개인정보 영향평가 사례 연구
-K병원의 영향평가 사례를 중심으로-

전동진*, 정진홍**

A case study of Privacy Impact Assessment
-Focus on K hospital Privacy impact assessment case-

Dong-Jin Jeon*, Jin-Hong Jeong**

요 약 개인정보보호법이 새로 제정이 되어 기업 및 기관에서 이에 대한 준비와 대책 마련이 활발히 전개되고 있다. 개인정보를 취급하는 정보시스템에 대하여 개인정보 침해의 위협을 사전에 예방 및 점검을 수행하는 개인정보영향평가를 K병원의 분석 사례를 통해 연구하였다. 결론적으로 K병원의 개인정보 영향평가 분석을 수행한 결과 평가영역별로는 대상기관관리체계는 79.0, 대상시스템의 보호수준은 97.9, 개인정보처리단계의 결과는 67.4이고 CCTV는 90.0으로 나타났다. 개인정보보호수준이 가장 낮은 항목은 개인정보생명주기관리 항목의 저장 및 보유단계 50.0, 이용 및 제공 64.1 및 파기 단계 66.7로 나타났다. 위험도 분석결과 고위험도 항목은 개인정보처리구역 항목 11.0과 개인정보생명주기 영역의 저장 및 보유단계 항목이12.5, 파기단계 항목이 13.0으로 높은 수치가 나왔다. 종합적으로 보면 고위험도이면서 저보호수준인 항목은 저장 및 보유단계와 파기단계로 파악이 되었다.

주제어 : 개인정보보호법, 개인정보영향평가, 위험도분석, K병원, 고위험도

Abstract Recently, many corporations and public institutions are busy preparing and providing measures in dealing with new privacy information law. This study reviews privacy impact assessments in order to perform preventing and diagnosis against potential threats focus on the K-hospital case. The quality of protection in K-hospital shows that the corporations itself is 79.0, the system is 97.0, the life cycle of the privacy is 67.4 and CCTV is 90.0. The lowest levels are saving and keeping 50.0, usage and offer 64.1 and destruction 66.7 among the life cycle of the privacy. The result of risk analysis shows that the highest levels are controlling for privacy 11.0, saving and keeping 12.5 and destruction 13.0. From the result, dangerous duplications are saving and keeping and destructions.

Key Words : Privacy information protection law, Privacy impact assessment, Risk analysis, K-hospital, High risk

1. 서론

정보기술의 발전과 이를 활용한 비즈니스 환경의 변화는 개인과 기업 모두에게 편의성과 신속성, 가용성과 효율성 등 다양한 이익을 제공한다. 이러한 정보통신 기술의 혁신적인 발전으로 인터넷을 이용한 기업 활동 및 상거래의 수요가 급격히 늘어나면서 기업들의 개인정보 수집 및 유통이 가능하게 되었다.

또한 기업들이 취급하는 개인정보가 다양화되고 활용범위가 증가함에 따라 기존의 한정된 부분의 기밀정보 보호 중심의 보호체계로는 전사적 차원으로 활용되고 있는 개인 정보를 보호하는 데 어려움이 발생하고 있다. 이러한 기존의 기술적, 관리적, 물리적인 보안조치와 더불어 운영 중인 개인정보 처리시스템에 대해 보호조치가 얼마나 잘 이루어지고 있는지 보호수준을 진단하고 법적

*서울과학종합대학원 경영학박사 수료, 제1저자 Email: ceo@koripo.com
**서울과학종합대학원 산업정보대학원장, 교신저자 Email: jhjeong@assist.ac.kr
논문접수: 2012년 7월 24일, 1차 수정을 거쳐, 심사완료: 2012년 8월 31일

인 규정을 준수하고 있는지 점검하는 개인정보영향에 대한 평가를 각 기관이나 기업에서 수행하는 경우가 많아지고 있다.

개인정보영향평가는 정부에서 2005년 '개인정보 영향평가 수행지침'을 마련하여 민간 기업이 자율적으로 개인정보 관련 시스템을 평가하고 개선할 수 있도록 구체적인 수행 절차 및 방법을 보급하였고, 많은 기업에서 개인정보영향평가를 수행하였다. 정부에서 제공한 개인정보 영향평가 수행지침은 공공, 민간, 통신, 금융 등 모든 분야에서 공통으로 적용할 수 있는 평가 기준 및 항목을 분류하여 개인정보의 영향을 사전에 예방하여 최소화하는 방안을 제시하였다[6].

이와 같은 추세에 따라 선진국은 이미 미국, 캐나다, 뉴질랜드 등 여러 나라에서 개인정보영향평가 제도를 도입하여 운영하고 있으며, 우리나라도 그 동안 법적근거 없이 행정안전부와 한국인터넷진흥원에서 시범적으로 개인정보영향평가를 시행하다가 마침내 2010년 3월 29일에 개인정보영향평가제도를 도입하는 "개인정보보호법"이 제정되어 개인정보 영향평가를 실시하는 법적근거를 갖게 되었다[8].

이 논문은 개인정보영향평가를 K병원의 사례로 하여 구체적인 개인정보영향평가 방법론에 초점을 두었다. 제2장에서는 이론적인 배경으로서 개인정보영향평가의 전반적인 정의 및 개요와 구체적인 개인정보의 영향평가의 영역과 항목에 대해서 다룬다.

제 3장은 연구방법으로서 새로 제정된 개인정보보호법의 개인정보영향평가 관련 조항과 행정안전부, 한국인터넷진흥원에서 제공한 개인정보 영향평가 수행안내서의 평가 영역과 평가 항목을 바탕으로 각 항목별 보안수준평가, 개인정보생명주기에 따른 개인정보 흐름도 분석, 위험도 분석, 개선방안을 도출하여 취약점을 사전에 예방하여 침해에 대비하는 시스템에 대해 논의하였다.

제 4장은 구체적으로 영향평가의 결과를 근거로 각 항목별 사항에 대하여 검토하고 미흡한 사항에 대하여 대책을 논의하였으며 특히 위험도가 큰 사항에 대해서는 개선방안에 우선순위를 두어서 방안에 대하여 대책을 마련하여 개인정보의 유출가능성을 최대한 차단하는 방안을 마련하였다.

2. 이론적 배경

2.1 개인정보영향평가의 정의

개인정보영향평가(PIA:Privacy Impact Assess ment)에 대한 정의는 선행 논문에서 많이 언급이 되었다. 개인정보영향평가란 정보시스템의 구축 및 운영으로 인해 이러한 개인의 민감한 프라이버시 정보에 미치는 영향을 예측하기 위한 분석기법 및 절차이다[7].

개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경시 동 시스템의 구축 • 운영 • 변경 등이 프라이버시에 미치는 영향(impact)에 대하여 사전에 조사 • 예측 • 검토하여 개선 방안을 도출하는 체계적인 절차를 말한다[16].

기존의 개인정보에 대한 보호제도는 프라이버시 침해가 발생되고 난 후에 그 원인을 분석해서 기술적인 대책을 강구하거나, 침해에 대한 법적, 행정적 조치를 위한 사후 구제적인 성격이었다면, 개인정보영향평가는 개인정보 침해피해에 대한 사전 예방적 수단의 성격이 강하다. 즉, 정보화 시스템 구축사업의 시작 단계에서부터 사전에 개인정보의 수집 및 활용으로 인해 개인의 프라이버시에 미치는 영향을 사전에 분석하고 이에 대한 적절한 대책을 마련하게 함으로써 침해사고가 발생할 가능성을 최소화하는 한편, 시스템 구축과정에서 또는 시스템 구축이 완료된 후에 개인정보 침해로 인해 기술적 보완조치를 하거나, 사업을 변경 또는 취소함에 따라 유발되는 비용을 방지할 수 있다[11].

개인정보영향평가는 정보화 사업이나 정보처리시스템에 한해 제한적으로 수행되는 것은 아니며, 정보화 사업이 아니더라도 개인정보를 수집하는 사업을 신규로 추진하거나, 기존 개인정보가 취급되는 업무에서 절차상 변경이 있는 경우에도 수행이 가능하다.

또한 우리나라는 개인정보보호법 제33조에 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 경우에는 개인정보영향평가를 실시하도록 규정하고 있으며, 구체적인 영향평가대상은 하위법령에 규정하고 있다.

구체적으로 개인정보보호법 시행령 제35조에 평가대상의 개인정보파일을 규정하고 있는데 첫째, 구축 · 운영 또는 변경하려는 개인정보파일로서 5만 명이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 둘째, 구축 · 운영하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축운영하고

있는 다른 개인정보파일과 연계하려는 경우로서 연계결과 50만 명이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일 셋째, 구축·운영 또는 변경하려는 개인정보파일로서 100만 명이상의 정보주체에 관한 개인정보파일 넷째, 개인정보 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 등으로 규정하고 있다.

즉 시스템의 구축·변경 및 운영 중인 환경에서 사전적 평가 수행을 통해 동 사업의 시행이 고객의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 그 영향을 줄이거나 없앨 수 있는 방안을 모색하는 것이다.

2.2 개인정보영향평가의 평가항목

표 1의 행안부 및 한국인터넷진흥원에서 제공한 개인정보영향평가 수행가이드의 평가영역 및 평가항목에 토대로 K병원의 개인정보 영향을 평가하였다.

평가항목은 기관이 개인정보보호를 위해 조치해야 하는 사항으로 총4개의 평가영역으로 구분되고 각 영역은 평가기관의 개인정보보호관리체계, 대상시스템의 개인정보보호관리체계, 개인정보처리단계별 보호, 특정 IT기술 및 활용 시 개인정보보호이고, 평가항목은 총 15개, 세부 조항 114개 로 구성되어있다.

〈표 1〉 개인정보영향평가 영역과 항목[12]

평가영역	평가항목
1. 대상기관 의개인정보보호 관리체계	1. 대상기관 개인정보보호조직 2. 개인정보보호 보호계획 3. 개인정보 처리방침 4. 개인정보 파일관리 5. 개인정보 위탁 및 제공시 안전조치 6. 개인정보 침해대응 7. 정보주체 권익보호 8. 개인정보처리구역보호
2.대상시스템의 개인정보관리	1. 대상시스템의 개인정보 관리 2. 대상시스템의 개인정보보호관리체계
3.개인정보 처리단계별 보호	1. 수집단계 2. 저장 보유단계 3. 이용 및 연계제공 단계 4. 파기단계
4. 특정 IT 기술 및 활용 시개인정보보호	1. CCTV활용 2. RFID활용 3. 바이오정보활용 4. 위치정보 활용

3. 연구 방법

K병원은 2012년 3월 한 달 간 개인정보처리의 주요시스템인 웹서버, MOCS(Midi cal Order Communi- cation system), PACS 등의 개인정보영향평가를 설문조사와 병행하여 탐색적 연구를 위한 인터뷰를 수행하였다. 개인정보시스템의 각 업무 담당자인 메디칼팀, 의료정보관리팀, 보안관리 담당자, 원무팀 등의 개인정보 처리 담당자와 4가지 평가영역의 114가지 중 RFID, 바이오활용, 위치정보 항목을 제외한 103가지 세부항목에 대하여 조사하였다.

3.1 개인정보 흐름도 분석

개인정보흐름도는 사업전체에 있어 개인정보의 흐름을 한 눈에 파악하여 평가항목의 취약성 분석과정에서 침해요인을 정확히 도출하는데 도움을 줄 수 있다.

3.2 개인정보보호 수준 분석

개인정보관리현황 진단 시 보안수준은 Y, P, N, N/A 등급으로 구분하여 진단하며, 평가 항목에 대하여 적용의 만족과 수행여부에 따라 표시된 부문에 점수를 표시하였다.

〈표 2〉 보안수준 표시 기호[12]

등급	내용	점수
이행 Y(Yes)	전반적으로 조치되어 있음(실제적으로 이행, 적용하고 있고 이에 대한 근거(문서)가 존재하는 경우	1
부분 이행 P(Partial)	부분적으로 조치되어 있음. 실제 이행, 적용하고 있으나 정확한 근거(문서)없이 인터뷰에 의하여 계획으로만 되어 있거나 이행, 적용여부의 확인이 어려운 경우	0.5
미이행 N(No)	해당 점검 항목에 대해 보호대책을 적용 안 됨, 이행 적용 계획도 없는 경우, 개인정보 침해가능성이 매우 높음	0
N/A	해당사항 없음	-

보안수준 산정 = (항목별 점수/항목별 합계) * 100

보안수준의 점수는 다섯 구간의 등급으로 분류하여 보안수준이 취약(0-50), 미흡(51-65), 보통(66-80), 양호(81-90), 안전(91-100)으로 등급을 부여한다.

3.3 위험도 분석

개선사항의 우선순위 선정을 위한 위험도 산정방법은 개인정보 취급업무를 자산으로 보고 업무 내의 개인정보의 조합수준에 따라 자산 가치를 산정하여 자산 가치, 침해요인발생가능성, 법적준거성을 조합하여 위험도를 평가하여 합산하는 방법을 적용할 수 있다.

자산가치가 높을수록 개인정보침해요인의 발생가능성이 높을수록 법률에 규정된 의무사항일 수록 개인정보 침해 위험도가 크다는 개념에서 생성한 위험도 산정방안이다.

〈표 3〉 개인정보 위험도 자산가치 수치[12]

조합수준	조합설명	자산가치	개인정보 영향도 설명	비고
P3 이상	개인을 식별할 수 있으며 악용할 경우 위험이 높은 정보(주민번호, 신용카드번호)	5	개인의 신분 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 매우 큰 정보	암호화 저장하고 화면에 표시할 경우 일부만 표시
P2+ P1		4	개인의 신분 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 높은 정보	
P2	개인을 식별 할 수 있으며, 악용할 경우 위험이 다소 낮은 정보(이름, 주소, 전화번호)	3	개인의 신분 과 신상정보에 대한 추정이 가능하며 노출 시 금액의 피해보상을 요구 받을 수 있는 수준	
P1	개인을 식별할 수 없으나, 개인을 식별할 수 있는 정보와 같이 노출 시 위험이 높은 정보(인종, 종교, 병역사항)	2	개인의 신분과 신상정보를 파악하기 어려우나 신상정보와 같이 노출 시 매우 민감한 정보	
G	정보가치가 낮은 정보	1	아무런 영향을 미치지 않는 수준	
S	서비스 관련 정보(예: 상담내용, 녹취내용, 위치정보, CCTV영상정보 등 등)	5	개인의 신분 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 매우 큰 정보	특정 업무 관련자에게만 열람 권한 부여

〈표 4〉 법적 준거성 가중치 부여 척도[12]

구분	법적준거성	중요도
높음	법적준수사항	1.5
낮음	법률외 요건	1

〈표 5〉 개인정보 침해요인 발생 가능성[12]

구분	발생가능정도	중요도
매우 높음	침해요인의 발생가능성이 높은 경우	3
높음	침해요인의 발생가능성이 그다지 높지 않은 경우	2
중간	침해요인의 발생가능성이 희박하다고 판단되는 경우	1
낮음	침해요인의 발생가능성이 없는 경우	0

〈표 6〉 개인정보 위험도 Matrix

법적준거성	상(1.5)			하(1.0)		
발생가능성 / 자산가치	상 (3)	중 (2)	하 (1)	상 (3)	중 (2)	하 (1)
최상(5)	14	11	8	11	9	7
상(4)	13	10	7	10	8	6
중(3)	12	9	6	9	7	5
하(2)	11	8	5	8	6	4
최하(1)	10	7	4	7	5	3

위험도 = 자산 가치 + (침해요인*법적준거성) + (취약성측면의 침해요인*법적준거성)
= 자산 가치(개인정보영향도) + (침해요인 발생가능성*법적준거성)*2[5]
위험도 산정 예: 자산가치(5) + [발생가능성(3)*법적준거성(1.5)]*2 = 14

3.4 개선방안 수립

위험도 산정 결과를 기반으로 자산에 대한 위험을 제거하거나 최소화하기 위한 개선방안을 도출한다. 개선방안을 수립하기위해 영향평가 주관부서, 시스템 및 네트워크 관리부서, 개발업체 등 평가와 관련된 전체 대상자의 의견을 수렴하여 우선순위 또는 단기, 중장기로 구분하여 도출한다. 도출된 개선방안을 기반으로 정보화사업 진행일정, 예산, 과제 성격 등을 고려하여 개선계획을 수립할 수 있다[11].

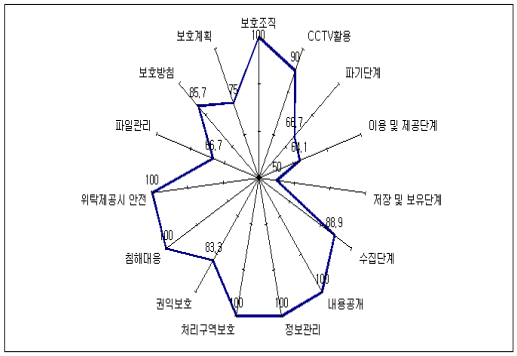
4. 개인정보 영향평가 결과

행정안전부의 개인정보영향평가수행가이드를 토대로 4가지 평가영역과 평가항목 15가지의 결과는 표 7과 같다. 전체 대상기관의 개인정보보호관리체계, 대상시스템의 개인정보 보호관리체계, 개인정보 라이프사이클상의 항목, 특정IT기술활용 분야를 파악하였다.

〈표 7〉 K병원 개인정보 영향평가 결과

평가 항목	항목수	Y	P	N	N/A
1. 개인정보보호조직	4	4	0	0	
2. 개인정보보호계획	2	1	1	0	
3. 개인정보보호방침	7	5	2	0	
4. 개인정보파일관리	6	4	0	2	
5.개인정보위탁 및 제공시 안전조치	2	2	0	0	
6. 개인정보침해대응	4	4	0	0	
7. 정보주체권익보호	3	2	1	0	
8. 개인정보처리구역보호	3	3	0	0	
9. 시스템의 개인정보관리	2	2	0	0	
10. 개인정보취급내용 공개	6	5	1	0	
11. 수집단계	12	6	3	3	
12. 저장 및 보유단계	4	2	0	2	
13. 이용 및 연계제공단계	40	19	7	11	3
14. 파기단계	3	1	2	0	
15. CCTV활용	5	4	0	0	

K병원의 평가항목 결과는 대상기관의 관리체계는 평균 79.0, 대상기관의 관리체계는 97.9, 개인정보처리 단계의 보호조치는 67.4이고 특정 IT기술인 CCTV활용분야는 90.0으로 나타났다.

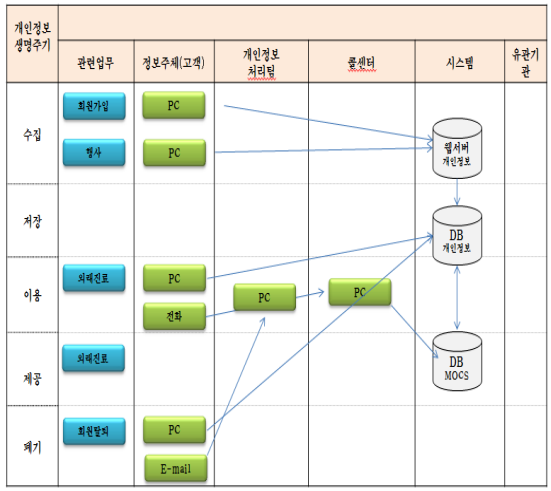


[그림 1] 전체 평가영역 보안수준 결과표

4.1 개인정보 흐름도 분석

4.1.1 홈페이지 개인정보시스템

웹사이트에서 개인정보를 수집하면 이 정보는 웹서버의 데이터베이스에 저장된다. 회원가입 외에 이벤트를 통한 개인정보 수집의 경우, 외부 영업마케팅의 수단이 아닌 병원 내부 행사진행 용도로 사용된다.



[그림 2] 홈페이지 개인정보 흐름도 분석

〈표 8〉 웹서버 개인정보 흐름표

항목	시스템	개인정보	담당자
수집	웹서버	성명, ID, 주민등록번호, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, I-PIN번호	업무담당자
저장	웹서버	성명, ID, 주민등록번호, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, I-PIN번호	업무담당자
이용	웹서버	성명, 주민등록번호, 주소, 전화번호, 휴대폰번호, 이메일	업무담당자
제공	웹서버 MOCS	성명, 주민등록번호, 주소, 전화번호, 휴대폰번호, 이메일	업무담당자
파기	웹서버	성명, ID, 주민등록번호, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, I-PIN번호	업무담당자

4.1.2 MOCS

MOCS는 K병원의 대표적인 시스템으로 의료시스템의 대부분을 제공한다. 웹서버에서 전달받은 진료예약정보 외에 오프라인에서 수행되는 진료접수, 진료예약, 수술동의 등 의료서비스를 위해 수집된 개인정보를 저장하며 관리한다. MOCS는 K병원이라는 의료기관 특성상 질병관리본부, 보건복지부 등에 또한 환자들의 개인정보를 제공한다.

4.2 개인정보 보호수준 분석

4.2.1 대상기관의 관리체계

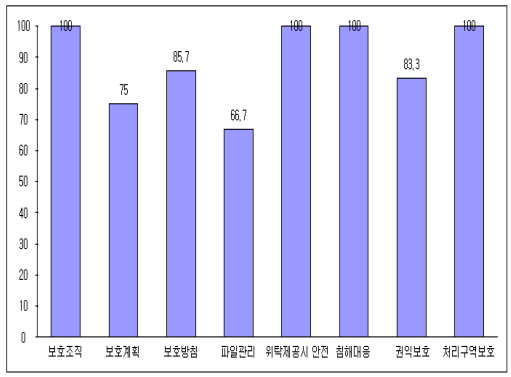
개인정보 관리체계에서는 조직, 교육, 개인정보보호방침, 개인정보 파일관리, 개인정보위탁 시 안전조치, 정보주체 권익 등에 관하여 분석하였다. 표 9의 개인정보 보호조직 관리체계는 조직에 대한 정책과 지침에 대한 부분으로 결과가 양호하게 나왔다. 그림 3에서 보듯이 개인정보 보호 계획과 개인정보보호 파일관리 항목은 다소 미흡한 결과가 나타났다.

의료기관 특성상 대부분의 모든 의사, 간호사가 개인정보를 취급하고 있는데 이와 관련하여 이들을 개인정보취급자로 분류하여 개인정보보호교육과 같은 별도 교육 및 통제 관리를 수행해야 한다.

개인정보파일의 생성이나 변경 시 행정안전부에 사항을 등록하고 파일대장을 작성해야 하는데 다소 미흡하였다. 이외 개인정보 파일의 경우 제3자와 연계하거나 제공하는 경우 '개인정보 목적 외 이용 등의 기록 및 관리 상태는 양호한 것으로 나타났다.

〈표 9〉 K병원 개인정보 영향평가 항목별 결과표 일부

보호조직	개인정보 보호책임자를 지정하고 있습니까?	Y
	개인정보 보호책임자에게 법률이 규정하는 업무를 부여하고 있습니까?	Y
	개인정보 취급자를 지정하고 있습니까?	Y
	개인정보 취급자에게 법률에서 규정하고 있는 업무를 부여하고 있습니까?	Y
보호계획	대상기관은 예산, 인력 등을 반영하여 개인정보보호 계획을 수립하고 있습니까?	P
	개인정보 보호 교육계획을 수립하여 시행하고 있습니까?	Y



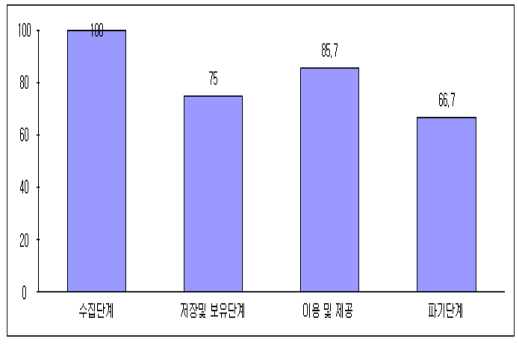
[그림 3] 대상기관 개인정보 관리체계

4.2.2 대상시스템의 개인정보보호관리 체계

대상시스템의 개인정보보호관리 체계 영역에서는 전체적으로 양호한 시스템관리상태로 파악되었다.

4.2.3 개인정보 생명주기 처리단계별 진단

그림 4에서 보면 전체적으로 파기단계와 저장 보유단계에서 보안수준이 미흡함을 나타내었다.



[그림 4] 개인정보 생명주기별 진단

■ 수집 단계

K병원은 개인정보를 수집함에 있어 진료서비스에 필요한 최소한의 정보만을 수집하고 있었다. 따라서 수집 항목은 그림 4에서와 같이 양호한 보안수준으로 결과가 나타났다.

■ 저장 및 보유 단계

저장 및 보유 단계에서 미흡했던 부분은 개인정보파일대장과 관련된 부분이다. 대상시스템에서 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우 행정

안전부장관에게 등록하는 절차가 수행된다.

K병원은 개인정보일람표를 통해 취급중인 개인정보를 체계적으로 관리할 필요가 있다. 개인정보일람표는 취급하는 개인정보의 종류, 라이프사이클, 개인정보 취급의 근거, 취급형태 등을 목록화한 것이다.

개인정보파일이나 개인정보가 기록된 매체가 보관되어 있는 전산실이나 자료실은 CCTV등을 통해 출입을 모니터링하고 기록을 관리해야 하며 외부 인력의 보호구역 출입 및 업무 수행에 대한 주의가 필요하다.

■ 이용 및 제공

개인정보보유목적에 따른 적합한 범위 내의 이용 및 제공현황에 대하여 분석하였다. K병원의 경우 불필요한 접근권한과 위탁 계약 시 책임여부가 명시되지 않음이 발견되었다. 환자 개인정보가 인턴, 간호 실습생, 임상간호사들에게 필요 이상으로 오픈 되어 있으며, 별도의 특별한 제제 없이 개인정보에 접근할 수 있음을 확인하였다.

인턴의 접근 권한이 병동 이동이 있을 때마다 접근권한이 변경되지 않고, 병동 이동 후에도 이전 실습 병동에 대한 접근권한이 유지됨을 확인했다. 또한 간호실습생, 임상간호사는 ID를 공유하여 사용하고 있다. 이는 업무상 필요한 최소한의 인원에게 최소한의 범위로 권한이 할당되지 않았음을 의미하며, 악의적인 개인정보 유출사고가 발생할 가능성을 의미한다.

또한 개인정보 위탁에 있어 계약서상의 개인정보 관리에 대한 책임을 명시하지 않았다. 개인정보 취급 위탁 시 위탁 계약서상에 개인정보 관리에 대한 보호의무와 책임을 명시 하여야 한다.

의료기관 특성상 개인정보 및 개인 의료정보를 타기관에 제공하고 있었다. 개인정보를 제공받는 기관은 질병관리본부, 국립 암 센터, 보건복지부 등으로 모두 관련 법적 근거 하에 최소한의 항목에 대해서만 제공한다. 하지만 개인정보 제공과 관련하여 정보주체의 동의를 받지 않았다. 오프라인을 통한 개인정보수집을 제외하더라도 온라인 고객의 상당수가 환자 등록번호를 가진 오프라인 고객임을 감안할 때, 홈페이지상의 개인정보취급방침에 개인정보를 제공하는 관련 근거를 명시할 필요가 있다.

■ 파기 단계

개인정보는 수집 시 동의 받은 목적을 달성하거나 법적 보유기간이 만료되면 그 즉시 삭제하여야 하나, K병원의 경우 개인정보에 대한 파기, 보유기간이 불명확 하였다. 의료서비스 관련 개인정보는 전산화 시켜 반영구적으로 보관하고 있으며, 의료법에서 요구하는 보유기간은 최소 보유기간으로 해당 기간이 지나도 즉시 삭제하지는 않는다.

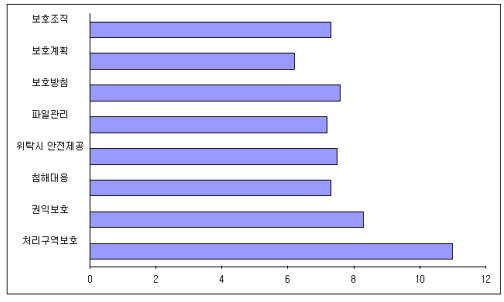
개인정보는 반드시 목적 이용 달성 또는 법적 보유기간이 만료되면 재생 불가능한 방법으로 파기해야만 한다. 또한 보유기간을 규정/지침에 명시하고, 이에 따라 안전하게 개인정보를 파기하여야 한다.

4.3 위험도 분석

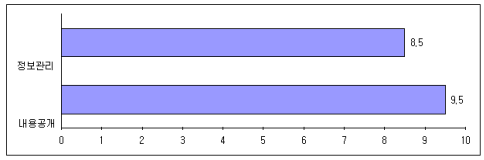
위험평가는 개인정보 침해 위험 요소별로 각각의 자산가치, 발생가능성, 법적준거성을 기준으로 위험도를 평가하여 수행하였다.

다시 말해 해당 개인정보 침해 요인 발생 가능성이 클수록, 그 파급 영향도가 클수록, 법률에 규정된 의무 사항일수록 해당 침해 요인이 통제되지 못하는 경우에 이로 인한 개인정보 침해 위험도가 크다는 개념에서 출발한 계량화 방안이다.

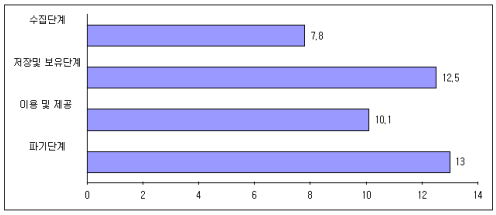
평가항목별로 위험도 중 고위험도는 개인정보처리구역보호 11.0, 저장 및 보유 12.5, 파기단계 13.0으로 분석 결과가 나타났다.



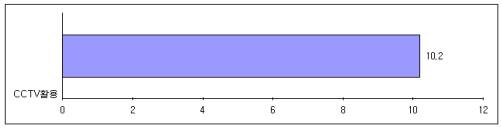
[그림 5] 대상기관의 개인정보 위험도



[그림 6] 대상시스템의 개인정보 위험도



[그림 7] 개인정보 생명주기별 개인정보 위험도



[그림 8] CCTV활용 개인정보 위험도

4.4 개선방안 수립

개인정보 영역별 위험도분석을 통한 고위험도 항목에 대하여 보호대책을 수립하고 취약점이 감소될 수 있도록 방안을 마련하고 적용하여야 한다. 영향평가 분석결과의 발견된 취약점에 대해 잠재위험에 대해 IT거버넌스의 People, Process, Technology관점에서 고위험도의 항목에 대해 개선방안을 수립하였다. 또한 향후 K병원의 안전한 개인정보관리체계를 위해서 취약점을 개선하고 지속적이고 체계적인 관리를 수행해야만 한다.

〈표 10〉 개선방안 수립

항목	잠재위험	People	Process	Technology
개인정보처리구역보호	개인정보를 처리하는 구역에 정기적으로 점검을 실시하지 않아 비인가자가 통제를 우회하여 침해유출 가능성	개인정보처리구역에 주기적으로 점검 및 관리	개인정보처리 구역 분리 및 시건 장치 설치	N/A
	개인정보보호구역 출입자의 출입시간을 기록하고 관리하여 추적 불가 가능성	개인정보처리구역의 관리 및 직원 보안교육실시	개인정보처리공간 구역 분리 및 출입대장 관리	N/A
저장및보유단계	개인정보가 저장된 저장매체에 대한 반입 및 출입에 따른 개인정보 유출 가능성	개인정보보호 교육 강화	저장매체 반입 및 출입 시 대장에 기록하도록 절차 수립	N/A
	저장매체에 주기적인 취약점 점검 부족으로 정보유출 발생 가능성	개인정보보호 교육 강화	이동형 저장매체 사용 시 승인받은 저장매체만 사용하도록 승인절차 수립	보안USB 도입 및 문서암호화 솔류션 도입
파기단계	보유기간 만료된 개인정보 파기하지 않아 정보주체에 소송 당할 가능성	개인정보보호 교육 강화 파기 사실 안내 교육	보유기간을 명확히 정하여 파기하는 프로세스 정립	물리적 파기장비 도입
	개인정보가 포함된 자료를 식별 불가능하도록 물리적으로 파기하지 않아 이면지로 활용 또는 유출 가능성	개인정보보호 교육 강화	개인정보가 포함된 문서는 이면지로 활용할 수 없도록 규정	물리적 파쇄장비 도입

5. 결 론

개인정보보호와 관련한 선행연구를 보면 법률과 제도가 완전하지 못하여서 많은 법제 분야와 기술적 측면의 많은 연구가 진행되어 왔다. 이제 개인정보보호법이 제정되고 개인정보영향평가시행이 공공기관을 시작으로 의무적으로 시행함에 따라 구체적인 사례를 살펴봄으로써 우리나라의 개인정보보호의 발전에 이 연구는 의의가 있다고 하겠다.

첫째, K병원의 전체 평가영역별 보안수준은 양호한 편이었다. 개인정보보호수준이 가장 낮은 항목은 개인정보 생명주기관리항목의 저장 및 보유단계 50.0, 이용 및 제공 64.1 및 파기단계에서 66.7로 나타나서 개인정보가 수집이후 저장되고 보유하는 시점부터 구체적인 기술적 보호조치 사항과 체계적인 관리정책을 수립하여 유출사고에 적극 대처해야 한다.

둘째, 위험도분석을 한 결과 고위험도 항목을 살펴보면 개인정보처리구역보호 11.0과, 저장 및 보유 항목 12.5 및 파기항목 13.0으로 분석이 되었다. 안전한 개인정보처리를 위하여 개인정보 처리구역을 분리하여 관리하여야 하며 직원출입 통제를 하고 보안교육을 강화하여야 한다. 승인된 저장매체를 이용하여 반출입시 대장에 기록하는 절차를 수립하고, 개인정보가 포함된 문서는 물리적 장

비로 파기하는 프로세스와 개인정보보호교육이 강화되어야 한다.

셋째, 공통적으로 고위험도와 보호 수준이 낮은 항목은 개인정보저장 및 보유단계와 파기단계, 개인정보처리항목으로 결과가 나타났다. 이에 대하여 개인정보처리항목과 저장 및 보유 항목의 미흡한 점을 해결하기 위하여 개인정보 처리구역을 분리하여 정기적으로 점검하고 출입자에 대한 대장을 구비하여 관리하고, 저장의 경우 개인정보의 반입 및 출입의 경우 통제사항을 만들고 명확한 보유기간을 정하여 개인정보를 파기하는 절차 수립 및 직원들의 개인정보보호교육의 강화를 하여야 한다.

참 고 문 헌

[1] 구병문, “프라이버시 영향평가제도의 국내법적 도입 방안”, 한국전산원 정보화이슈분석, 2004.06.

[2] 김소정, “한국의 프라이버시보호정책개선 방안연구-공공영역의 프라이버시영향평가 도입을 중심으로”, 고려대 정보보호대학원 박사학위논문, 2004.

[3] 김지원, “개인정보보호 관리체계 인증제도”,한국인터넷진흥원(정보통신서비스 개인정보보호 워크숍 자료), 2009.11.

[4] 김희완, 유재성, 김동수, “정보시스템 감리에서 개인정보 영향평가를 통한 개인정보 보호”, 한국콘텐츠학회논문지 제11권 제3호, 2011.

[5] 박순기, “이동통신사를 위한 개인정보영향평가(PIA)적용 방안에 관한 연구”, 동국대 국제정보대학원, 2006.

[6] 송익준, “AHP기법을 이용한 개인정보영향평가 점검항목별 가중치 산정에 관한 연구”,동국대학교 석사학위논문, 2010.06, 3p.

[7] 신영진, 김호성, “공공기관의 개인정보 영향평가제도 도입에 관한 연구-개인정보 영향평가의 평가체계 및 평가항목을 중심으로”, 한국행정학회, 동계학술대회, 2010, 2p.

[8] 장호익, “개인정보영향평가에 관한 법제연구”, 숭실대 박사학위논문, 2011.06, 13p.

[9] 정연수, 안준모, 권선경, “개인정보사전영향평가제도 도입방안에 관한 연구(1)”, 한국인터넷진흥원, 2003.

[10] 주경식, “개인정보보호법제에 관한 연구-개인정보 영향평가를 중심으로-”, 한양대 석사 학위, 2008.

[11] 최재용, “국가정보공유를 위한 개인정보영향평가모델의 실증적 연구”, 숭실대 대학원 박사학위, 2011.12, 7p.

[12] 행정안전부, 한국인터넷진흥원, “개인정보 영향평가 수행 안내서”, 2011.12.

[13] British Standard BS10012:2009 Data protection-Specification for a personal information management system.

[14] Cooper, Tom, “Impact of Privacy and Confidentiality on Valuation: An International Perspective”, Journal of Financial Management & Analysis. 2010

[15] Frank White, "The Use of Privacy Impact Assessment in Canada", Privacy files, 2001.

[16] Office of Management and Budget. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002(M-03-22)

[17] Stewart Blair, "Privacy Impact Assessment", Privacy Law & Policy Reporter, July 1996.

전 동 진 (Dong-Jin Jeon)

- 1995년 2월 : 서울대학교 자원공학과 석사 졸업
- 2010년 8월 : UBC(University of British Colombia) SMEI 수료
- 2000년 2월 : 아시아나항공 전산팀 근무
- 2009년 6월 : 마이크로소프트 컨설팅사업부 근무
- 현재 : 한국정보보호연구소 대표
- 관심분야 : 개인정보보호법

정 진 홍 (Jin-Hong Jeong)

- 1983년 2월 : 고려대학교 법학/일반사회학 석사
- 1993년 2월 : 한양대학교 법학 박사
- 1996년 2월 : University of Iowa College of Law, Research Professor(LL.M.)
- 2001년 5월 : 국가정보대학원(주임교수/학과장)
- 2009년 3월 : 산업기밀보호센타(처장/실장)
- 현재 : 서울과학종합대학원 산업정보대학원장
- 관심분야 : 산업보안, 개인정보보호법