ISSN 2234-4438
융합정보논문지 제7권 제3호 pp. 83-90, 2017 DOI : https://doi.org/10.22156/CS4SMB.2017.7.3.083

효율적인 개인정보 관리를 위한 IPIMS 설계

전병진[1], 신승수[1], 이준연[2*]
[1]동명대학교 정보보호학과, [2]동명대학교 미디어공학부

An IPIMS Design for Efficient Personal Information Management

Byung-Jin Jeon[1], Seung-Soo Shin[1], Jun-Yeon Lee[2*]
[1]Department of Information Security, Tongmyong University
[2]School of Digital Media Engineering, Tongmyong University

요 약 본 연구의 목적은 기업체의 정보보안 관리자가 모든 임직원들의 개인정보 보유 현황을 인지해야 하는 한계성을 해결하고자 한다. 본 연구에서는 정보보안 관리자와 부서별 정보보안 담당자가 개인별, 부서별 개인정보 보유 현황을 최소화할 수 있도록 효율적인 개인정보 보유 현황 관리시스템을 제안한다. 이를 위해 개인정보 보유 현황의 대상이 되는 점검대상 컴퓨터와 개인정보 보유 현황의 결과를 확인할 수 있는 점검결과를 PVA 시스템으로부터 효율적인 개인정보 보유 현황 관리시스템으로 전송하는 방법에 대해 연구하고, 확인된 개인정보 보유 현황을 최소화할 수 있는 방법에 대해서도 연구한다. 기존 PVA 시스템을 정보보안 관리자가 관리하는 One channel 방식을 정보보안 관리자와 정보보안 담당자가 관리할 수 있도록 Two channel 방식으로 변경하여 개인정보 보유 현황을 최소화한다.

키워드 : 정보유출, 개인정보, IPIMS, 인사정보, 데이터베이스

Abstract The purpose of this study is to solve the limitations that the information security manager of company should recognize the personal information of all employees. In this study, we propose efficient personal information retention status management system to minimize information retention status of personal information and department by information security manager and departmental information security officer. To do this, we study the method of transferring the check result from the PVA system to the efficient personal information retention management system, also study ways to minimize the amount of personal information we hold. It is possible to minimize the possession of personal information by changing the one channel method managed by the information security administrator of the existing PVA system to the two channel method so that the information security manager and the information security officer can manage it.

Key Words : Information Leakage, Privacy, IPIMS, Human Resource, DataBase

1. 서론

현대사회는 ICT기술의 발전으로 대량의 정보가 인터넷을 통해 다루어지는 시대이다. 대량의 정보 중에는 매년 15만 건 이상의 개인 신상 정보, 예금 정보 등도 포함되어 있다[1,2]. 최근 들어 개인정보 유출 사례가 급증하고 있는 추세이다. 그러나 대부분의 개인정보 유출 사건은 외부 해킹으로 발생한 것보다 내부의 악의적인 사용자가 유출하는 것으로 나타나 정보유출에 대한 심각성이 증가하고 있다[3]. 합법적으로 개인정보를 수집했더라도 시스템의 개인정보 보호 미 조치로 개인정보가 유출될 때에도 과징금을 부과하고 있으며, 기업의 존폐를 위협

Received 2017-06-02 Revised 2017-06-07 Accepted 2017-06-20 Published 2017-06-30
*Corresponding author : Jun-Yeon Lee (jylee@tu.ac.kr)

할 수도 있다[4-6]. 2013년 12월 모 은행에서 고객 개인정보 13만 여건이 유출되는 사건이 발생되었고, 2014년 4월 모 카드사에서도 1억여건의 정보가 유출 되었다[7]. 악의적인 내부 사용자에 의한 개인정보 관련 유출 사고로 인해 기업에서는 법정 분쟁 등에 따른 비용의 발생과 기업 이미지의 추락 등을 겪고 있으며, 개인정보가 유출된 직원들의 정보가 무분별하게 사용됨에 따라 프라이버시 침해 및 보이스 피싱 등의 피해 사례가 증가하고 있다[8]. 기업은 개인정보 유출을 막기 위해 DRM(Digital Right Management)과 DLP(Data Loss Prevention) 기능이 제공되는 PC보안솔루션을 도입하여 운영하고 있다[9,10]. 그리고 휴대전화와 메일로 통보하는 개인정보 유출 방지 시스템에 관한 연구가 진행되고 있다[11-13]. 그러나 개인 컴퓨터에 설치된 개인정보 보유 확인 에이전트(PVA : Privacy Verification Agent)에서 감지한 개인정보를 저장하는 시스템은 개인별 점검결과 만을 조회할 수 있도록 설계되었다[14].

최근에는 공공기관, 중소기업과 민간 기업은 개인정보 파일을 운영하는 경우 개인정보를 안정적으로 운용할 수 있도록 정보와 기능을 가진 SP-PIA(Safety Protection -Privacy Impact Assessment : 개인정보보호를 위한 PIA 정보시스템)을 운영하고 있다[3]. 또한, 개인정보 유출 징후 임계값을 설정하고 초과할 경우 정보보안 담당자에게 경고 메시지를 발송하는 시스템을 개인정보를 대량으로 취급하는 금융회사에 적용하고 있다[15].

지금까지 연구되어진 개인정보 보호 시스템들은 기업의 업무 형태를 감안하지 않고 개인 정보유출에 대한 부분만을 고려하여 개발되었다. 그리고 기업 내부 직원의 고의나 실수에 의해 임직원의 개인정보가 유출되는 사고들이 여러 차례 발생하면서 개인정보 보유 현황 관리시스템의 필요성을 인식하게 되었다. 따라서 효율적으로 개인정보 보유 현황을 관리할 수 있는 새로운 시스템이 필요하다.

개인정보 보유 현황 관리시스템은 많은 기업체에서 사용되고 있다. L사의 PVA 시스템은 정보보안 관리자에게만 모든 직원들의 개인정보 보유 현황을 관리할 수 있는 권한을 부여하기 때문에 많은 시간과 비용이 발생한다. 따라서 정보보안 관리자의 업무 부하를 감소시키기 위해 부서별 정보보안 담당자를 지정하고 개인정보 보유 현황 점검결과를 분석하여 개인정보 보유 현황을 최소화할 수 있는 효율적인 개인정보 보유 현황 관리시스템을 제안한다.

본 논문에서 제안한 효율적인 개인정보 보유 현황 관리시스템은 기존의 개인정보 보유 현황 관리시스템 점검결과를 부서별로 수치화해서 신속하게 제공한다. 또한 권한을 부여받은 정보보안 담당자는 소속 부서의 개인정보 보유 현황을 조회한다. 정보보안 관리자에게는 기존 개인정보 보유 현황 관리시스템에서의 조회 권한 뿐 아니라 부서별로 수치화해서 가독성을 증가시켜 준다.

본 논문은 다음과 같이 구성된다. 2장에서는 개인정보 보호 시스템에 관련된 연구를 분석하고, 3장에서는 악의적인 사용자의 개인정보 보유 현황을 확인할 수 있도록 효율적인 개인정보 보유 현황 관리시스템을 설계하고 구현한다. 4장에서는 효율적인 개인정보 보유 현황 관리시스템으로 악의적인 사용자의 개인정보 보유 최소화 방법을 분석하고 5장에서는 결론을 맺는다.

2. 관련연구

개인정보 운용 실태를 반영하여 김상복 등은 개인정보영향평가 정보관리시스템(SP-PIA)을 설계하여 구현했다[3]. SP-PIA 정보시스템은 개인정보 유출 징후에 대한 평가자, 수요기관, 중소사업자의 의견을 수렴하여 임계값을 설정하고 임계값을 초과할 경우 정보보안 담당자에게 경고 메시지를 발송하는 시스템이다.

개인정보 유출 모니터링 시스템은 KRI(Key Risk Indicator) 자동측정 모듈, 통합 모니터링 모듈, 위험관리 모듈의 서브시스템들로 구성되어 있다[8]. 위험관리 모듈의 서브시스템은 관리자가 정의한 특정 임계치를 초과한 경우 Mail, SMS, Pop-Up 등을 이용하여 정보를 제공하는 위험관리 모듈과 정의된 위험의 현재 정도 및 관련 핵심위험요인, 핵심위험지표 들의 현재 현황을 파악할 수 있는 기능의 화면과 관리자가 설정한 임계치 이상의 비정상 사용자들에 대해서는 소명처리를 할 수 있는 화면으로 구성되어 있다.

효율적인 개인정보 보유 현황 관리시스템을 설계하기 위해 L사에서 도입한 개인정보 보유 현황 관리시스템을 분석한다. 정보보안 관리자는 개인정보 보유 현황 관리를 위한 시나리오를 등록한다. 등록된 시나리오에는 점검패턴(주민등록번호, 계좌번호, 여권번호, 운전면허증 번호 등), 점검일자 등을 저장하면 정보보안 관리자가 등

록한 점검일자에 개인 컴퓨터에 설치된 PVA를 실행시킨다. PVA는 개인 컴퓨터에 저장된 모든 파일을 점검한 후 시나리오에 등록된 점검패턴을 포함하고 있는 파일을 찾아내고, PVA 서버로 점검결과를 전송한다.

정보보안 관리자는 전송받은 점검결과를 조회하여 개인정보를 보유하고 있는 파일이 하나라도 존재하는 인원들에게 온·오프라인으로 전달하여 조치하도록 한다. 개인정보 보유 인원들은 파일을 확인 후 삭제 또는 암호화를 해야지만 점검완료가 된다. 이와 같은 개인정보 보유 현황 관리시스템의 실행화면은 Fig. 1과 같다.

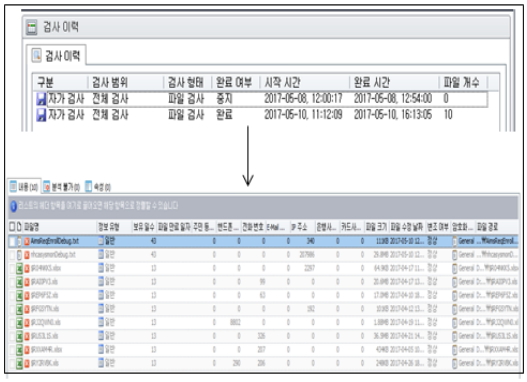

Fig. 1. PVA System

근무 인원이 작은 기업체의 PVA 시스템은 개인정보 유출에 대한 사전 탐지 및 대응이 실시간으로 가능하다. 그러나 L사(12,000명 이상)의 개인정보 보유 현황 관리 시스템은 개인정보 유형이 다양하고 근무 인원이 많아서 개인정보 보유 현황을 정보보안 관리자의 능력만으로 최소화하기에는 한계가 있다. 그래서 정보보안 관리자에게 트리형태로 부서별 개인정보 보유 현황 및 점검결과를 확인할 수 있는 권한과 기존 선정되어 있는 400여명의 부서별 정보보안 담당자에게 해당 부서의 개인정보 보유 현황 조회 권한을 부여해서 개인정보 보유 현황 최소화를 관리할 수 있게 하는 효율적인 개인정보 보유 현황 관리시스템을 제안한다.

3. 개인정보 관리시스템

본 장에서는 L사의 임직원 및 협력사 인원들이 악의적인 목적으로 기업체내의 개인정보 데이터를 유출할 수 있는 방법이 다양하게 존재하기 때문에, 이러한 문제점을 해결하고자 효율적인 개인정보 보유 현황 관리시스템(IPIMS : Improved Privacy Information Management System)을 제안한다.

3.1 시스템 구성과 데이터 흐름

IPIMS은 기업의 임직원과 협력사원들이 사내 업무시스템에 접속해서 악의적인 목적으로 개인정보 데이터를 수집해서 외부로 유출하는 것을 최소화하기 위해 임직원과 협력사원들이 사용하는 PVA의 점검 결과를 정보보안 운영 DB에 30분 간격으로 전송한다. 전송된 개인정보 보유 현황 정보를 기업의 부서정보 테이블과 연동하여 부서별 개인정보 현황을 정보보안 관리자가 확인할 수 있다. 정보보안 관리자는 해당 부서의 정보보안 담당자에게 온라인으로 점검결과를 통보하여 개인정보 보유 현황을 최소화한다. 또한, 정보보안 담당자는 IPIMS에 접근해서 소속 부서원들의 개인정보 보유 현황을 확인 후, 온·오프라인으로 부서원들에게 불필요한 개인정보를 삭제 또는 암호화한다.

3.1.1 시스템 구성

IPIMS는 PVA 시스템과 개인정보 보유 현황 관리 시스템으로 구성된다. PVA 시스템은 임직원과 협력사원들의 컴퓨터에 설치된 PVA 점검 결과를 MSSQL DB에 저장하고 접근 권한자는 정보보안 관리자이다. IPIMS은 PVA 점검 결과를 수신한 후, 부서별로 개인정보 보유 현황을 ORACLE DB에 저장하고 접근 권한자는 정보보안 관리자, 정보보안 담당자이다. 이와 같은 시스템 구성은 Fig. 2와 같다.

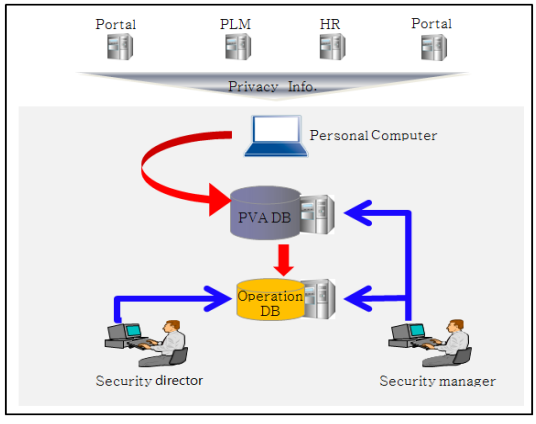

Fig. 2. System configuration

3.1.2 데이터 흐름

IPIMS의 데이터의 범위는 부서정보, 점검대상, 점검결과이다. 첫 번째, 부서정보는 인사정보(HR : Human Resource)를 하루에 한 번 전송받다. 두 번째, 점검대상은 임직원의 경우 입사 시 받은 컴퓨터와 업무상 필요에 의해 추가로 받은 컴퓨터이고, 협력사원의 경우 협력사에서 받은 컴퓨터의 현황을 Java App.을 통해 30분에 한 번씩 IPIMS 점검대상 테이블로 전송한다. 컴퓨터 이름과 사번으로 조회해서 있으면 데이터를 수정하고, 없으면 등록한다. 세 번째, 점검결과는 PVA DB에 저장된 개인별 개인정보 점검결과를 Java App.을 통해 30분에 한 번씩 IPIMS 점검결과 테이블로 전송한다. 컴퓨터 이름, 사번, 점검결과를 조회해서 있으면 데이터를 수정하고, 없으면 등록한다. 이와 같은 데이터 흐름은 Fig. 3과 같다.

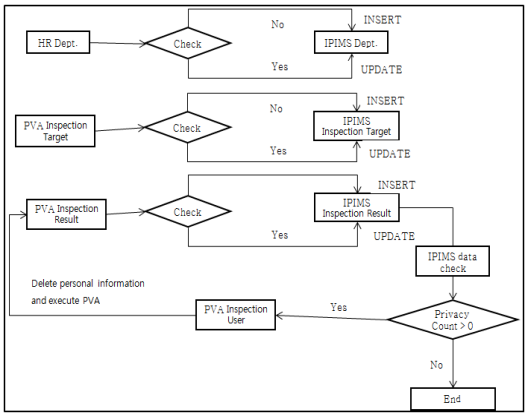

Fig. 3. Data flow of IPIMS

3.2 시스템 구현

IPIMS의 구현 환경은 하드웨어와 소프트웨어로 구성된다. 그리고 IPIMS의 프로토콜을 구현하기 위해 단계별 모듈을 정의하고 프로토콜을 설계한다. 그리고 설계된 프로토콜을 이용하여 프로그램 모듈을 구현한다.

3.2.1 모듈 환경

시스템 구현 환경의 하드웨어는 서버와 구현 소프트웨어로 구성된다. 서버의 운영체제는 Window7이고, 데이터베이스는 MSSQL과 ORACLE이다. 구현 소프트웨어는 Weblogic, Java, Jsp이다. 이와 같은 IPIMS의 구현 환경과 모듈은 Table 1와 같다.

Table 1. Implementation Environments of IPIMS

Div.	Component		Qty	Model
H/W	SERVER	CPU	1	Intel Core i7-2670QM
		Memory	1	8GB
S/W	OS	Window7 64bit		
	WAS	Weblogic8.1.6		
	Language	Jdk1.4, Jdk1.6		
	SQL Query	Ansi SQL		
	DataBase	MSSQL2008, Oracle 10g		

3.2.2 모듈 흐름도

IPIMS을 구현하기 위해서 5개의 모듈이 필요하다. 첫 번째, PVA 점검대상 테이블을 IPIMS 점검대상 테이블로 전송하는 모듈이다. 두 번째, PVA 점검결과 테이블을 IPIMS 점검결과 테이블로 전송하는 모듈이다. 세 번째, 전송된 개인별 개인정보 보유 현황 점검결과를 조회하는 모듈이다. 네 번째, 전송된 개인별 개인정보 보유 현황 점검결과를 수치화하여 부서별로 조회하는 모듈이다. 다섯 번째, 부서별 점검결과 인원 중 점검자와 미점검자의 현황을 확인할 수 있는 모듈이다. IPIMS의 구현 모듈의 흐름은 Fig. 4과 같다.

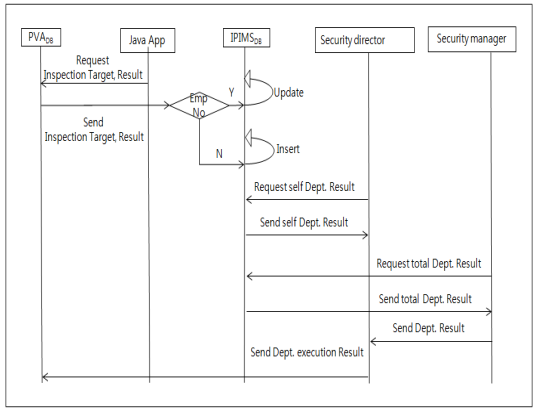

Fig. 4. Module flow of IPIMS

3.2.3 모듈별 프로토콜 구현

IPIMS의 모듈별 프로토콜을 다음과 같은 순서로 구현한다. 첫 번째, PVA_{DB} 점검대상 테이블을 Java App.을 이용해서 $IPIMS_{DB}$ 점검대상 테이블로 전송하는 프로토콜이다. 점검대상 테이블 전송 프로토콜은 월, 컴퓨터 이름, 사번 등으로 실행한다. 점검대상 테이블 전송 모듈의 프로토콜 및 실행화면은 Fig. 5와 같다.

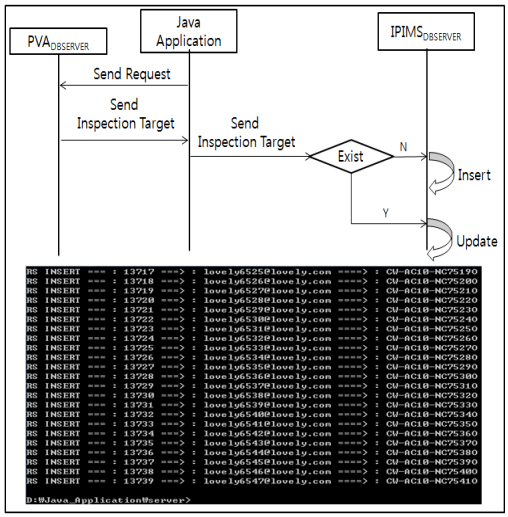

Fig. 5. Inspection target send protocol and execution screen

두 번째, PVA_{DB} 점검결과 테이블을 Java App.을 이용해서 $IPIMS_{DB}$ 점검결과 테이블로 전송하는 프로토콜이다. 점검결과 테이블 전송 프로토콜은 월, 컴퓨터 이름, 사번 등으로 실행한다. 점검결과 테이블 전송 모듈의 프로토콜 및 실행화면은 Fig. 6와 같다.

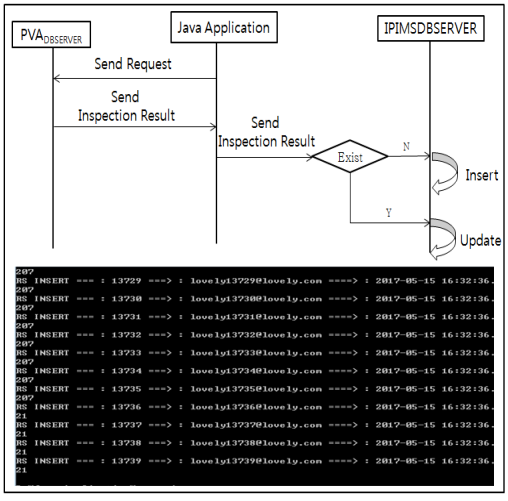

Fig. 6. Inspection result send protocol and execution screen

세 번째, $IPIMS_{DB}$ 점검결과 테이블로 전송된 개인별 개인정보 보유 현황 점검결과를 조회하는 프로토콜이다. 정보보안 관리자는 전체, 소속별 개인정보 보유 현황을 조회하지만, 정보보안 담당자는 해당 부서의 인원에 대한 개인정보 보유 현황만 조회한다. 개인별 개인정보 보유 현황 점검결과를 조회하는 프로토콜 및 실행화면은 Fig. 7과 같다.

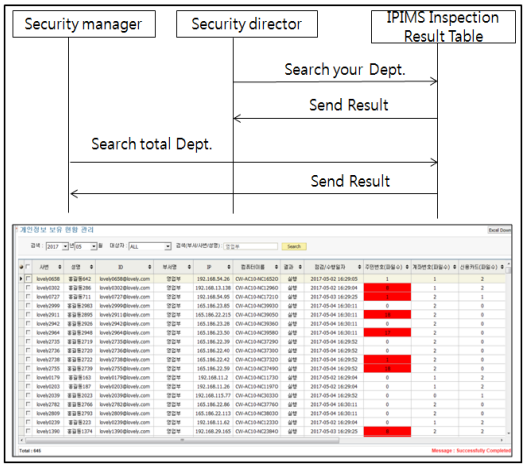

Fig. 7. Personal information retention management protocol and execution screen

네 번째, $IPIMS_{DB}$ 점검결과 테이블로 전송된 개인별 개인정보 보유 현황 점검결과를 부서별로 수치화해서 조회하는 프로토콜이다. 정보보안 관리자와 정보보안 담당자는 부서별로 개인정보 보유 현황을 조회한다. 부서별 개인정보 보유 현황을 조회하는 프로토콜 및 실행화면은 Fig. 8과 같다.

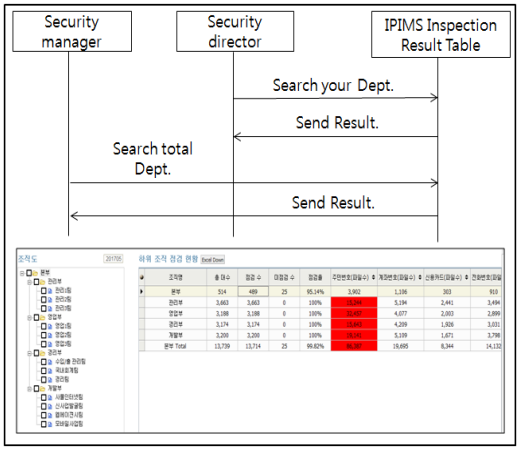

Fig. 8. Personal information retention management protocol and execution screen

다섯 번째, 부서별 개인정보 보유 현황에서 점검자 수

와 미점검자 수를 더블클릭했을 경우 부서원들의 점검여부와 개인정보 보유 현황을 자세히 조회한다. 점검자와 미점검자 조회 프로토콜 및 실행화면은 Fig. 9와 같다.

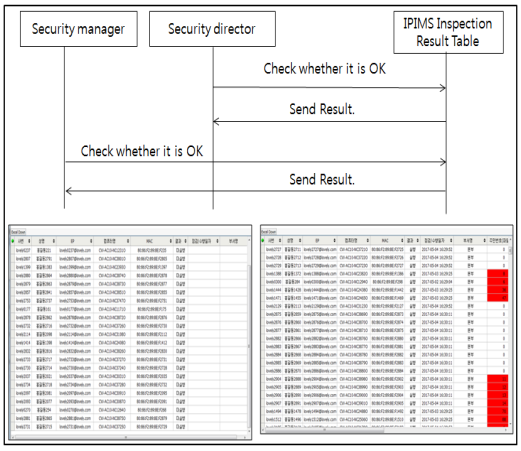

Fig. 9. Inspector status protocol and execution screen by department

4. 분석

본 논문에서 제안한 IPIMS의 분석은 보유한 개인정보 중 주민등록번호를 200건 이상 보유하고 있는 직원 상위 5명과 상위 4개의 부서를 대상으로 분석한다.

4.1 분석 환경

IPIMS의 분석 대상은 사무직·생산직·협력업체까지 포함한 직원 수가 12,000명이 넘는 L사(대기업)를 선정했다. L사를 선정한 이유는 다양한 개별 보안시스템과 개인정보 보유 현황 관리시스템이 구축되어 있기 때문이다. IPIMS의 분석을 위해 사용된 점검결과 데이터는 2017년 5월 1일부터 31일까지 한 달간의 데이터이다.

L사에서 한 달간 PVA 시스템에서 IPIMS로 전송된 점검결과 데이터 건수는 13,739건이며, 개인정보 때문에 부서 및 직원 이름을 익명으로 사용했다. L사에 근무하는 12,000명 중에서 한 달간 PVA 시스템을 실행하지 않은 직원은 25명이며, 직원 수보다 점검결과 데이터가 많은 이유는 한 직원 이름으로 생산라인이나 회의실 컴퓨터를 등록해 놓았기 때문이다.

PVA 점검결과 비율은 99.9(25/13,739)%이고 주민등록번호를 200건 이상 보유하고 있는 인원은 54명이다. 주민등록번호 200건 이상을 보유한 직원들 중 상위 5명과 상위 4개의 부서를 분석대상으로 선정한 후, 개인정보 보유 최소화 및 최소화에 걸린 시간을 분석한다. 선정된 상위 5명과 4개 부서의 익명성을 보장하기 위해 사용자 A~E로, I~Ⅳ로 명명한다. 한 달간 PVA 시스템에서 IPIMS으로 전송된 점검결과 데이터의 분석 대상 수와 점검율 등은 Table 2와 같다.

Table 2. Analysis types and inspection rate

Analysis Types	Count
Inspect Target Data Count	13,739
User	12,000
Unchecked Count	25
Checked Count	13,714
Checked Rate	99.99%
More than 200	54
Target User	5
Target Dept.	4

4.2 분석 결과

직원들이 보유한 개인정보 중 주민등록번호, 계좌번호, 신용카드번호, 전화번호 보유 현황에 대해 분석한다. 정보보안 관리자는 특정 직원에게 직접 메일을 발송하는 One channel 방식을 이용해서 개인정보를 암호화 또는 삭제하도록 한다. 그리고 정보보안 관리자는 부서의 정보보안 담당자에게 메일을 발송하고 특정 직원에게 직접 메일을 발송하는 Two channel 방식을 이용해서 개인정보를 암호화 또는 삭제하도록 한다. 두 가지 방식을 적용해서 개인정보 보유 최소화 시간을 비교 분석한다.

본 논문에서 제안한 IPIMS을 이용해서 개인정보 중 주민등록번호를 200건 이상 보유한 상위 5명의 직원들을 선택하여 개인정보 보유 최소화에 걸린 시간을 분석한다. 분석기간 중에 직원들이 수집한 주민등록번호 전체 건수는 86,387건이고, 직원 1인당 보유하고 있는 주민등록번호는 평균 6.28건(86,387/13,739)이다. 그러나 상위 5명이 보유하고 있는 주민등록번호는 직원 1인당 주민등록번호 보유 건수의 40배다. 주민등록번호를 200건 이상 보유한 직원들 중 상위 5명은 Fig. 10과 같다.

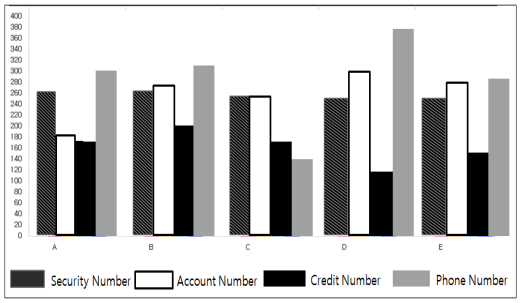

Fig. 10. Top 5 employees with more than 200 resident registration numbers

제안한 IPIMS을 이용해서 개인정보 중 주민등록번호를 많이 보유한 상위 4개 부서를 대상으로 분석한다. 분석기간 중에 직원들이 수집한 주민등록번호 전체 건수는 86,387건이고, 부서별(18개) 보유하고 있는 주민등록번호는 평균 4,799건(86,387/18)이다. 그러나 상위 4개의 부서가 보유하고 있는 주민등록번호는 I 부서는 1.07배, Ⅳ부서는 3.27배다. 개인정보 중 주민등록번호를 많이 보유한 상위 4개의 부서는 Fig. 11과 같다.

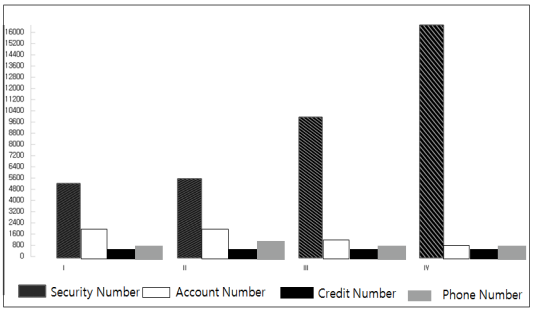

Fig. 11. Top 4 Dept. with a lot of resident registration numbers

IPIMS을 이용해서 개인정보 보유 현황을 분석한 결과 Ⅱ~Ⅳ 부서는 영업과 수·출입 업무를 담당하는 부서이다. 이와 같은 부서의 특징은 거래업체의 대표자와 담당자의 개인정보를 정보보안 관리자에게 개인정보 취급자 교육을 받은 후 보유한 경우이고, 개인정보 보유 상위 5명 중 직원 A~D가 소속된 부서이다. 그러나 I 부서의 직원 E인 경우는 사내시스템을 유지 보수하는 개발 업무를 맡고 있는 개발관련 부서의 소속 직원이다. 온라인을 통한 개인정보 유출 때문에 정보유출 통합모니터링 시스템에 악의적인 사용자로 등록하고 관리가 필요하다.

기존 PVA 시스템과 제안한 IPIMS의 분석 결과는 Table 3과 같다.

Table 3. Compare of PVA and IPIMS

	PVA	IPIMS
Personal Inspection Result	O	O
Dept. Inspection Result	X	O
Access Security manager	O	O
Access Security manager	X	O

5. 결론

PVA 시스템에서는 정보보안 관리자가 전체 직원들의 개인정보 보유 현황을 관리한다. 이러한 One channel 관리 방식으로 개인정보 보유 현황을 최소화하는 경우 많은 시간과 비용이 발생한다. 그러나 IPIMS에서는 악의적인 사용자에 의한 개인정보 유출을 최소화하기 위해 PVA 점검대상과 점검결과를 30분 간격으로 수신한 후 기존 부서 정보와 연계하여 정보보안 관리자와 정보보안 담당자가 부서별 개인정보 보유 현황을 최소화되도록 개선하였다. 제안한 방식은 기존 개인정보 보유 현황 관리 시스템에 접근할 수 없었던 정보보안 담당자에게 권한을 부여하여 부서의 개인정보 보유 현황을 관리하고, 정보보안 관리자와 Two channel 방식으로 개인정보 보유를 최소화했다.

Acknowledgments

본 논문은 2017학년도 동명대학교 교내학술연구비 지원에 의하여 연구되었음.

REFERENCES

[1] H. C. Kim, “A Study on the Destruction of the Personal Information,” *The Journal of Comparative Private Law*, Vol. 21, No. 3, pp. 1109-1138, 2014.

[2] D. J. Cho, “The development of IT technology and protection of personal information,” *KOREAN LEGAL CENTER*, The Justice 158-1, pp. 49-58, 2017.

[3] S. B. Kim and B. M. Chang, “Design and Implementation of Privacy Impact Assessment Information System,” *Journal of Korean Institute of Information Technology*, Vol. 13, No. 6, pp. 87-104, 2015. DOI : 10.14801/jkiit.2015.13.6.87

[4] D. K. Lee and J. I. Lim, “Forecast System for Security Incidents,” *Journal of The Institute of Electronics and Information Engineers*, Vol. 53, No. 6, pp. 69-79, 2016.
DOI : 10.5573/ieie.2016.53.6.069

[5] S. H. Bae, J. S. Shin, S. H. Chun and H. S. Chung, “A Study on Improving the Privacy for personal information collected for statistical processing,” *Journal of Convergence Society for SMB*, Vol. 6, No. 2, pp. 25-30, Jun. 2016.
DOI : 10.22156/cs4smb.2016.6.2.025

[6] H. J. Mun, Y. C. Hwang and H. Y Kim, “Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey,” *Journal of Convergence Society for SMB*, Vol. 5, No. 2, pp. 1-6, Jun. 2015.

[7] H. T. Chae and S. J. Lee, “Security Policy Proposals through PC Security Solution Log Analysis,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 24, No. 5, pp. 961-968, Oct. 2014.
DOI : 10.13089/jkiisc.2014.24.5.961

[8] S. K. Cho and M. S. Jun, “Privacy Leakage Monitoring System Design for Privacy Protection,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 22, No. 1, pp. 99-106, Feb. 2012.

[9] B. J. Jeon, D. B. Yoon and S. S. Shin, “Improved Integrated Monitoring System Design and Construction,” *Journal of Convergence for Information Technology*, Vol. 7, No. 1, pp. 25-33, Jan. 2017.
DOI : 10.22156/cs4smb.2017.7.1.025

[10] B. J. Jeon, D. B. Yoon and S. S. Shin, “Integrated Monitoring System using Log Data,” *Journal of Convergence for Information Technology*, Vol. 7, No. 1, pp. 35-42, Jan. 2017.
DOI : 10,22156/CS4SMB.2017.7.1..035

[11] M. S. Kim and D. W. Kang, “Information leakage prevention system design for small business,” 2008.

[12] J. Y. Lee and S. Y. Kang, “Design and Verification of the Integrated Log Analysis System for Enterprise Information Security,” *Journal of Digital Contents Society*, Vol. 9, No. 3, pp. 491-498, Sep. 2008.

[13] K. S. Yu, S. H. Im and H. B. Kim, “Technology trend and development direction of integrated log management system,” *Korea Institute Of Information Security And Cryptology*, Vol. 23, No. 6, pp. 90-99, 2013.

[14] B. G. Seo and D. H. Park, “Development on Early Warning System about Technology Leakage of Small and Medium Enterprises,” *Journal of Intelligence and Information Systems*, Vol. 23, No. 1, pp. 143-159, Mar. 2017.

[15] S. J. Park and J. I. Llim, “A study on the development of SRI(Security Risk Indicator)-based monitoring system to prevent the leakage of personally identifiable information,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 22, No. 3, pp. 637-644, Jun. 2012.

저 자 소 개

전 병 진(Byung-Jin Jeon) [정회원]

- 1998년 2월 : 동명전문대학 전산학과 전문학사
- 2004년 2월 : 동서사이버대학교 전산학과 공학사
- 2017년 2월 : 동명대학교 정보보호학과 공학석사
- 2017년 3월 ~ 현재 : 동명대학교 정보보호학과 박사과정

<관심분야> : 정보통신, Iot, 물리보안, 안드로이드

신 승 수(Seung-Soo Shin) [정회원]

- 2001년 2월 : 충북대학교 수학과 이학박사
- 2004년 8월 : 충북대학교 컴퓨터공학과 공학박사
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야> : 암호프로토콜, 무선 PKI, 네트워크 보안, IoT, 빅 데이터

이 준 연(Jun-Yeon Lee) [정회원]

- 1990년 8월 : 중앙대학교 컴퓨터공학과 공학사
- 1992년 8월 : 중앙대학교 컴퓨터공학과 공학석사
- 2000년 2월 : 중앙대학교 컴퓨터공학과 공학박사
- 2000년 3월 ~ 현재 : 동명대학교 미디어공학과 교수

<관심분야> : 클라우드 컴퓨팅, IoT, IaaS, ITS