개인정보 유출방지 프레임워크에 관한 연구

A Study on Privacy Framework for Prevention Leakage

이 야 리
(주)소만사

Lee Yari
Somansa Co. Ltd.

요약

현대 사회는 정보화에 따른 혜택과 더불어 부작용 현상으로 개인정보의 유출 사고로 사회적 불안감 및 관심을 증가시키고 있다. 우리나라 「개인정보보호법」은 공공, 민간 부문의 모든 개인정보 처리자에게 공통으로 적용되고 전자문서와 수기문서에도 적용된다. 그러나 업무특성에 따라 여러 곳에 다양한 형태로 산재되어 있는 개인정보 관리는 쉽지 않으며 정보 유출에 대한 우려 또한 크다고 볼 수 있다. 따라서 본 연구에서는 체계적인 개인정보 보호 관리를 통해 사전에 정보 유출을 방지할 수 있는 개인정보 유출방지 프레임워크를 제안하였다.

I. 서론

최근 3년간 카드 3사, 홈플러스, 인터파크 사고에 이르기까지 대규모 개인정보 유출 사고가 발생하였다. 우리나라 「개인정보보호법」은 공공, 민간 부문의 모든 개인정보 처리자에게 공통으로 적용되고 전자문서뿐 아니라 수기문서에도 적용된다[1]. 그러나 실제 일반 업무 담당자들의 컴퓨터, 각 기관에 전자문서나 수기문서 형태로 다양하게 수집, 활용, 보관되어 있는 관리 대상 정보는 여러 곳에 산재되어 개인정보 보호 관리측면에는 어려움이 따를 수밖에 없으므로 유출에 대한 우려 또한 크다고 볼 수 있다[2]. 따라서 본 연구에서는 개인정보 유출방지를 사전에 통제할 수 있는 개인정보 보호 관리의 일환으로 개인정보 자산보유 현황, 개인정보 과다조회 및 접속기록관리, 개인정보 외부공유 유출통제 및 개인정보 통합관제 체계로 구성된 개인정보 유출방지 프레임워크를 제안하였다.

Ⅱ. 개인정보 유출방지 체계 사례

개인정보 유출방지 체계를 구축하여 운영하고 있는 OO기관은 개인정보 보호를 위해 엔드포인트(Endpoint), 네트워크(Network) 영역에 개인정보보호 솔루션을 도입하여 운영하고 있으며, 개인정보 취급자에 대한 개인정보 유출을 사전 예방[4]하기 위한 활동을 하고 있다. 다음 표 1은 개인정보보호를 위한 솔루션 운영 현황이다.

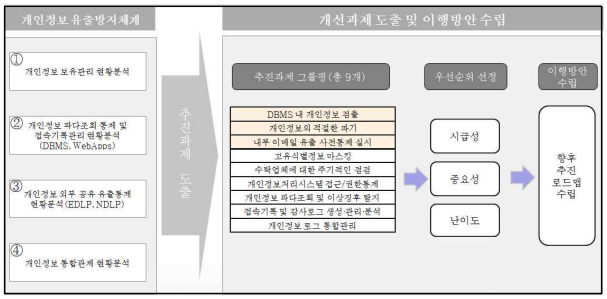
표 1. 개인정보보호 솔루션 운영 현황

NO	솔루션 분류	설치 위치
1	방화벽, 웹방화벽, 침입차단(IPS)	공개망네트워크 (사용자와 웹서버사이)
2	웹사이트 개인정보 노출 통제	네트워크 혹은 독립서버 (크롤링방식)
3	웹서버취약점점검툴, 서버보안 솔루션, 웹쉘솔루션	웹서버 외
4	Network DLP(Web DLP)	네트워크
5	EndPoint DLP/개인정보파기/ 출력물보안/DRM/ NAC/ PC보안	EndPoint(PC, 모바일단말)
6	망분리	Endpoint(PC)
7	세이프브라우징 (SAFE-BROWSING):유해사이트 차단 및 악성코드 배포사이트 차단, APT차단솔루션	네트워크(내부 사용자와 인터넷 사이)
8	바이러스 백신	EndPoint(PC) 및 게이트웨이 서버
9	DB 암호화 솔루션	네트워크(WAS-DB 구간)
10	Server DLP	서버팜
11	DB 접근통제	네트워크(PC-DB구간)
12	WAS 과다조회 통제	네트워크(WAS –DB 구간)

본 사례의 엔드포인트-네트워크간 운영되고 있는 기술적 보호조치에 대한 효과[3]는 웹상에 노출된 개인정보 페이지 분석, 유해사이트 및 악성코드 · 바이러스 차단, PC와 모바일단말에 저장된 개인정보 파일에 대한 검출, 삭제, 암호화 보관, 키보드 후킹 방지, USB와 출력물을 통해서 개인정보 유출 방지, 무선 통신에 대한 인증과 접속통제, 개인정보 암호화 적용, 서버 내 개인정보 검출 및 암호화(파일, DB), DBMS에 대한 사용자별 접근통제, 개인정보 처리시스템 접속이력 로깅 및 분석 등을 기대할 수 있다.

Ⅲ. 개인정보 유출방지 프레임워크

개인정보 유출방지 프레임워크 구성은 그림 1과 같이 먼저, 개인정보 관리 현황에 대한 분석을 통해 개선사항을 도출하고 도출된 과제를 시급성, 중요성, 난이도의 3가지 측면에서 우선순위를 선정함으로써 향후 이행해야 할 방안을 수립한다.



▶▶ 그림 1. 개인정보 유출방지 프레임워크 구성도

1. 과제 분류 및 우선순위 선정기준

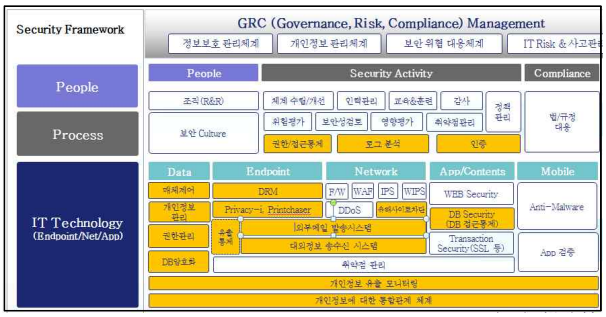
개인정보 자산보유 현황, 개인정보 과다조회 및 접속기록관리, 개인정보 외부공유 유출통제 및 개인정보 통합관제 체계 총 4가지 영역에 대한 분석 결과 도출된 개선방안에 대해 조직의 정책 방향 영역(Strategy), 조직의 구성 및 R&R 정의 영역(Structure), 프로세스 수립 영역(Process), 임직원의 의식 및 행동 변화 영역(People), 기술 통제 활동 영역(Technology) 관점에서 과제를 분류하고 시급성(법위반 사항 기준 3단계), 중요성(위험감소 효과 기준 3단계), 난이도(구현의 용이성 기준 3단계)에 대한 우선순위를 선정하였다(그림 2 참조).

우선순위					추진과제 그룹명	과제영역
NO	시급성	중요도	난이도	합계		
1	3	3	3	9	DBMS 내 주기적인 개인정보 검출 및 암호화	Technology
2	3	3	3	9	내부 이메일 전송에 대한 유출 사전통제 실시	Technology
3	3	3	3	9	보유연한이 경과한 PC 내 개인정보의 적절한 파기	Technology
4	3	2	3	8	고유식별정보 마스킹	Technology
5	3	3	2	8	수탁업체에 대한 주기적인 점검	Process
6	3	3	1	7	개인정보처리시스템 접근/권한 통제 강화	Technology
7	3	3	1	7	접속기록 및 감사로그 생성·관리·분석	Technology
8	3	3	1	7	개인정보 과다조회 및 이상징후 탐지	Technology Structure
9	3	3	1	7	개인정보 로그 통합관리	Technology Structure

▶▶ 그림 2. 개선과제별 우선순위

개인정보 자산보유 현황, 개인정보 과다조회 및 접속기록관리, 개인정보 외부공유 유출통제 및 개인정보 통합관제 체계 총 4가지 영역에 대한 분석 결과로 과제를 분류하고 우선순위를 선정하였다.

최종적으로 그림 3에서 개인정보 유출방지 체계 개선을 위해 GRC(Governance, Risk, Compliance) 측면의 관리체계를 내재화하여 이행하는 방안을 제안하였다.



▶▶ 그림 3. 개인정보 유출방지 프레임워크

■ 참 고 문 헌 ■

[1] 행정자치부, “개인정보 보호 실태점검”
[2] 정영철, “사회복지시설 개인정보 보호 관리현황과 과제”, 한국보건사회연구원 보건복지포럼, 제242권, 제4호, pp. 57-68, 2016.
[3] 최일훈, “개인정보보호와 DLP 최신 기술동향”, G-Privacy 2016, 2016.
[4] 이동근, 임종인, “보안사고 예보시스템”, 전자공학회논문지 제53권 제6호, 2016.