J Korea Industr Inf Syst Res Volume 17 Number 6
http://dx.doi.org/10.9723/jksiis.2012.17.6.073

C쇼핑몰 개인정보 영향평가 사례연구

(A case study of Privacy Impact Assessment for C-Shopping Mall)

전 동 진*, 정 진 홍**
(Dong-Jin Jeon and Jin-Hong Jeong)

요 약 이 논문은 개인정보를 취급하는 정보시스템에 대하여 개인정보 침해에 대한 위협을 사전에 예방 및 점검을 수행하는 개인정보영향평가를 C쇼핑몰의 분석 사례를 통해 연구하였다. 결론적으로 C쇼핑몰의 개인정보 영향평가 분석을 수행한 결과 평가영역별로는 대상기관관리체계는 29.2, 대상시스템의 보호수준은 68.8, 개인정보처리단계의 결과는 25.5이고 신기술은 60.0으로 나타났다. 개인정보보호수준이 가장 낮은 항목은 대상기관의 개인정보파일관리 16.7, 개인정보생명주기관리 항목의 저장 및 보유단계 12.5, 이용 및 제공 단계 11.5, 파기 단계 16.7로 나타났다. 위험도 분석결과 고위험도 항목은 개인정보생명주기 영역의 저장 및 보유단계 항목이13.3, 파기단계 항목이 13.0으로 높은 수치가 나왔다. 종합적으로 보면 고위험도이면서 저보호수준인 항목은 저장 및 보유단계와 파기단계로 파악이 되었다.

핵심주제어 : 개인정보보호법, 개인정보영향평가, 위험도분석, 고위험도

Abstract This paper reviews Privacy Impact Assessments in order to perform preventing and diagnosis against potential threats focused on the C-Shopping mall case. The quality of protection in C-shopping mall shows that the corporations itself is 29.2, the system is 68.8, the life cycle of the privacy is 25.5 and CCTV is 60.0. The lowest levels are the corporation's management 16.7, the life-cycle's saving and keeping 12.5, usage and offer 11.5 and destruction 16.7 among the life cycle of the privacy. The result of risk analysis shows that the highest levels are saving and keeping 13.3 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, High risk

1. 서 론

인터넷 및 전자상거래의 활용이 급속히 확산되면서 인터넷 서비스업체에 제공된 개인정보가 범죄에사용되는 등 무분별하고 부주의한 개인정보 수집 및 이용이 급증하고 있고 개인정보 유출로 인한 정신적 물질적 피해가 속출하고 개인정보의 유통 및 매매가 증가하고 있어 개인정보보호의 필요성이 요구되고 있다. 개인의 이름·주소·주민등록번호·전화번호 등 신상정보의 단순한 수집·이용보다 개인의 여러 가지 거래내용·사회활동 내용과 신상정보를 조합함으로써 그 개인의 사상·성향·관심분야·자산상태·대인관계·취미 등 내면적 가치를 본인이 모르는 사이에 분석·활용할 수 있다는 데에 있다. 또한 백화점 고객정보 누출사건에서처럼

* 서울과학종합대학원 경영학박사 수료, 제1저자
Email: ceo@koripo.com
** 서울과학종합대학원 산업정보대학원장, 교신저자
Email: jhjeong@assist.ac.kr

개인정보의 남용·약용은 프라이버시 침해의 정도를 넘어 개인의 생명·신체에 위해를 가하는 원인이 될 수도 있다[2].

특히 최근에 발생한 각종 개인정보에 대한 침해 행위는 그 발생빈도와 피해규모가 날로 커지고 있으며, 유출된 개인정보가 보이스 피싱, 스팸 발송, 아이디도용 등 각종 범죄수단으로 활용되는 등 2차, 3차 피해 발생이 더욱 심각한 문제로 대두되고 있다. 이러한 측면에서 개인정보를 기반으로 한 정보통신서비스를 도입함에 있어 시스템 구축 사업의 전 과정에 걸쳐서 개인의 프라이버시에 미치는 영향을 사전에 분석하고, 침해가 발생하지 않도록 개선대책을 수립하게 함으로써 개인정보 침해로 인한 피해를 사전에 예방하게 하는 개인정보영향평가(Privacy Im pact Assessment)의 수행 필요성은 그 어느 때보다도 높다고 할 수 있다[1].

민간 기업은 물론 국가 공공기관이 전자정부의 확산 때문에 수많은 개인정보를 집적, 관리하고 있다. 이로 인해 개인정보와 같은 민감한 정보의 취급 이슈가 있는 정보화사업에 있어 그 기획단계에서부터 개인정보보호에 영향을 줄 수 있는 요소들을 찾고 그 관리수준과 위험도를 평가해야하는 필요성을 인식하고 있다. 이에 따라 한국인터넷진흥원은 2005년 기업에 적용할 수 있는 PIA가이드를 제정, 배포하였고 2009년에는 개인정보 영향평가가 공공기관을 대상으로 수행되고 있다. PIA는 단순한 시스템 평가 차원을 넘어 개인정보를 포함하는 사업 시행으로 인해 개인의 프라이버시에 미칠 수 있는 중대한 영향을 사전에 파악하고 그 영향을 줄이거나 없앨 수 있는 방안을 모색하는 것이기 때문에 보안수준평가 방법을 포함하고 있다[1].

이 논문은 개인정보영향평가를 소규모 C쇼핑몰의 사례로 하여 구체적인 개인정보영향평가 방법론에 초점을 두었다. 제 2장에서는 이론적인 배경으로서 개인정보영향평가의 전반적인 개념과 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.

그리고 마지막으로 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 개념

개인정보영향평가(PIA: Privacy Impact Asse ssment)란 개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경시 동 시스템의 구축·운영·변경 등이 프라이버시에 미치는 영향에 대하여 사전에 조사·예측·검토하여 개선방안을 도출하는 체계적인 절차를 의미 한다[5].

개인정보영향평가제도는 개인정보에 대한 침해가 발생하기 이전에 내부적으로 문제를 예측하고 검토를 하여 국가기관에 대한 국민의 신뢰를 증진시키고, 사후적인 대처로 인한 추가비용을 감소시킬 수 있게 한다. 또한 각종 시스템의 설계단계에서부터 개인정보보호의 관점에서 계획을 수립하도록 함으로써 비용을 체감하고 사전 예방적인 효과를 거둘 수 있게 한다[7]. 이러한 PIA의 핵심은 개인정보의 흐름을 분석하고 그것을 도식화 시킨 후 개인정보유출 위험을 찾는 것이다. 도출된 위험은 위험의 크기에 따라 수치화된 위험도를 표기하게 되고 위험도의 크기가 높은 순으로 보안대책을 마련하는 방식을 택한다. 또한 PIA의 절차 중 가장 큰 특징은 정보시스템 자산에 대한 위험분석 및 평가를 포함하고 있다는 점이다. 평가된 모든 위험에 대한 보안대책을 수립하고 적용하는 것은 많은 예산을 수반하는 일이므로 수용 가능한 위험의 정도(Degree of Assurance)를 정한 후 위험의 정도(위험도)가 높은 위험부터 합의된 DOA까지 보완대책을 수립하는 방식을 택한다. 이러한 방식은 기업이 위험에 대한 대책을 세우고 비용 효과적으로 위험을 관리하기 위한 중요한 방법론이라고 할 수 있다[1].

개인정보 영향평가를 실시하는 경우는 크게 다음과 같다.

첫째, 개인정보시스템을 구축하는 경우로 개인정보 취급절차가 새롭게 마련됨에 따라 그 과정에서 개인정보 침해위험의 발생가능성에 대한 영향평가가 필요하다.

둘째, 기존에 구축된 개인정보파일의 수집·보유·이용·제공, 파기 등 취급절차를 변경하는 경우로서 수집경로가 온라인에서 오프라인에서 확대되는 경우이다.

셋째, 개인정보파일을 타 기관과 연계·제공하는 경우로서 개인정보를 보유하고 있던 기관의 관리체계를 벗어나고 접근 인원 또한 넓어지는 경우이다.

마지막으로 C쇼핑몰의 경우처럼 기존 운영 중인 서비스에서 개인정보의 수집·보유·이용·제공·파기 등의 절차에서 중대한 개인정보 침해위험이 우려되거나 개인정보 관리체계를 점검하고 개선하기 위해서도 개인정보 영향평가를 수행할 수 있다[11].

2.2 개인정보영향평가의 평가 항목

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

평가항목은 기관이 개인정보보호를 위해 조치해야 하는 사항으로 총 4개의 평가영역으로 구분되고 각 영역은 평가기관의 개인정보보호관리체계, 대상시스템의 개인정보보호관리체계, 개인정보처리단계별 보호, 특정 IT기술 및 활용 시 개인정보보호이고, 평가항목은 총 18개, 세부 조항 114개로 구성되어있다.

2.3 연구 방법

2012년 4월 한 달 간 C쇼핑몰의 개인정보처리 주요 시스템인 웹서버, 고객관리시스템 등의 개인정보영향평가를 설문조사와 병행하여 탐색적 연구를 위한 인터뷰를 수행하였다. 개인정보시스템의 각 업무 담당자인 관리자, 총무, 경영자 등의 개인정보 처리담당자와 4가지 평가영역의 114가지 중 RFID, 바이오활용, 위치정보 항목을 제외한 103가지 세부항목에 대하여 조사하였다.

<표 1> 개인정보영향평가 영역과 항목

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. 대상시스템의개인정보보호 관리체계
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

2.4 개인정보흐름도 분석

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

2.5 개인정보보호 수준 분석

개인정보관리현황 진단 시 보안수준은 Y, P, N, N/A 등급으로 구분하여 진단하며, 평가 항목에 대하여 적용의 만족과 수행여부에 따라 표2에 표시된 부문에 점수를 표시하였다.

<표 2> 보안수준 표시 기호[11]

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), 미흡(81-90), 안전(91-100)으로 등급을 부여한다.

2.6 위험도 분석

개선사항의 우선순위 선정을 위한 위험도 산정방법은 개인정보 취급업무를 자산으로 보고 업무내의 개인정보의 조합수준에 따라 자산 가치를 산정하여 자산 가치, 침해요인발생가능성, 법적준거성을 조합하여 위험도를 평가하여 합산하는 방법을 적용할 수 있다. 표 3을 보면 자산가치가 높을수록, 표 4의 법률에 규정된 의무사항일 수록, 표 5의 개인정보침해요인의 발생가능성이 높을수록 개인정보 침해 위험도가 크다는 개념에서 생성한 위험도 산정방안이다. 위험도를 전체적으로 계산하여 보면 표 6과 같다.

<표 3> 개인정보 위험도 자산가치 수치[11]

조합수준	조합설명	자산가치	개인정보 영향도 설명	비고
P3이상	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,P1을 조합하면 파악이 되는 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 요구받을 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[11]

구분	법적준거성	중요도
높음	법적준수사항	1.5
낮음	법률외 요건	1

<표 5> 개인정보 침해요인 발생 가능성[11]

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

2.7 개선방안 수립

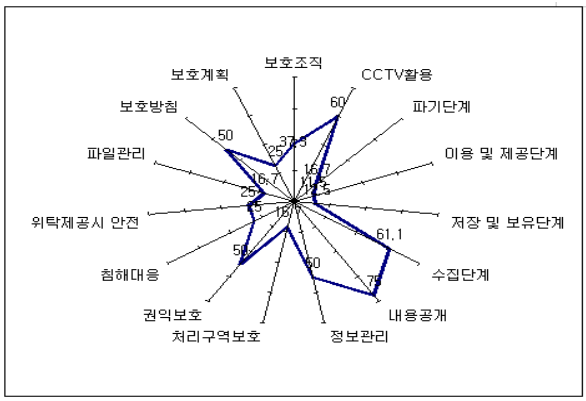
위험도 산정 결과를 기반으로 자산에 대한 위험을 제거하거나 최소화하기 위한 개선방안을 도출한다. 개선방안을 수립하기위해 개인정보처리 담당자, 시스템 담당자 및 개발업체 등 평가와 관련된 전체 대상자의 의견을 수렴하여 우선순위 또는 단기, 중장기로 구분하여 도출한다. 도출된 개선방안을 기반으로 정보화사업 진행일정, 예산, 과제 성격 등을 고려하여 개선계획을 수립할 수 있다.

3. 개인정보 영향평가 결과

행정안전부의 개인정보영향평가수행가이드를 토대로 4가지 평가영역과 평가항목 17가지의 결과는 표 7과 같다. 전체 대상기관의 개인정보보호관리체계, 대상 시스템의 개인정보 보호관리체계, 개인정보 라이프사이클상의 항목, 특정IT기술활용 분야를 파악하였다.

<표 7> C쇼핑몰 개인정보 영향평가 결과

평가 항목	항목수	Y	P	N	N/A
1. 개인정보보호조직	4	1	1	2	
2. 개인정보보호계획	2	0	1	1	
3. 개인정보보호방침	7	2	3	2	
4. 개인정보파일관리	6	0	2	4	
5.개인정보위탁 및 제공시 안전조치	2	0	1	1	
6. 개인정보침해대응	4	0	2	2	
7. 정보주체권익보호	3	0	3	0	
8. 개인정보처리구역보호	3	0	2	1	
9. 시스템의 개인정보관리	2	1	0	1	
10. 개인정보취급내용 공개	6	3	3	0	
11. 수집단계	12	4	3	2	3
12. 저장 및 보유단계	4	0	1	3	
13. 이용 및 연계제공단계	40	1	7	31	1
14. 파기단계	3	0	1	2	
15. CCTV활용	5	2	2	1	



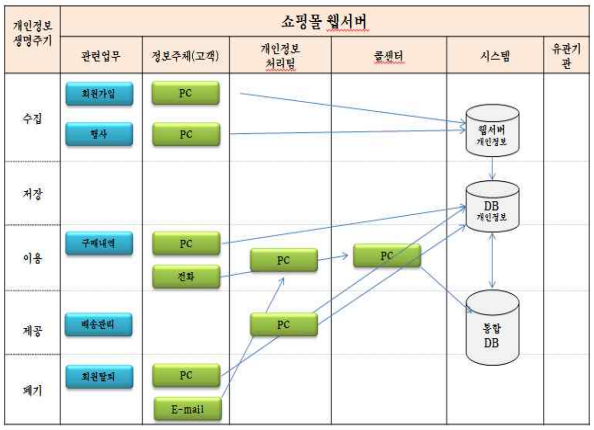
<그림 1> 전체 평가영역 보안수준 결과표

C쇼핑몰의 전체 평가항목 결과는 그림 1에서 나타난 것과 같이 대상기관의 관리체계는 평균 29.2, 대상기관의 관리체계는 68.8, 개인정보처리 단계의 보호조치는 25.5이고 특정 IT기술은 60.0으로 나타나 보호수준은 매우 미흡한 것으로 나타났다.

3.1 개인정보 흐름도 분석

3.1.1 웹서버 개인정보시스템

웹사이트에서 개인정보를 수집하면 이 정보는 웹서버의 데이터베이스에 저장된다. 가격 행사로 인한 이벤트의 경우 설문조사 데이터를 수집하여 통계분석을 실시하여 마케팅에 활용한다. 그림 2에 자세한 흐름도와 표 8에 개인정보 수집항목을 나타내었다.



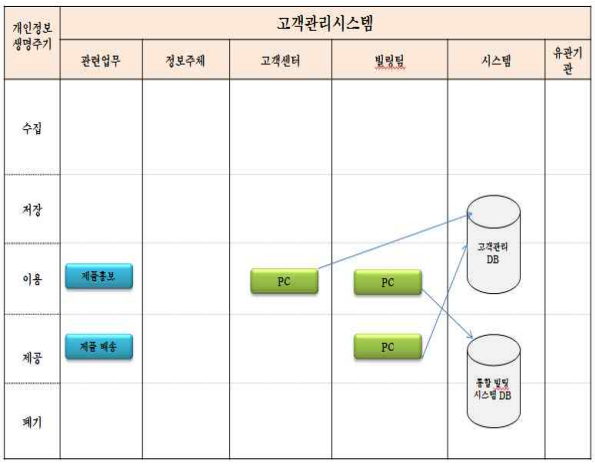
<그림 2> 홈페이지 개인정보 흐름도 분석

<표 8> 웹서버 개인정보 흐름표

항목	시스템	개인정보	담당자
수집	웹서버	ID, 비밀번호,성명,닉네임 주민등록번호,이메일,생년월일, 주소, 전화번호,혼인여부, 관심분야, 사진첨부	관리자
저장	웹서버	ID, 비밀번호,성명,닉네임 주민등록번호,이메일,생년월일, 주소, 전화번호,혼인여부, 관심분야, 사진첨부	관리자
이용	웹서버	ID, 성명,닉네임 주민등록번호,이메일,생년월일, 주소, 전화번호,혼인여부, 관심분야, 사진	관리자
제공	개인 PC	ID, 성명,닉네임 주민등록번호,이메일,생년월일, 주소, 전화번호,혼인여부, 관심분야	관리자
파기	웹서버	ID, 비밀번호,성명,닉네임 주민등록번호,이메일,생년월일, 주소, 전화번호,혼인여부, 관심분야, 사진첨부	관리자

3.1.2 고객관리 시스템

그림 3에 고객관리시스템의 개인정보 흐름도를 나타내었다. C쇼핑몰의 고객관리와 택배, PG 및 빌링을 위한 시스템으로 구성되어 있다. 웹서버에서 전달받은 고객 정보를 통하여 상품 배송을 위하여 고객과의 연락 및 마케팅 목적 및 고객서비스 관리 시스템이다.



<그림 3> 고객관리시스템 흐름도 분석

3.2 개인정보보호 수준 분석

3.2.1 대상기관의 관리체계

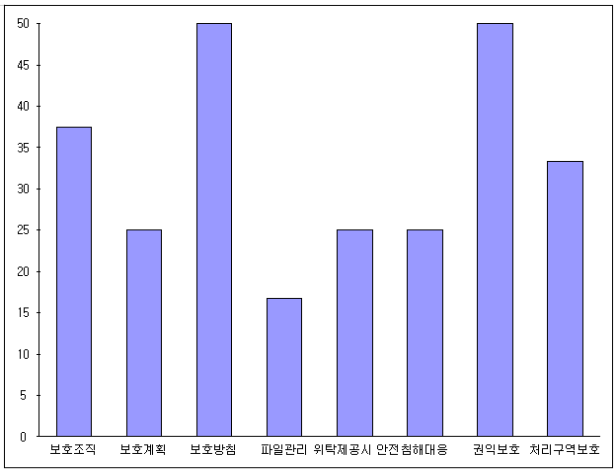
개인정보 관리체계에서는 조직, 교육, 개인정보보호 방침, 개인정보 파일관리, 개인정보위탁 시 안전조치, 정보주체 권익 등에 관하여 분석하였다. 표 9의 개인정보 보호조직 관리체계는 조직에 대한 정책과 지침에 대한 부분으로 결과가 미흡하게 나왔다. 그림 4에서 보듯이 개인정보 보호 계획과 개인정보보호 파일관리 항목은 매우 미흡한 결과가 나타났다.

C쇼핑몰의 경우 개인정보보호에 대한 인식 부족 및 정보보호교육에 대하여 취약하여 개인정보보호에 대한 교육 및 통제 관리를 수행하여야 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 미흡한 것으로 나타났다.

<표 9> C쇼핑몰 개인정보 영향평가 항목별 결과표 일부

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



<그림 4> 대상기관 개인정보 관리체계

3.2.2 대상시스템의 개인정보보호관리 체계

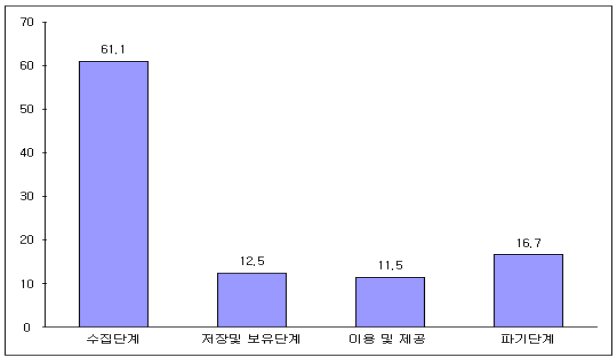
대상시스템의 개인정보보호관리 체계 영역에서는 전체적으로 미흡한 시스템관리상태로 파악되었다.

3.2.3 개인정보 생명주기 처리단계별 진단

그림 5에서 보면 전체적으로 파기단계와 저장 보유 단계에서 보안수준이 극히 낮음을 알 수 있다.

3.2.3.1 수집 단계

C쇼핑몰은 개인정보를 수집함에 있어 닉네임 성별, 혼인여부, 관심분야, 메일링 수신, SMS 수신등 향후 마케팅을 위한 정보도 같이 수집하여서 필요 사항 외의 정보도 수집하고 있다. 이는 거의 모든 타 쇼핑몰도 동일함을 알 수 있고 수집에 관련된 DB스키마를 재설계하여 최소한의 정보를 수집하여야 한다.



<그림 5> 개인정보 생명주기별 진단

수집 항목은 전체적으로 보안수준이 그림 5에서와 같이 미흡한 보안수준으로 결과가 나타났다.

3.2.3.2 저장 및 보유 단계

저장 및 보유 단계에서는 대상시스템에 대한 개인정보파일의 대장도 존재하지 않고 신규로 보유하거나 변경되는 경우 개인정보파일대장에 반영하는 절차가 없다. 또한 개인정보 및 비밀번호의 암호화 수준도 낮은 상태로 되어 있어 매우 취약함을 알 수 있다.

3.2.3.3 이용 및 제공 단계

C쇼핑몰은 수집된 개인정보에 대하여 개인정보를 목적 외의 용도로 타 기관에 연계, 제공할 경우에도 별도의 동의를 받는 절차가 마련되어 있지 않고 있다. 각 정보주체에 대하여 로그인 횟수, 일반글 등록수, 답변글 등록 수, 마지막로그인 날짜, IP번호 등도 시스템에서 관리하여 마케팅에 활용하고 있다. 각 회원에 대한 포인트 및 기타 구매 정도에 따라 레벨을 정하여 관리하고 있다.

수집된 개인정보 외에 모든 온라인 활동에 대하여 자체적으로 관리하고 있으며 개인정보 관리에 대한 직원들의 권한 설정이 안 되어 있고 웹애플리케이션 개발에 있어 접속이 제한이 안 되어 있다.

개인정보 취급 업무시 승인처리에 대한 절차가 없고 개인정보처리시스템의 처리내역에 관한 사항을 로그파일로 기록하게 설계가 되어 있지가 않다.

유무선 개인정보처리단말기에서 ID, 패스워드, 계좌번호, 카드번호 등 민감정보 입력 시 키보드해킹방지 기술을 적용하지 않았다.

또한 개인정보 접근 및 이용로그를 안전하게 기록하고 보존하기 위한 분리된 내부 망에 존재하는 별도

저장장치에 백업 보관하여야 한다.

3.2.3.4 파기 단계

C쇼핑몰은 개인정보파일의 보유기간이 경과하거나 보유목적이 달성되었을 경우 파기하여야 하는데 파기를 하지 않고 있다. 이용 목적을 달성한 개인정보를 보관할 경우 해당 개인정보 파일을 다른 개인정보와 분리하여 보관하지 않고 있다.

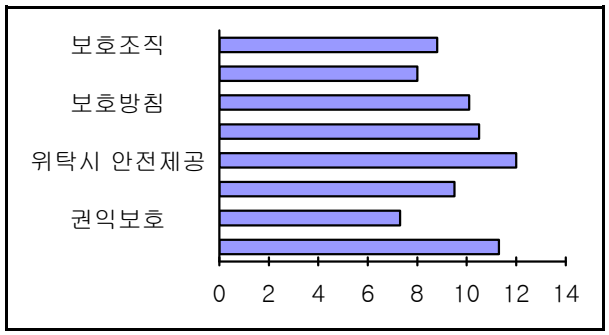
개인정보의 보유기간이 종료되어 파기할 경우 복구 또는 재생이 불가하게 파기하도록 하여야 한다.

3.3 위험도 분석

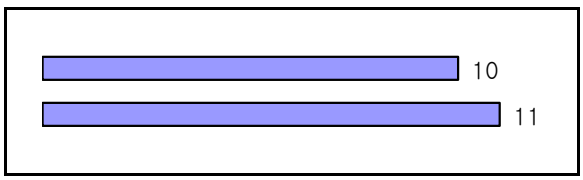
위험평가는 개인정보 침해 위험 요소별로 각각의 자산가치, 발생가능성, 법적준거성을 기준으로 위험도를 평가하여 수행하였다.

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

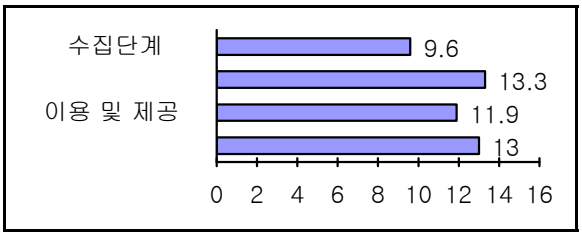
그림 6에서 그림 9까지 분석 결과를 살펴보면 평가항목별로 위험도 중 고위험도는저장 및 보유 13.3, 파기단계 13.0으로 분석 결과가 나타났다.



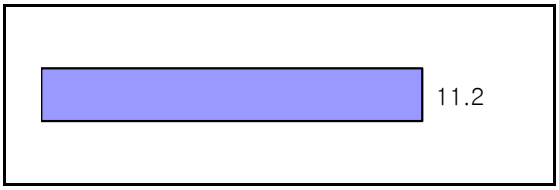
<그림 6> 대상기관의 개인정보 위험도



<그림 7> 대상시스템의 개인정보 위험도



<그림 8>개인정보생명주기별 개인정보 위험도



<그림 9> CCTV활용 개인정보 위험도

3.4 개선방안 수립

개인정보 영역별 위험도분석을 통한 고위험도 항목에 대하여 보호대책을 수립하고 취약점이 감소될 수 있도록 방안을 마련하고 적용하여야 한다. 영향평가 분석결과의 발견된 취약점에 대해 표 10에 잠재위험에 대해 IT거버넌스의 People, Process, Technology관점에서 고위험도의 항목에 대해 개선방안을 수립하였다. 또한 향후 C쇼핑몰의 안전한 개인정보관리체계를 위해서 취약점을 개선하고 지속적인 모니터링을 하여 체계적인 관리를 수행해야 한다.

<표 10> 개선 방안 수립

항목	잠재위험	People	Process	Technology
저장 및 보유 단계	개인정보가 신규로 보유하거나 변경에 따른 대장에 기입하지 않아 개인정보 유출 가능성	개인정보보호 교육 강화	개인정보대장에 기록하도록 절차 수립	N/A
	중요개인정보를 저장 보유 하는 경우 암호화 하지 않아 개인정보 유출 가능성	개인정보보호 교육 강화	중요 개인정보를 저장 보유하는 경우 암호화하는 절차 수립	암호화 솔류션 도입

이용 및 제공 단계	업무상 필요한 최소한의 인원이 접근이 아니어 개인정보 유출 가능성 높음	개인정보보호교육 강화	최소한의 인원만 접근 가능한 프로세스 정립	접근제어 솔류션 도입
	개인정보를 타기관에 연계 제공할 경우 별도의 동의 를 받지 않아 법률 위반으로 소송 가능성	개인정보보호교육 강화	별도의 동의를 받는 프로세스 정립	N/A

4. 결 론

개인정보에 대한 인식이 최근 침해유출 사고 이후에 많이 달라지고 있고, 개인정보가 기업의 자산인 동시에 안전성을 확보해야 할 필요성이 점점 높아지고 있다. 이 연구는 구체적인 개인정보영향평가 수행 사례를 통하여 개인정보보호에 대한 안전성 확보를 방안을 제시하는데 의의가 있다. 향후 연구과제는 개선방안을 지속적으로 개선 유지할 수 있도록 하는 모니터링 시스템을 체계화하는 연구를 하고 있다.

첫째, C쇼핑몰은 소규모로 운영 되어서 개인정보보호에 대한 인식도 부족한 상태인지라 C쇼핑몰의 전체 평가영역별 보안수준은 극히 미흡하여서 적극적인 개인정보의 보호에 대한 대책 마련이 시급하다. 개인정보보호수준이 가장 낮은 항목은 대상기관의 개인정보파일관리 항목 16.7,개인정보 생명주기관리항목의 저장 및 보유단계 12.5, 이용 및 제공 단계 11.5, 파기단계에서 16.7로 나타나서 개인정보 파일관리에서부터 개인정보가 수집이후 저장되고 이용 및 파기하는 시점까지 구체적이고 기술적 인 보호조치 사항과 체계적인 관리정책을 수립하여 유출사고에 적극 대처해야 한다.

둘째, 위험도 분석을 한 결과 고위험도 항목을 살펴보면 위탁 및 제공시 안전조치 12.0, 저장 및 보유 항목 13.3 및 파기항목 13.0으로 분석이 되었다. 개인정보의 안전성확보 조치로서 개인정보를 저장 및 보유할 경우 암호화 수준을 높여서 저장을 하고, 개인정보처리 업무상 필요한 최소한의 인원이 접근제어 하여야 한다. 개인정보가 포함된 문서 및 장치는 물리적 장비로 파기하는 프로세스를 마련하여야 한다.

셋째, 공통적으로 고위험도와 보호 수준이 낮은 항목은 개인정보저장 및 보유단계, 이용 및 제공, 및 파기단계 항목으로 결과가 나타났다. 이에 대하여 개인저장 및 보유 항목의 미흡한 점을 해결하기 위하여 개인정보 대장을 마련하여 신규 또는 변경시 대장 기입하는 프로세스를 마련하고, 이용 및 제공의 경우 개인정보의 정보주체에 별도의 동의를 받도록 하는 절차도 마련하여야 한다. 또한 개인정보를 파기하는 절차 수립 및 직원들의 개인정보보호교육의 강화를 하여야 한다.

참 고 문 헌

[1] 김명현, “개인정보보호 수준 평가지표 개발에 관한 연구”, 전남대학교 대학원 정보보호 협동과정, 2011.08.

[2] 김영렬, “개인정보보호의식 측정 척도의 개발과 개인정보 중요성에 관한 인지도 조사”, 한국산업정보학회논문지 제 15권 제 5호, 2010.12.

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

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

[5] 김희완, 유재성, 김동수, “정보시스템 감리에서 개인정보 영향평가를 통한 개인정보 보호”, 한국콘텐츠학회논문지 제 11권 제3호, 2011.

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

[7] 송익준, “AHP기법을 이용한 개인정보영향평가 점검 항목별 가중치 산정에 관한 연구”,동국대학교 석사학위논문, 2010.06.

[8] 안태희, “우리 나라 실정에 맞는 개인정보의식에

관한 Measurement개발과 개인정보에 관한 의식 조사",한국산업정보학회 학술대회논문집, 2001,05.
[9] 장호익, "개인정보영향평가에 관한 법제연구", 숭실대 박사학위논문, 2011.06.
[10] 정연수, 안준모, 권선경, "개인정보사전영향평가제도 도입방안에 관한 연구(1)", 한국인터넷진흥원, 2003.
[11] 주경식, "개인정보보호법제에 관한 연구-개인정보 영향평가를 중심으로-", 한양대 석사 학위, 2008.
[12] 최재용, "국가정보공유를 위한 개인정보영향평가 모델의 실증적 연구", 숭실대 대학원 박사학위, 2011.12, 1p.
[13] 행정안전부, 한국인터넷진흥원, "개인정보 영향평가 수행 안내서", 2011.12.
[14] British Standard BS10012:2009 Data protection-Specification for a personal information management system.
[15] Cooper, Tom, "Impact of Privacy and Confidentiality on Valuation: An International Perspective", Journal of Financial Management & Analysis. 2010
[16] Frank White, "The Use of Privacy Impact Assessment in Canada", Privacy files, 2001.
[17] Office of Management and Budget. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002(M-03-22)
[18] Stewart Blair, "Privacy Impact Assessment", Privacy Law & Policy Reporter, July 1996.

전 동 진 (Dong-Jin Jeon)

- 1995년 2월 : 서울대학교 자원공학과 석사
- 2010년 8월 : UBC(University of British Colombia) SMEI
- 2000년 2월 : 아시아나항공 전산팀
- 2009년 6월 : 마이크로소프트 컨설팅사업부
- 현재 : 한국정보보호연구소 대표
- 관심분야 : 개인정보보호법
- E-Mail : ceo@koripo.com

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
- E-Mail : jhjeong@assist.ac.kr

논 문 접 수 일 : 2012년 08월 22일
1차수정완료일 : 2012년 09월 04일
2차수정완료일 : 2012년 10월 12일
게 재 확 정 일 : 2012년 10월 26일