효과적인 개인정보 유출 방지를 위한 개인정보보호통합시스템 설계

정수호*, 류근호*
*충북대학교 컴퓨터과학과
e-mail:jsh8562@gmail.com

Designing an Integrated Privacy System for Effective Privacy Protection

Soo Ho Jeong*, Keun Ho Ryu*
*Dept of Computer Science, Chungbuk National University

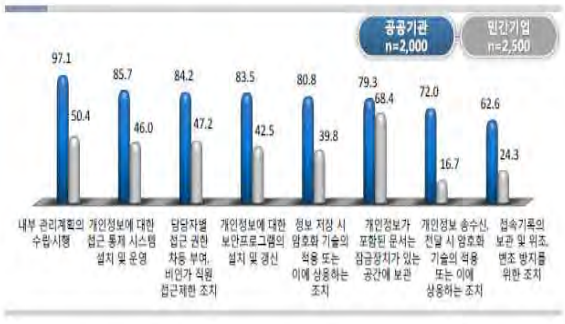
요 약

오늘날 빅데이터, AI, IoT 등 IT기술이 발달함에 따라 기업들은 다양하고 수많은 정보를 수집 축적하고 있다. 특히, 개인정보에 대해 습득 및 취급이 쉬워져 기업들은 대량의 개인정보를 보유하고 있다. 이로 인해, 해킹, 내·외부 직원의 고의 및 실수 등으로 발생하는 개인정보 유출 사고는 우리 사회에 큰 문제이다. 정부 및 유관기관은 개인정보보호법, 개인정보 안전성 확보조치기준 등 법령을 마련해 개인정보를 안전하게 처리하기 위한 최소한의 가이드라인을 제시하여 공공기관 및 민간기업이 개인정보를 안전하게 처리하도록 유도하고 있다. 하지만, 이러한 노력에도 불구하고 개인정보 유출 사고는 해마다 빈번하게 일어난다. 본 논문은 이기종 개인정보보호 솔루션의 유기적인 통합 방안과 운영방안 등을 고안하여 개인정보보호통합시스템 설계를 통해 효과적인 개인정보 유출 사고 방지에 이바지하고자 한다.

키워드: 개인정보, 개인정보보호, 개인정보 유출 사고, 개인정보보호 솔루션, 정보보호, 정보보안

1. 서론

오늘날 제4차 산업혁명은 정보통신 기술(ICT)과 다른 영역들의 융합으로 실현되고 있다. IoT, 빅데이터, 머신러닝을 이용한 AI기술의 발달 등이 제4차 산업혁명에 모습이다. 기업들은 다양하고 수많은 정보가 수집 및 축적함으로써 자연스럽게 무분별한 개인정보 습득 및 취급이 가능해지고 있다. 부작용으로 매년 일어나고 있는 개인정보 유출 사고는 우리 사회에 큰 문제이다. 우리나라는 개인정보를 보호하기 위해「개인정보보호법」을 제정하는 등 많은 노력을 해왔다[8][9]. 공공기관, 사기업 등 각 기관은 법령을 준수하기 위해 개인정보보호 솔루션을 도입·운영하고 있다. (그림1)은 2016년에 한국인터넷진흥원에서 시행한「2016년 개인정보보호 실태조사」에서 도출된 개인정보를 안전하게 관리를 위한 기술적 조치 현황이다[1].



(그림 1) 개인정보의 안전한 관리를 위한 조치 (단위: %)

하지만, 이런 노력에도 불구하고 개인정보 유출 사고는 매년 빈번하게 일어난다. 통합 관리하여 효과적으로 개인정보를 보호할 수 있는 개인정보보호통합시스템을 설계하여 제안하고자 한다.

본 논문은 1장 서론, 2장 관련연구, 3장 개인정보통합시스템 설계, 4장 평가 및 결론으로 구성하여 서술하고자 한다.

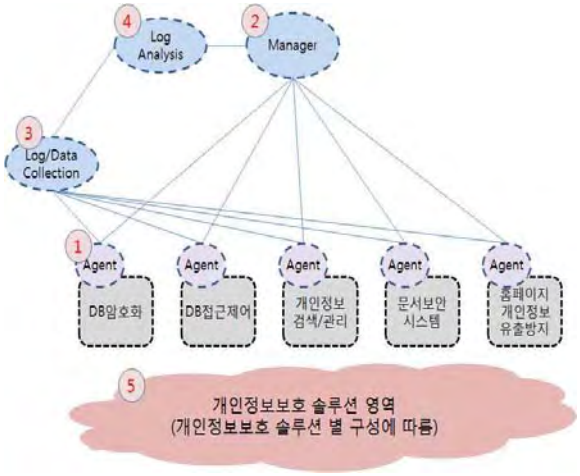
2. 관련 연구

DB로부터의 개인정보 유출 방지를 위한 기술요소로 DB접근제어는 권한에 따라 DB 접근을 허용 및 차단할 수 있다. DB암호화는 전체, 테이블, 칼럼 단위 암호화를 통해 개인정보 등 기밀정보를 암호화하여 보호한다[2].

PC에 저장된 개인정보를 포함한 전자문서의 유출에 의한 개인정보 유출 방지를 위해선 문서보안관리(DRM)기술을 이용한다. DRM은 PC에서 전자문서 생성 및 수정하여 저장하거나, 또는 업무시스템에서 문서를 다운로드 받아 PC에 저장하는 시점에 암호화한다[3]. 이는 개인정보가 포함된 문서를 암호화하여 문서가 유출되더라도 해커 등 제3자가 열람하는 것을 막을 수 있다. PC 내 개인정보 현황 관리를 위해 개인정보 검색 솔루션을 이용한다. 일반적으로 사용자의 PC에 클라이언트 검색 솔루션이 설치되어 PC 내의 개인정보를 검색하고 사용자에게 알려 준다. 이때 사용자는 검색된 개인정보를 파기 또는 DRM과 연동하여 암호화 등 보안 조치를 할 수 있다[4].

기존 연구에서는 DB, PC, 웹페이지 등 개인정보가 처리되는 요소별로 개인정보 유출 방지를 위하여 각각의 요소에 맞는 개인정보보호 솔루션들을 제안하고 있으나 관리 페이지 또는 프로그램이 분산되어 있어 제한된 인력으로 정책 등을 관리하는 데 한계가 있다. 이에, 본 연구에서는 이기종 간의 개인정보보호 솔루션을 연동하여 통합관리 할 수 있는 개인정보보호통합시스템을 설계하여 제안하고자 한다.

3. 개인정보보호통합시스템 설계



(그림 2) 개인정보보호통합시스템 구성도

① Agent: 개인정보보호통합시스템의 Manager과 연동하여 개인정보보호 솔루션 정책 등 관리
② Manager: 개인정보보호 솔루션의 정책 데이터 연동, 모니터링 출력, 소명요청 등 관리
③ Log/Data Collection: 개인정보보호 솔루션에서 생성되는 로그와 데이터를 수집
④ Log Analysis: 로그 및 데이터 분석하여 개인정보 유출 위험 탐지
⑤ 개인정보보호 솔루션 영역: 실제 문서암호화 등 개인정보 유출 방지 행위 수행

본 논문에서 제시하는 개인정보보호통합시스템은 ⑤ 영역과 같이 후단에 개인정보보호 솔루션 영역을 설계하여 각 개인정보보호 솔루션 고유의 구성을 유지할 수 있다.

Agent와 Manager간의 TCP/IP 프로토콜 통신으로 개인정보보호 솔루션을 제어할 수 있다. 또한, 개인정보보호 솔루션의 대용량 로그 수집에 의한 병목현상 발생 등을 대비해 수집과 분석을 각각 Log/Data Collection, Log Analysis로 나누어 설계했다. Log/Data Collection은 '메시지 필터링', '로그 분류', '로그 길이 통일' 3단계 전처리 과정을 통해 다양한 개인정보솔루션 로그를 정규화한다. 수집된 로그는 Log Analysis를 이용하여 '개인정보 유형별 중요도', '개인정보건수', '행위자', '유출 시고 라이프사이클 구간' 4가지로 나누어 위험도 유형별 평가 내역에 따라 점수를 산정하여 개인정보 유출 사고 위험 행위여부 판단 및 심각도 등을 탐지한다.

4. 평가 및 결론

시스템에 대한 평가는 우리나라에서 발생한 주요 개인정보 유출 사고인 '2014년 카드 3사 개인정보 유출 사고[6]' 당시에 개인정보보호통합시스템을 운영 중이라 가정하고 개인정보 유출 사고를 효과적으로 방지할 수 있는지를 증명하여 수행하고자 한다. 2014년에 발생한 카드 3사 개인정보 유출 사고는 외부직원이 제공받은 테스트 DB에서 1억4천 건의 고객정보를 USB에 담아 유출한 사건이다.

만약 개인정보보호통합시스템을 운영했다면 외부직원이 암호화된 DB 조회하는 행위와 PC내 개인정보 보유 현황, 암·복호화 등 개인정보 처리 내역을 통합 화면에서 볼 수 있어 외부직원의 불법적인 행위를 탐지하는데 용이했을 것이다. 또한, DB에서 개인정보를 조회하여 PC에 문서로 저장하는 순간 개인정보 문서로 탐지되고 개인정보보호담당자와 외부직원에게 알림을 전송하여 암호화를 강제할 수 있다. 외부직원이 해당 파일을 복호화를 하면 복호화 내역이 모니터링 되어 제어 가능하며 USB로 옮길 때 매체제어에 탐지되어 외부직원에게 소명을 요청해 불법행위를 억제할 수 있다. 결국, 개인정보를 유출하였을 지라도 개인정보보호통합시스템은 개인정보 처리 전 구간을 모니터링하고 있기 때문에 신속한 추적과 대응이 가능하다.

향후 연구로는 본 논문에서 제안한 개인정보보호통합시스템의 주요기능을 도출하여 설계하고 시스템 취약점에 대한 연구를 해야 할 것이다.

참고문헌

[1] 한국인터넷진흥원. "2016년 개인정보보호 실태조사". 행정자치부·개인정보보호위원회. 2016
[2] 윤선희. "안정적인 DB보안 시스템 구축을 위한 보안 기술요소 분석에 관한 연구". 한국컴퓨터정보학회논문지. pp.143-152. 2014
[3] 문진규. "내부 정보 유출 발지를 위한 DRM 적용 방법 설계". 한국정보과학회 학술발표논문집. pp.7-10. 2007
[4] 강구형. "전자정부하에서 각 행정기관 홈페이지의 개인정보 노출 방지에 대한 연구(석사)". 한남대학교. 2007
[5] 카드사 고객정보 1억400만건 유출… 사상 최대. http://www.sisain.co.kr/news/articleView.html?idxno=19063
[6] 박장수, 이임영. "정보보호:단일 정보유출 시나리오를 이용한 개별 보안솔루션 로그 분석 방법" 정보처리학회논문지. pp.65-72. 2015
[7] 최종욱, 이용진, 박주미. "DLP방식의 문제점 극복을 위한 E-DRM 방식의 개인정보 보호 기술". 정보보호학회논문지, pp.1103-1113. 2012
[8] 행정안전부. "2016년 개인정보보호법령 및 지침·고시 해설". 행정안전부. pp.10-12. 2016
[9] 행정안전부. "개인정보 안전성 확보조치 기준 해설서". 행정안전부. pp.1-91. 2017