Lee, YunHo Ch “A Study for Detection of Personal Information Leakage According to File Type” KOREA INFORMATION SCIENCE SOCIETY. 2009

[5] Woonseok Kim “An Overview of New Personal Information Protection Law”Chungnam National University Law Research Institute 2011

[6] Dong Rye Kim, Gi Chang Shim, Moon-seog

Jun"Study To prepare a study on the Privacy Act Personal Information Protection System"Korea Institute Of Information Security And Cryptology. 2011

저자 소개

이 정 민(준회원)

- 2001년 2월 : 인하대학교 금속공학과 졸업(학사)
- 2014년 3월 ~ 현재 : 고려대학교 정보보호대학원 석사 과정

<관심분야 : 전자금융법규, 금융회사 개인정보보호, 개인정보 라이프사이클, 취약점 보안>

김 인 석(정회원)

- 1973년 홍익대학교 전자계산학과(학사)
- 2003년 동국대학교 정보보호학과(석사)
- 2008년 고려대학교 정보경영공학과(박사)
- 2009년~현재 고려대학교정보보호대학원교수

<관심분야 : 전자금융보안, IT 감사, 전자금융법규>