공 학 석 사 학 위 논 문

인터넷 원서 접수 시스템의 개인정보보호 방안 연구

2009년 8월

부 경 대 학 교 산 업 대 학 원

전산정보학과

정 갑 규

공 학 석 사 학 위 논 문

인터넷 원서 접수 시스템의 개인정보보호 방안 연구

지도교수 이 경 현

이 논문을 공학석사 학위논문으로 제출함.

2009년 8월

부 경 대 학 교 산 업 대 학 원

전산정보학과

정 갑 규

이 논문을 정갑규의 공학석사
학위논문으로 인준함

2009 년 8 월 26 일

주 심 공학박사 김 창 수 (인)

위 원 이학박사 이 경 현 (인)

위 원 이학박사 신 상 욱 (인)

목 차

표 목 차

그 림 목 차

A Study on Privacy Protection of Internet-Based Admission Application System

Jung Kap-Kyu

Graduate School of Industry

Pukyong National University

Abstract

With the advancement of information society and the increase of economic values of personal information, the collection and use of personal information have been widely proliferating through the entire areas in the society. However, personal privacy intrusions and mental and monetary damages are continuously occurred due to the personal information leakage and misuses and abuses of personal information.

On recent, most of colleges and universities adopted on-line admission application systems which are applicable to all processes of receiving the admission applications such as preparations, electronic payments of examination fees and issuing of admission tickets for examination etc. The systems are very useful and have greatly beneficial to both sides of the universities and the applicants.

However, there are some possibilities which great damages may occur due to the negative effects such as mass leakage of the personal information due to the system hacking, the situation of inability to receive applications due to simultaneous rushing applications near the closing time of the receiving procedure, etc. Therefore, in this paper, we issue the privacy protections in the Internet-based application system which are widely accepted and entrusted with agencies by most universities and colleges.

We simulate on the evaluations of Privacy Impact Assessment from the

viewpoints of a series of processes such as reviews of policies and systems relating to the protection of personal information, analyses of personal information streams, analyses of factors for personal information leakage, risk evaluations and deriving the improvement plans, etc. And we deduce the problems and improvement measures relating to personal information leakage, and finally we try to establish a safe environment structure which provides a secrecy against the personal information leakage when students and parents are submitting the entrance applications for the universities and colleges.

Ⅰ. 서론

정보기술의 발달로 개인정보[1]가 대량 집적되고 수집과 이용, 공유가 용이해졌으나, 유출 위험은 크게 높아졌다. 한번 유출된 개인정보를 회수하는 것은 불가능에 가깝고, 스팸메일 발송 등 제 2,3의 오·남용으로 이어지는 등 그 피해 또한 예측이 불가하다. 또한 홈페이지 상의 무분별한 개인정보 노출도 심각한 문제이다. 인터넷 상에서는 구글 등 강력한 검색엔진에서 검색어의 적절한 조합만으로도 노출된 개인정보를 쉽게 구할 수 있다. 정부에서 2005년도부터 시작한 홈페이지 개인정보 노출실태 점검결과[표 1]를 보면 대량의 개인정보를 보유한 기관, 기업에서도 개인정보가 담긴 파일이 간단한 검색어로 노출되었던 것으로 나타났다[7].

[표 1] 2007년 하반기 공공기관 홈페이지 개인정보 노출실태 점검 결과 [9]

대상	점검기간	노출사이트(개)	노출건수(건)
주요 사이트(800개)	1차: 7. 1. - 8.31.	309	47,636
	2차: 9. 1. - 10. 5.	100	10,154
	3차:11. 7. - 11.30.	29	557
서브 사이트(486개)	1차:10. 6. - 11. 6.	44	6,643
	2차:12. 1. - 12.17.	20	2,169

이에 대한 대책으로 정부에서는 개인정보유출방지시스템 도입 확대, 웹사이트 개인정보 노출 집중점검 대상 사이트를 지속적으로 확대, 노출에

1) **개인정보의 개념**

"개인정보"라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다(공공기관의 개인정보보호에 관한 법률 제2조) [9].

따른 징계 처벌 강화 등으로 개인정보유출이 크게 줄었지만, 아직도 많은 기관들이 전담 전문인력 부족 및 체계적인 관리 미흡으로 개인정보보호에 많은 어려움이 있는 실정이다.

한편 대입원서접수에 관하여 살펴보면 인터넷 원서접수 시스템이 활성화되기 전의 대입원서 접수 처리는 매우 방대한 업무였다. 대학 측에서는 입학 원서 및 요강 등의 인쇄물 준비, 전산시스템 구축, 접수창구 설치, 접수요원 편성, 지원자 정보의 입력 및 대조, 전형결과 통보 등의 주 업무 및 각종 부대업무로 인해 많은 예산과 인력이 투입되었고, 그에 따라 전형료가 올라가게 되어 지원자에게 부담을 주었으며 또한, 지원자 측에서도 원서의 구입, 원서 작성, 접수 대학으로 이동, 대기, 접수 등의 행위로 시간적 금전적으로(교통비 숙박비 등) 큰 부담이 되었다.

현재는 지원서 작성, 전형료 전자결재, 수험표 발급 등 대입원서접수 전 과정을 인터넷 기술을 적용하여 온라인 처리함으로써 대학과 수험생 모두에게 획기적으로 시간적 금전적 손실을 줄이는 등 국가적으로 대단한 정보화 효과를 누리고 있으며, 인터넷 원서대행업체 등 신종 정보서비스사업도 번창하고 있다. 하지만 해킹으로 인한 개인정보 대량 유출의 위험성, 마감시간에 접수폭주로 인한 접수마비 사태 등 그에 따른 역기능으로 큰 피해가 발생할 소지가 있다.

본 연구에서는 인터넷 원서 접수 업무 전반에 대하여 개인정보 영향평가 기법을 이용한 체계적인 개인정보 흐름분석 및 위험대책수립으로 효과적인 개인정보 보호 방안을 제시하고자 한다. 개인정보 영향평가 방법은 한국정보보호진흥원(KISA)에서 개발한 방법론을 적용하였다.

Ⅱ. 인터넷 원서접수시스템의 현황과 문제점

인터넷 원서 접수 방법은 대행업체을 통한 인터넷 접수와 대학 자체 인터넷 접수 방법이 있다. 2009학년도 정시 모집 원서 접수 유형별 대학(4년제) 현황([표 2])를 보면 자체 인터넷 원서접수을 하는 대학은 일부 몇 개 대학에서 채택하고 있을 뿐이고 대부분의 대학(95%)은 대행업체에 위탁을 하고 있다[8]. 대행업체를 통한 인터넷 원서 접수는 지난 2002년부터 시작되었고 현재는 2개 회사가 독점하고 있다. 학생들의 이용편의와 학교의 부담 감소라는 장점 때문에 2003년 200만건, 2006년 300만건을 고비로 2009년에는 250만건 정도로 추산되어 국내 대학의 약 95%가 대행업체를 통해 원서를 접수하고 있다. 2005년 말 원서 접수 마감일 접수 폭주로 인한 인터넷 접수 시스템 마비로 상당수 대학이 원서접수기간을 연장하는 초유의 사태도 발생하였다. 정시모집의 경우 대부분의 지원자들이 짧은 기간에 원서를 제출하기 때문에 이를 감당할 수 있는 서버를 자체적으로 구축하기 힘들어 대부분 대학에서는 인터넷 원서 접수를 대행업체에 맡기고 있다.

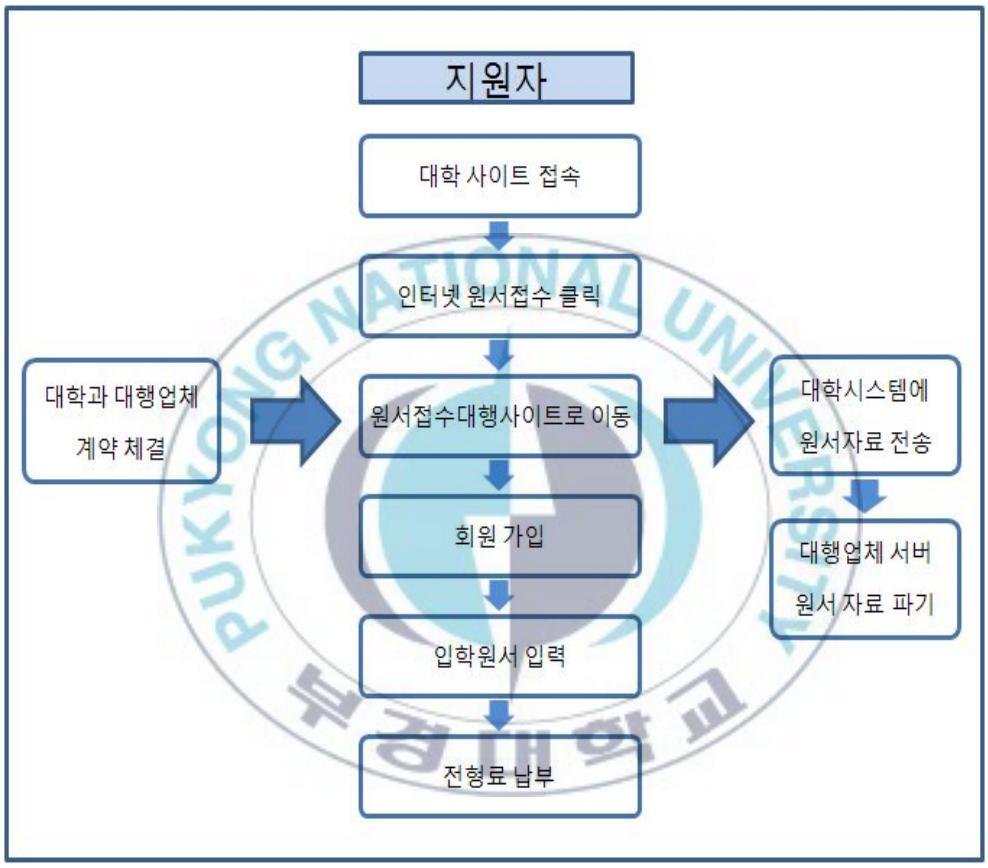
[그림 5]는 대부분 대학의 인터넷 원서접수 업무 흐름도이다[8]. 인터넷으로 원서를 제출하는 수험생들은 반드시 대행업체 홈페이지 회원으로 가입해야 하며, 업체에서 요구하는 항목을 기재해야 한다. 수험생이 기재한 수능점수와 지원대학, 신상정보는 물론 학부모의 휴대전화와 전화번호까지 대행업체 서버에 저장된다. 그러나 이러한 정보가 업체에서 관리되고 있어, 해당업체의 개인정보보호방침과 대학과 해당업체간의 계약서에 개인정보보호 조항이 명시되어 있지만 실제로 개인정보유출 사례 및 오남용 사례가 있는지 또는 일정 기간 후 폐기하는 지 등의 여부 확인에는 한계가 있을 수 밖에 없다. 이에 따라 개인정보 유출에 대한 불안은 항상 존재하고 있다.

[표 2] 2009학년도 정시 모집 원서 접수 유형별 대학(4년제) 현황

구분	대학명
인터넷접수	가천의과학대, 가톨릭대, 강남대, 강원대, 건국대, 경기대, 경북대, 경상대, 경성대, 경인교육대,경희대, 계명대, 고려대, 공주교육대, 광신대, 광운대, 광주교육대, 국민대, 군산대, 금오공과대, 단국대, 대구가톨릭대, **대구교육대**, 대진대, 덕성여대, 동국대, 동덕여대, 동명대, 동아대, 동의대, 명지대, 목포해양대, 부경대, 부산가톨릭대, 부산대, 부산외대, 배재대, 삼육대, 상명대, 서강대, 서경대, 서울교육대, 서울대, 서울산업대, 서울시립대, 서울신학대, 서울여대, 서원대, 성결대, 성균관대, 성신여대, 세종대, 수원대, 숙명여대, 순천대, 숭실대, 아주대, 안동대, 안양대, 연세대, 영남대, 울산과학기술대, 울산대, 이화여대, 인천대, 인하대, 장로회신학대, 전남대, 전북대, 전주교육대, 제주대, 조선대, 중앙대, 중원대, 진주교육대, 청주대, 창원대, 청주교육대, 총신대, 추계예술대, 춘천교육대, 충남대, 충북대, 충주대, 포천중문의대, 포항공대, 한경대, 한국기술교육대, 한국교원대, 한국산업기술대, 한국외대, 한국체육대, 한국항공대, 한국해양대, 한남대, 한북대, 한성대, 한세대, 한신대, 한양대, 홍익대 **(101개 대학)**
인터넷접수 및 창구접수	가야대, 감리교신학대, 강릉대, 건동대, 건양대, 경남대, **경동대**, 경북외대, 경운대, 경원대, 경일대, 경주대, 고신대, 공주대, 관동대, 광주대, 광주여대, 그리스도대, 극동대, 금강대, 꽃동네현도사회복지대, 나사렛대, 남부대, 남서울대, 대구대, 대구예술대, 대구외대, 대구한의대, 대불대, 대신대, 대전대, 동서대, 동신대, 동양대, 루터대, 목원대, 목포가톨릭대, 목포대, 백석대, 부산교육대, 부산장신대, 상지대, 서남대, 서울기독대, 서울장신대, 선문대, 성공회대, 성민대, 세명대, 순천향대, 신경대, 신라대, 아세아연합신학대, 영남신학대, 영동대, 영산대, 예수대, 예원예술대, 용인대, 우석대, 우송대, 원광대, 위덕대, 을지대, 인제대, 인천가톨릭대, 전주대, 중부대, 진주산업대, 청운대, 초당대, 침례신학대, 칼빈대, 탐라대, 평택대, 한국국제대, 한국성서대, 한동대, 한라대, 한려대, 한밭대, 한서대, 한영신학대, 한일장신대, 한중대, 협성대, 호남대, 호남신학대, 호서대, 호원대 **(90개 대학)**
창구접수	광주가톨릭대, 대전가톨릭대, 대전신학대, 명신대, 수원가톨릭대, 영산선학대, 중앙승가대 **(7개 대학)**

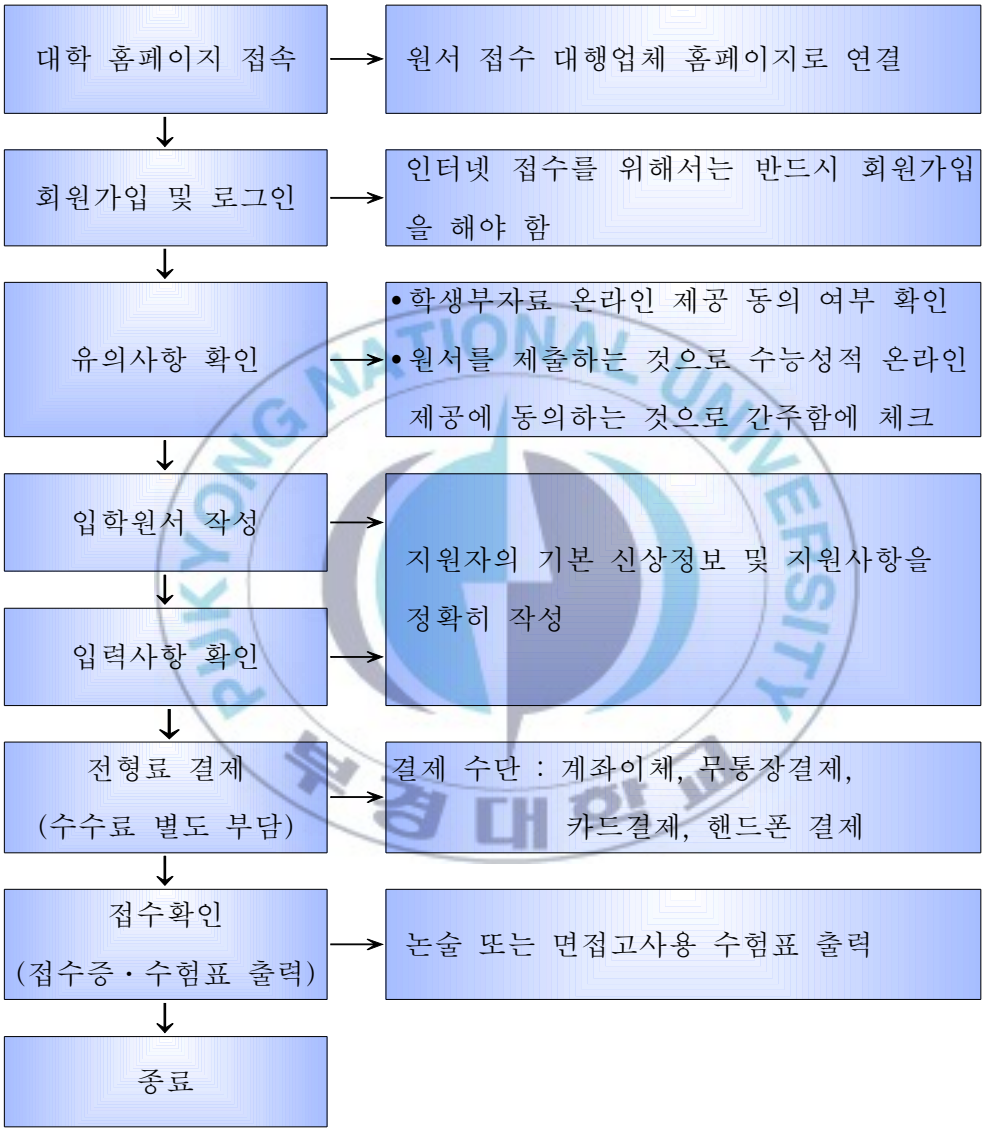
※ 밑줄 친 대학은 자체 원서접수시스템으로 원서접수하는 대학 임

[그림 1]은 현재 대부분 대학에서의 대행업체를 통한 인터넷 원서접수 업무 전체 흐름도이다. 계약 체결 → 원서 입력 및 전형료 납부 → 대학으로 원서접수자료 전송 → 원서접수자료 파기 순으로 진행 된다[8].



[그림 1] 인터넷 원서접수 업무 흐름도

[그림 2]는 해당 대학 지원자가 인터넷 원서접수 대행업체를 접속하여 원서를 작성하는 상세 절차도이다[8].



[그림 2] 지원자 인터넷 원서접수 상세 절차도

Ⅲ. 이론적 배경

1. 개인정보영향평가 제도

가. 개요

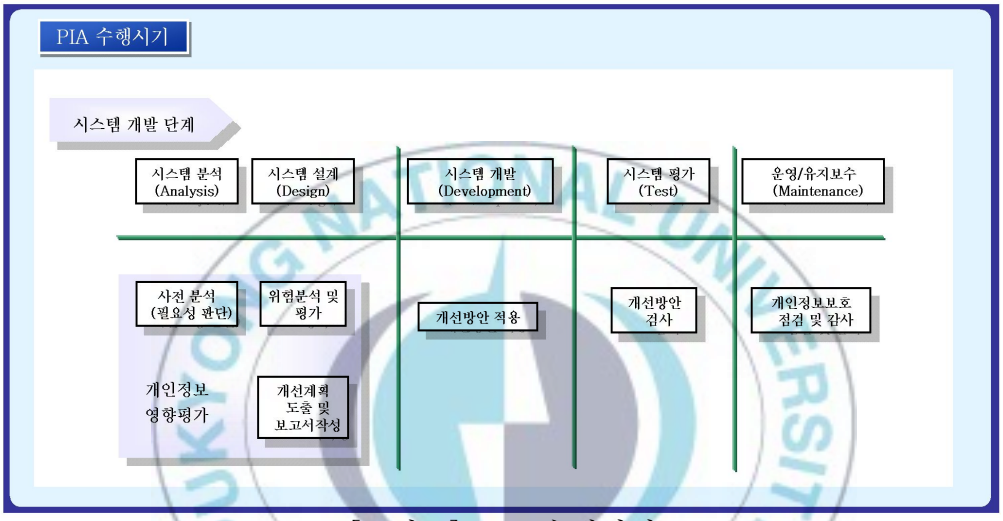
개인정보영향평가(PIA : Privacy Impact Assessment)란 정보시스템의 개발·운영 시 고객의 개인정보가 사업에 미칠 부정적 영향을 사전에 측정·분석하여 대책을 수립하는 일련의 과정으로써 개인정보 관련 법·제도 요구사항 준수 여부, 수집·저장·관리되는 고객 개인정보의 현황 및 위험분석을 통한 위험수준 도출, 고객의 개인정보 활용 시 발생 가능한 개인정보보호 대책 수립·적용, 고객의 개인정보 보호를 위한 제도적 장치(조직·역활·책임) 구축 등의 결과물을 도출한다[1][2].

새로운 시스템을 구축하거나, 기 시스템을 변경하는 경우에 발생할 수 있는 개인 정보 침해요인을 사전에 분석하여, 도입·구축 후의 조치보다 시행착오와 비용을 대폭 절감할 수 있다. 그러나 운영 중인 기존 시스템이라도 개인정보의 수집, 이용 및 관리상에 중대한 침해 위험이 발생할 가능성이 있다면 개인정보영향평가를 실시해 취약성을 진단하고 개선하는 것은 명백한 효과가 있다[12].

최근 개인정보보호 강화를 위한 법 제정 동향을 살펴보면 공공기관으로 제한된 '공공기관의 개인정보보호에 관한 법률'를 개정하기위하여 2009년 2월 행정안전부가 입법예고한 개인정보보호법은 그 적용 범위를 공공·민간 등 국가사회 전반으로 확대(제2조)하였고, 특히 개인정보 취급자에 대한 사전 규제가 가능한 개인정보영향평가를 의무화 한다(제31조)는 내용이 포함되어 있다[6].

나. 평가 시기

개인정보 영향평가는 새로운 시스템을 구축하는 경우에 발생할 수 있는 개인정보 침해 요인을 사전 분석하는 것이므로, 일반적으로 시스템 구축 전단계인 사업방향설정 및 업무 정의 단계, 시스템 제안 단계, 시스템의 예비설계 및 모형 설정 단계 등에서 수행 된다.



[그림 3] PIA 수행시기

다. 평가 대상 사업 범위

(1) 개인정보를 다량 보유•관리하는 정보시스템의 신규 구축 사업

(2) 신기술 또는 기존 기술의 통합으로 프라이버시 침해 가능성이 우려되는 기술을 사용하는 사업

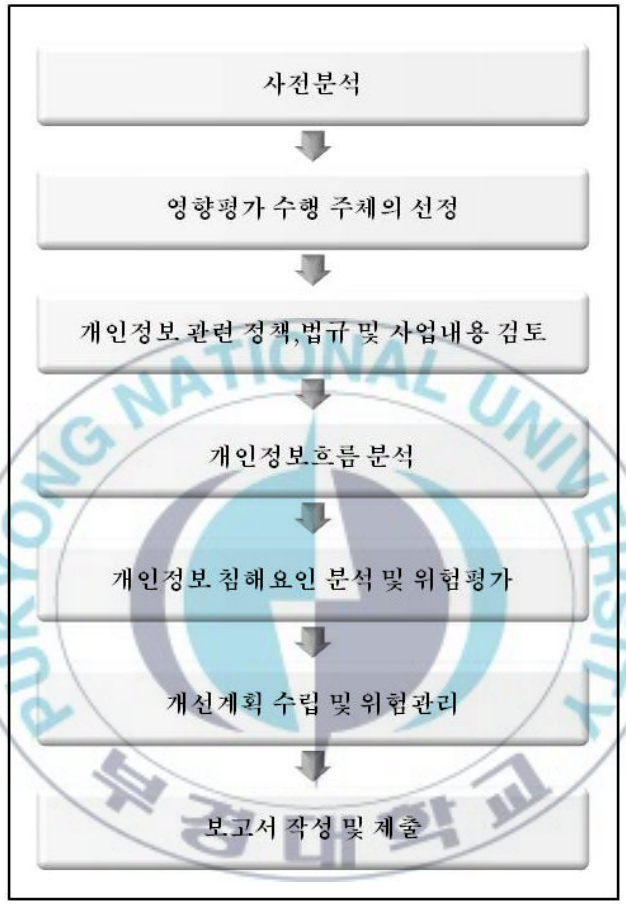
(3) 개인정보를 보유•관리하는 기존 정보시스템을 변경하는 사업

(4) 개인정보의 수집•이용•보관•파기 등 일련의 단계에서 중대한 개인정보 침해 위험이 발생할 가능성이 있는 사업

※ 다만, 개인정보의 수집•이용 등과 관련된 새로운 정보시스템의 구축이 경미한 변경인 경우에는 영향평가를 수행하지 않을 수 있다.

라. 평가 절차 및 방법

평가 절차는 [그림 4]과 같이 사전분석 등 7단계로 진행된다.



[그림 4] 개인정보영향평가 절차

(1) 사전분석

시행 또는 변경하고자 하는 사업에 대한 개인정보 영향평가의 필요성 여부를 결정하는 단계이다.

- 제공하는 서비스의 특성을 고려하여 당해 사업의 개인정보 침해 가능성을 기준으로 영향평가의 필요성을 검토

- 개인정보 영향평가의 필요성 여부를 검토할 경우에는 영향평가 수행 시 활용할 수 있는 자원(예산, 인력, 기간, 사업 수행부서•개발자 등 주요 이해관계자, 평가자료 확보의 용이성 등)을 고려하여야 한다.
- 사업 내용에 대한 전반적이고 대략적인 예비조사를 수행한 후 '사전분석 질의서'[표 3]의 질문사항 중 하나 이상에 해당하는 경우에는 개인정보 영향평가를 수행한다.

[표 3] 사전분석 질의서

질 문	Y/N
정보주체의 동의 여부를 불문하고 개인정보를 신규로 수집, 이용, 공개하거나 기존 개인정보의 수집, 이용, 공개 범위를 확대하는가?	
당해 사업의 수행을 위해 개인정보의 수집대상(또는 수집항목)이 확대되는가?	
당해 사업이 개인정보의 수집 방법을 기존에 정보주체로부터 직접 수집하는 방식에서 간접적으로 수집하는 방식으로 변경하는가?	
구축 시스템이 개인정보 DB에 대한 접근을 관리 또는 통제하기 위해 사용되는 보안체계에 중대한 변화를 초래하는가?	
영업양도•합병 등을 통해 개인정보의 일부 또는 전부가 타기관에 이전되는가?	
구축되는 시스템을 통해 다량의 개인정보를 신규로 수집하여 이를 이용•저장•관리하는가?	
당해 사업의 수행을 위해 개인정보를 수집•이용•저장•관리•파기하는 기존의 업무 수행 절차에 중대한 변경이 초래되는가?	
구축되는 시스템이 기업 내의 다른 시스템과의 연동을 통해 개인정보를 수집, 이용, 저장, 관리, 파기하는 업무 수행 절차상의 변동을 가져오는가?	
당해 사업의 수행을 위해 구축되는 시스템을 기업 내부의 개인정보 DB와 연동하는가?	
구축되는 시스템을 통해 그룹 내 계열사•자회사 등의 개인정보 DB가 통합•집중되는가?	

[표 3] 계 속

질문	Y/N
개인정보가 기입되어 있는 문서들을 전자적 시스템으로 전환하는 경우인가?	
구축되는 시스템을 통해 기존에 수집한 익명의 정보가 본인 확인이 가능한 정보 형태로 변경되는가?	
기존의 정보시스템에 신기술을 적용하는 등의 새로운 활용법을 채택함으로써 기존에 수집되거나 향후 수집될 정보가 본인 확인이 가능한 형태로 변경되는 등 시스템 관리상에 중대한 변화가 발생하는가?	
당해 사업의 수행을 위해 개인정보 수집 등의 업무처리 절차를 변경함으로써 기존에 예상치 못한 개인정보의 사용 또는 폐기를 야기하거나 본인 확인이 가능한 형태의 정보를 추가적으로 수집해야 하는 필요성이 있는가?	
당해 사업의 수행을 위해 본인 확인이 가능한 정보(금융정보, 재정정보 등)가 추가적으로 수집됨으로써 프라이버시의 침해 위험이 증가되는가?	
당해 사업의 수행을 위해 새로이 수집하는 개인정보 또는 기존의 개인정보 DB를 타 기관(제3자)과 공유하거나 연계하여 이용할 필요가 있는가?	
당해 사업의 수행을 위해 타 기관으로부터 개인정보를 제공받거나 타 기관의 개인정보 DB를 공유 또는 연계하여 이용할 필요가 있는가?	
당해 사업의 내용이 정보주체의 개인정보를 제3자에게 제공•공유 또는 판매하는 것을 예정하고 있는가?	
서비스 이용 과정에서 생성되는 정보를 기존에 수집한 개인정보와 결합함으로써 정보주체의 프라이버시에 영향을 미칠 수 있는 2차적 정보가 생성되는가?	
당해 사업의 수행을 위해 기존에 수집된 개인정보를 개인정보 수집 시 정보주체에게 고지한 수집목적 또는 이용목적 외로 사용할 가능성이 있는가?	
구축되는 시스템이 위치정보, RFID 등 신규 서비스를 제공하기 위한 것으로서 정보주체의 프라이버시 침해 문제가 발생할 가능성이 있다고 예측되는가?	
당해 사업 내용이 개인정보보호 관련 법령, 지침, 가이드라인 또는 기업 내부의 개인정보보호정책 등에 위반될 것으로 예측되는가?	

(2) 영향평가 수행 주체의 선정

사업 주관 부서, 개인정보 소유 부서, 시스템 운영부서, 개인정보관리책임자, 기업 내 최고의사결정권자 또는 외부 전문가 등으로 영향평가팀을 구성한다.

- 개인정보 영향평가를 수행하는 자는 정책·전략수립 지식, 기술·시스템 분석 지식, 위험평가 및 프라이버시 관련 지식, 운영 프로그램 및 사업계획에 대한 지식 등이 필요
- 개인정보 영향평가를 수행할 수 있는 능력이나 경험이 있는 내부 직원의 존재 여부 등을 파악하여 기업 자체적으로 평가팀을 구성할 것인지 외부 인력을 활용할 것인지 여부를 판단
- 평가팀을 구성한 후에는 개인정보관리책임자가 각각의 구성원에게 역할 및 책임 사항을 배분

[표 4] 영향평가팀 구성의 예

부서 / 수행 단계	사업주관부서	개인정보소유부서	시스템운영부서	개인정보관리책임자	최고의사결정자	기타
영향평가 필요성 검토	○			○		
개인정보 관련 정책, 법규 및 사업내용 검토	○	○		○		외부 전문가 참여 가능
개인정보 흐름 분석	○		○	○		
개인정보 침해 요인 및 위험평가	○		○	○		
개선계획 수립 및 위험관리	○	○	○	○		
보고서 작성 및 제출	○			○		
보고서 검토 및 사업지속 여부 판단					○	

(3) 개인정보 관련 정책, 법규 및 사업내용 검토

본격적인 영향평가 수행 이전에 현재 조직 내 개인정보 관련 주요 사항에 대한 검토를 수행하고 개인정보 영향평가 점검표를 사용하여 개인정보보호 현황을 파악한다.

- 개인정보 관련 내부 정책 및 조직 체계 검토
  - 조직 내의 개인정보 관리절차•방법 및 개인정보보호정책
  - 개인정보관리책임자 및 담당자의 역할과 책임 사항
  - 개인정보보호 관련 조직 체계 등
- 개인정보보호 관련 법령•지침 및 가이드라인 등 조사
  - 시행 또는 변경하고자 하는 사업에 적용되는 각종 개인정보보호 관련 법령•지침•가이드라인 및 기업 내부 규정 등에 대한 조사를 실시한다.
- 시행 또는 변경하고자 하는 사업 내용 검토
  - 「사업개요표」및「사업절차도」를 작성하여 시행 또는 변경하고자 하는 사업의 추진배경, 목표, 사업개요 및 당해 사업에 직•간접적으로 영향을 미치는 제반 사항에 대한 검토 및 분석을 한다.

(4) 개인정보흐름 분석

시행 또는 변경하고자 하는 사업에서 취급하는 개인정보 및 이를 포함하는 자산을 확인하고 개인정보의 흐름을 한 눈에 파악할 수 있도록 도표화하는 단계

- 개인정보 자산의 종류 및 처리단계, 개인정보에 대한 통제 및 접근권한, 제3자 제공 여부 등을 한눈에 볼 수 있도록 도표화
- 각종 보안장치를 포함한 정보시스템구조도 분석

(가) 개인정보의 종류

개발하려고 하는 시스템에서 활용하는 개인정보를 파악하고, 각 개인정보의 민감도 등을 고려하여 분류 한다. [표 5]는 정부지방혁신분권위원회에서 개인정보를 분류한 예이다[10].

[표 5] 개인정보 분류 예

분류		예시
속성정보		이름, 성별, 나이, 생년월일, 주민등록번호, 주소, 전화번호, 이메일주소, 혈액형, 신장, 체중, 사진, 지문, 기타 개인을 타인으로부터 식별하고 특성을 규정하는 정보
활동정보	가족, 출신 및 생활환경	결혼•이혼경력, 가족관계, 습관, 주거, 여행, 레저활동, 자선단체 가입 등
	학력 및 교육	학력, 출신학교, 성적, 학교생활, 기능, 자격 등
	고용 및 경력	취업, 사업경력, 구직•채용, 인사, 근태, 근무평정기록 등
	재산•신용•납세	수입, 임금, 투자, 지출, 채무, 보험, 재산, 연금, 보조금, 납세사실 등
	사회보장 및 행정서비스	정부로부터의 급부, 급여, 면허•특허•인가, 행정계약 등
	기타	기타 개인의 일상생활과 관련된 정보
민감정보		인종•민족, 국적, 정치적 성향, 종교, 노조•사회단체활동,보건•의료, 성생활, 장애기록, 행정처분사실, 전과•수형기록, 병역사항, 기타 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보

(나) 업무절차도 작성

다양한 배경 지식을 가진 담당 실무자들이 당해 사업과 개인정보의 흐름에 대한 이해를 쉽게 하고, 상호간의 의사소통을 원활하게 하기위해 계획된 사업의 주요 업무절차와 그에 따라 조직 내에서 개인정보가 어떻게 흘러가는지를 대략적으로 보여주는 도표인「업무절차도」를 작성한다.

(다) 개인정보 흐름표 작성

업무절차 단계에서 수집•이용•보관•파기되거나 제3자에게 제공되는 개인정보를 구체적으로 분석하기 위해「개인정보 흐름표」를 작성한다.
「개인정보 흐름표」의 작성 방법은 다음과 같다.

- 개인정보를 포함하고 있는 자산의 목록을 분류
- 업무절차 단계별로 수집•이용•보관•파기되거나 제3자에게 제공되는 개인정보를 기술
- 관련 담당자들의 역할 및 책임 기술
- 개인정보 자산의 접근 방법과 접근 권한에 대한 나열

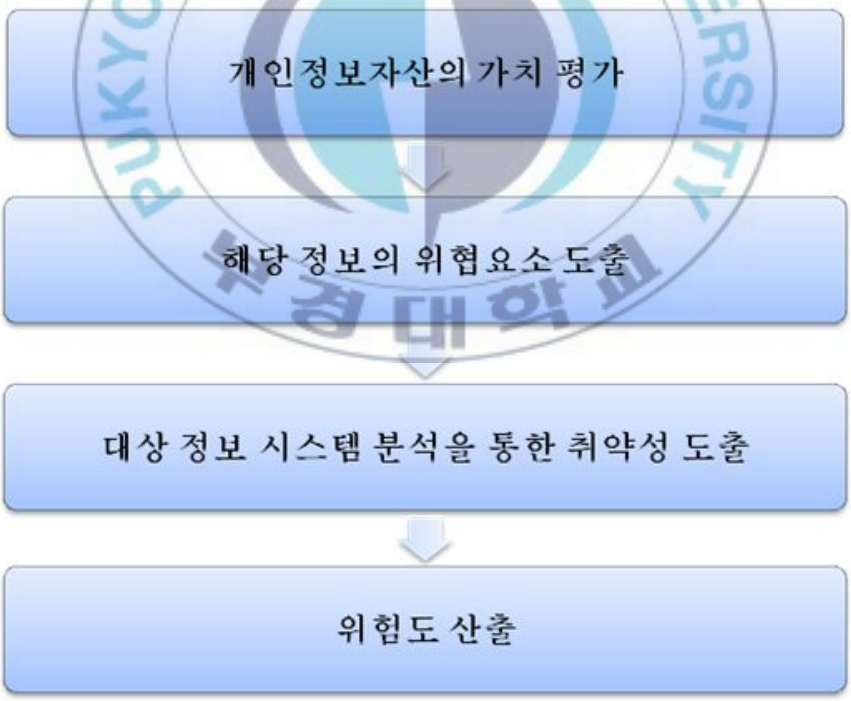
(라) 시스템 구조도(보안 메커니즘 포함) 작성

시스템 설계상 원천적으로 내재된 개인정보 자산의 위험을 분석하는데 활용하기 위해 시스템 구조도를 작성한다. 시스템 구조도는 보안 메커니즘을 포함하여야 하고, 이를 통하여 개인정보보호를 위한 기술적•물리적•관리적 보안 메커니즘의 타당성을 검토한다.

(5) 개인정보 침해요인 분석 및 위험평가

시행 또는 변경하고자 하는 사업과 관련된 주요 개인정보 자산에 대하여 주어진 영향평가 점검표를 바탕으로 침해요인을 분석하고 위험평가 하는 단계

- 영향평가팀은 영향평가 점검표를 활용하여 인터뷰 등의 방법으로 시행 또는 변경하고자 하는 사업의 개인정보 자산에 대한 가치를 평가하고 이에 대한 침해 요소를 파악한다.
- 영향평가 점검표의 결과를 기초로 위험평가를 실시하고, 위험도를 산출한 후 도출된 개인정보 침해 가능성이 있는 위험들에 대한 위험평가 결과표를 작성한다.



[그림 5] 침해요인 분석 및 위험평가 절차

[그림 4]는 개인정보 침해요인 분석 및 위험평가 시 한국정보보호진흥원에서 제시하는 위험 평가 방법 중 한 모델이다.

[그림 6] 위험평가방법 흐름도

(가) 개인정보자산의 가치평가

개인정보자산의 가치평가는 보호되어야하는 중요한 개인정보를 식별하고 각 자산의 중요도를 고려하여 유사한 자산을 그룹핑을 한 후 개인정보 자산 정보에 대하여 기밀성, 무결성, 가용성이 각각 결여되었을 경우 발생하는 영향 즉 민감도 평가를 실시한다. 평가결과는 유효성을 확보하기 위하여 현실과의 일치성 여부가 검토되어야 한다. [표 6] 및 [표 7]은 각각 위험평가 수행대상 개인정보자산 그룹핑 목록표 및 민감도 평가 목록표 예시이다.

[표 6] 개인정보 자산 그룹핑 목록표

개인정보자산그룹	개인정보자산	개인정보처리단계	소유자	접근방법	사용자(접근권한)	이용목적	제공처	보관처

[표 7] 개인정보 자산 민감도 평가 목록표

자산목록				민감도		
개인정보자산그룹	개인정보자산	.....	....	C (기밀성)	I (무결성)	A (가용성)

(나) 해당 정보의 위협요소 도출

“위협”이란 개인정보 자산의 기밀성, 무결성, 가용성을 위태롭게 할 수 있는 활동 또는 상황으로 정의할 수 있다. 대상 정보가 존재하는 물리적•논리적 공간의 특성을 파악하고 나타날 수 있는 위협요소를 출연 빈도와 함께 DB화하여 각 개인정보들과 맵핑한다.

위협요소가 이미 발생한 경우에는 이력정보를 바탕으로 통계적 분석을 통해 빈도를 측정하고, 아직 발생하지 않은 위협은 기존에 발생한 위협(예 : 고객 가입신청서 도난 빈도 등)과 비교하여 빈도를 추정한다. 이러한 위협 DB는 사고 및 침해 발생 시 주기적으로 갱신하여 항상 현실과 부합하도록 유지해야 한다.

(다) 대상 정보시스템 취약성 도출

“ 취약성”이란 위협이 개인정보 자산에 기밀성, 무결성, 가용성의 상실을 가져올 수 있게 하는 상황으로 정의되며, 일반적으로 대상 시스템의 취약성은 반드시 내재되어 있다. 취약성은 단순한 기술적인 요인에서부터 사회공학적인 요인에 이르기까지 다양하며, 특히 전자적 공간에서만 가질 수 있는 취약성은 정보 유통 및 이전 속도의 증가에 따른 위협과 관계가 있다.

실제로는 기술적 요인보다는 80% 이상이 접근 권한의 불확실성, 권한 관리자의 이해 부족, 오동작, 실수, 관리 절차의 미비, 규정•절차의 미준수 등 사람에 의한 것이 대부분을 차지하고 있다. 취약성은 위협 요소와 연계되어 하나의 시나리오를 이루기 때문에 이러한 시나리오가 현실에서 가능한 것인지를 검토해야 한다.

[표 8]은 위협/취약성 평가표 예시이다. “위협”이 “취약성”을 이용함으로 별도로 구분하지 않는다.

[표 8] 위협/취약성 평가 결과표

자산 평가							위협/취약성 평가	
자산목록				민감도				
개인정보 자산그룹	개인정보 자산	.....	....	C	I	A	위협/취약성	정도

(라) 위험도 산출

위험"이란 개인정보 자산에 대한 위협과 취약성으로 말미암아 자산에 발생할 수 있는 부정적 영향을 의미한다. 개인정보 자산의 민감도 평가 결과와 위협/취약성 평가 결과를 종합하여 기밀성, 무결성, 가용성 측면의 위험도를 산출한다.

위험도 산출(Risk Value) = 개인정보 자산의 민감도(Asset Value) + 위협의 정도(Threats Value) + 취약성의 정도(Vulnerability Value)

[표 9]는 위험도 산출 결과를 정리한 위험평가 결과표 예시이다

[표 9] 위험평가 결과표

자산 평가							위협/취약성 평가		위험 수준		
자산목록				민감도					Risk Value		
개인정보 자산그룹	개인정보 자산	.....	....	C	I	A	위협/ 취약성	정도	C	I	A

(6) 개선계획 수립 및 위험관리

보장수준(DoA)를 결정하고 그에 따라 관리되어야 할 위험에 대한 통제방안을 마련하는 단계 (DoA : 보장수준(Degree of Assurance)

- 사업수행 부서의 요구사항을 고려하여 개인정보 소유자, 사용자 및 기타 관련 주체간의 합의로 보장수준(DoA)을 결정
- 보장수준(DoA)에 따라 관리되어야 할 위험과 잔여위험을 분리하고 관리되어야 할 위험에 대한 통제 방안을 마련
- 위험에 대한 통제 방안 마련 과정에서 의견충돌이 생기는 경우에는 최고의사결정권자가 참여하여 의사결정을 할 수 있도록 함

(가) 보장수준(DoA) 결정

- 위험평가표에서 위험이 높은 것부터 순서대로 정리한 후 위험도가 가장 높은 것부터 각각 평가하여 조치를 취할 대상인지를 판단한다.
- 더 이상 조치를 취할 대상 위험이 아닌 수용할 만한 위험(Acceptable Risk)이라고 판단되면 그 정도를 보장수준(DoA: Degree of Assurance)으로 정의한다.

※ 보장수준(DoA)은 기관 환경에 따라 다양하게 정의될 수 있으며, 개인정보 보호를 강화하고자 하는 경우에는 보장수준(DoA)을 낮게 정의하면 된다.

(나) 위험평가 결과를 바탕으로 개선 계획 수립

- 위험 요소를 제거하거나 최소화할 수 있는 대처 방안을 마련한다.
- 위험 요소 해결을 위해 유사 사례에 대한 벤치마킹 등을 수행한다.
- 담당자(개인정보취급자)들이 취약 사항을 시정하기 위해 취해야 할

조치 사항과 책임 사항 등을 마련한다.

- 위험요소 제거 및 개선을 위한 총괄 계획표를 마련한다.

(7) 보고서 작성 및 제출

영향평가 보고서에는 사전 준비단계에서부터 위험관리까지 모든 절차의 내용과 결과를 정리하여 문서화하는 단계이다.

- 개인정보 사전영향평가 결과를 최종적으로 검토 또는 승인할 수 있는 관계 기관에 보고서를 제출하고, 영향평가의 결과를 웹 또는 출판의 형태로 일반에게 공개하여 일반의 의견을 수렴할 수 있도록 한다.
- 잔존 위험이나 이해관계자 간의 의견 충돌이 있는 경우에는 최고의사결정권자(CEO 등)를 토론에 참여시킴으로써 해당 사업의 중단•지속 여부 및 개인정보보호 정도에 대한 합의를 도출한다.
- 회의 결과를 통해 최종 개선안이 도출되면 시스템 구축에 반영

[표 10] 개인정보 영향평가보고서 작성 예시

1. 표지

- 날짜, 대상 사업명, 담당자, 연락처 등을 기입

2. 요약

- 영향평가에 대한 간략한 요약, 결론과 개선 사항을 요약된 형태로 기술

3. 목차

- 보고서의 주요 장과 절, 그리고 이들이 수록된 페이지 번호를 명시

4. 상세보고서

■ 개 요

- ● 사업 수행의 동기
- ● 조직구조 및 프라이버시 관리 절차 약술(보고절차)
- ● 영향평가의 범위 및 대상(제안서의 범위와 구체성에 따라 다를 수 있음)
- ● 참가자 및 역할과 권한에 대한 설명
- ● 개인정보 관련 법률과 정책
- ● 용어 설명

■ 사업의 개요 및 설명

■ 정보 흐름 분석

- ● 업무절차도 작성
- ● 개인정보 흐름표 작성
- ● 시스템 구조도 작성

■ 침해요인 분석

■ 위험 관리 계획(위험평가표, 개선 계획안)

■ 결과에 대한 보고 및 논의

마. 평가 사례

(1) 국외 사례

개인정보 영향평가는 개인정보보호 제도 가운데 선진적인 제도로 주요 국가에서 이미 도입하여 시행 중에 있다. 공공부문의 경우 법적 근거에 의해 의무적으로 시행하여 그 평가 결과를 공개하고 있으며, 민간부문의 경우 대부분 기업 자율로 시행하고 있다.

[표 11]은 미국,캐나다, 호주 및 뉴질랜드 평가사례이다[6].

[표 11] 외국 평가 사례

구분	미국	캐나다	호주 및 뉴질랜드
실시 근거	- '02년 전자정부법 - 관리예산처 프라이버시 영향평가 지침	- '02년 PIA지침	- 자율 시행
평가 대상	- 모든 정부기관 - 관련 업체 수행자	- 모든 정부기관	- 의무나 제한 없음
평가 주체	- 해당 정부 기관	- 해당 정부기관	- 해당 기관 자체 또는 외부 건설팅
평가 결과의 공개	- 기관 웹사이트, 기타 - 예산 요구 시 포함	- 인터넷, 기타	- 의무가 없어 공개되지 않는 경우가 많음

(2) 국내 사례

(가) 공공분야

공공분야에서의 개인정보영향평가 제도는 아직 도입 초기이다. '04년부터 개인정보영향평가에 대한 논의가 시작되어, 한국정보보호진흥원(KISA)을 통해 '05년에 지침이 마련됨에 따라 '07년 서울시, 외교부 및 교과부의 일부 시스템 구축에 영향평가제도를 적용하였고, '08년에 16개 공공사업에 개인정보영향평가를 실시하여 개선사항을 도출하였다[11].

(나) 민간분야

민간분야에서는 '기업의 개인정보영향평가 수행 가이드라인' 개발과 관련하여 '05년 이동통신 3사가 대리점·판매점을 대상으로 자체적으로 수행하였고 '05년 이동통신사 모바일RFID 시범서비스(2개) 사업에 대한 자체 영향평가를 실시하는 등 미미한 실정이다. [표 12]는 민간부문에서의 개인정보영향평가를 활성화 하기위하여 국내 최대의 개인정보를 보유하고 있어 유출되면 엄청난 피해가 예상되는 이동통신 3사에 대하여 2005년 실시한 개인정보영향평가 분석 결과이다[5].

- **개인정보 영향평가 제도 정착의 현실적인 문제점**
  - 평가제도에 대한 규제적 인식 및 자율 시행 노력의 부재
  - 명확한 기준이 없어 어떤 사업을 영향평가 실시 대상으로 해야 할지 판단이 어려움
  - 개인정보 영향평가을 위한 전문 인력 및 예산 부족 등이 있다
- **개인정보 영향평가 제도 활성화 방안**
  - 규제에 대한 타율적인 관점보다 개인정보 침해 RISK를 최소화한다

는 자율적 관점으로 인식 변화 필요

- 개인정보 영향평가 수행 지원을 위한 교육과정 개설 셋째, 개인정보 영향평가 법제화 등이 필요

[표 12] 이동통신 3사 개인정보영향평가 분석 결과

항목	분석 결과
사전 분석	사업 계획 및 구축 시 개인정보 침해요인 및 위험요소에 대한 사전검토를 개인정보보호 관련 법률에 부합하는 정책 및 내부지침에 따라 전담부서/담당자를 지정하여 시행하고 있으나, 실제적인 역할과 업무구분에 있어 미흡함
개인정보의 수집·이용·제공·공유	사업목적과 부합하는 정보만을 수집하고 있고, 개인정보의 임의적 사용을 통해 발생할 수 있는 위험요소에 대한 검토를 시행하고 있었으나, 내부사용이나 타부서 활용에 대한 감사가 없어 무단 사용에 대한 정확한 현황을 파악에 한계
개인정보 처리의 위탁 등	개인정보 위탁 계약서에 위탁 사실, 보호 관련 명시, 고객에게 위탁 사실 사전 고지, 무단 사용 벌칙 명시하고 있고, 위탁업체 직원 교육 을 주기적으로 실시하고 있으나 감사가 점검 수준이라 사전 예방 강화를 위한 상당한 보완이 필요
개인정보의 보유 및 파기	이용약관 및 내부지침이 명시되어 있고 계약 해지 시 별도 DB에 일정 기간 해지고객의 개인정보를 보관하여 파기하는 것으로 보이나, 위탁 업체로 부터의 수거는 잘 안 되고 있음
정보주체의 권리보장을 위한 조치	고객이 개인정보 열람·정정할 수 있고 개인정보보호방침 변경 시 이를 고지
개인정보보호를 위한 인적·물리적 보안 조치	개인정보 접근권한을 제한하여 비인가자로 인한 침해를 방지하고 있으며 백업시스템이나 인적 보안 강화를 위한 교육이 일반 보안교육수준이라 운영 및 담당자에 대한 세부 교육계획이 마련되어 있지 않음. 침해사고발생 시 사후보안 대책이 미흡하며, 시스템에 대한 점검은 이루어지나 감사는 시행되지 않았음

Ⅳ. 인터넷 원서접수 시스템에 대한 개인정보영향평가 수행

1. 개요

현재 대부분의 대학에서 인터넷 원서 접수 시스템이 불가피하게 다수의 개인정보를 다루고 있으므로 인터넷 상에 공개된 정보를 기반으로 개인정보영향평가를 모의 수행한다.

직접 해당 대행업체 및 대학의 주체 또는 위탁을 받아 수행하는 것이 아니므로 전반적이고 자세한 시스템에 대한 정보를 구하기 어려웠다. 따라서 정확하고 엄밀한 분석, 평가 및 개선 사항을 도출하기는 한계가 있기 때문에 시험적으로 수행한 영향평가임을 밝혀 둔다.

인터넷 원서 접수 시스템은 운영 중에 있고 개인정보 침해 가능성이 크므로 새로운 시스템 구축이나 시스템 변경 시 수행하는 사전분석 단계는 생략하고 영향평가 수행 주체는 본 연구 제안자가 수행하는 것으로 한다.

2. 개인정보 관련 정책, 법규 및 사업내용 검토

영향평가 수행이전에 대행업체의 개인정보보호 관련 법규, 조직 및 사업내용을 검토한다. 검토한 결과를 [표 13]에 나타내었다. 개인정보보호를 위한 정책은 각 회사마다 『개인정보취급방침』,『이용약관』등에 해당 법률에 근거하여 구체적으로 잘 작성되어 있으나 관련 법규에 행정안전부로 통합된 (구)정보통신부의 『개인정보취급방침』이 아직도 표기되어 있고 개인정보보호 전담인력(조직)에 대한 구체적인 권한 관리 세분화가 되어 있지 않아 이에 대한 인력보강 등의 조치가 필요할 것으로 보인다.

[표 13] 개인정보보호 관련 정책, 법규 및 사업내용 검토

대행업체 / 구분	A, B사 공통
법규	『정보통신망이용촉진 및 정보보호에 관한 법률』, (구)정보통신부의 『개인정보취급방침』
정책	『개인정보취급방침』,『이용약관』의 개인정보보호 조항
사업내용	인터넷 원서접수 대행
개인정보보호 전담인력(조직)	『개인정보취급방침』에 명시적인 전담부서가 없고 개인정보관리 책임자만 지정 되어 있음

3. 개인정보흐름 분석

대행업체에서 취급하는 원서접수와 관련된 개인정보 및 이를 포함하고 있는 자산을 분류하고, 개인정보 자산의 종류, 처리단계, 시스템 구조도, 통제 및 접근권한, 제3자에 제공여부 등을 분석한다. 개인정보보호를 위한 기술적 대책으로 [표 14]는 원서 작성 및 원서 접수를 위하여 반드시 필요한 회원 가입 시 업체별로 수집하는 개인정보 항목을 필수와 선택으로 구분하여 정리하였다. 사업 목적 달성에 필요한 최소한의 정보를 수집하는 것으로 볼 수 있으나 '생년월일' 등은 해당 목적에 부합하지 않으며 학교명, 학년, 반, 학생성적, 희망계열, 희망대학 등 가입 시 필수가 아닌 선택항목을 필수 항목인 것처럼 입력을 유도하는 부분은 개선되어야 할 것이다.

수집, 이용, 3자 제공 여부 등 각 단계별로 회원의 동의를 구하여 처리하고 있으며, 보유 기간 및 파기 절차를 구체적으로 기술되어 있다. 통제 및 접근 권한 대책이 개인정보 관련 담당자 등 최소한의 인원으로 제한하고 있

으나 이에 대한 내·외부 감사 실시 등 개선 방안이 필요한 것으로 보인다.

[표 14] 수집되는 개인정보 목록

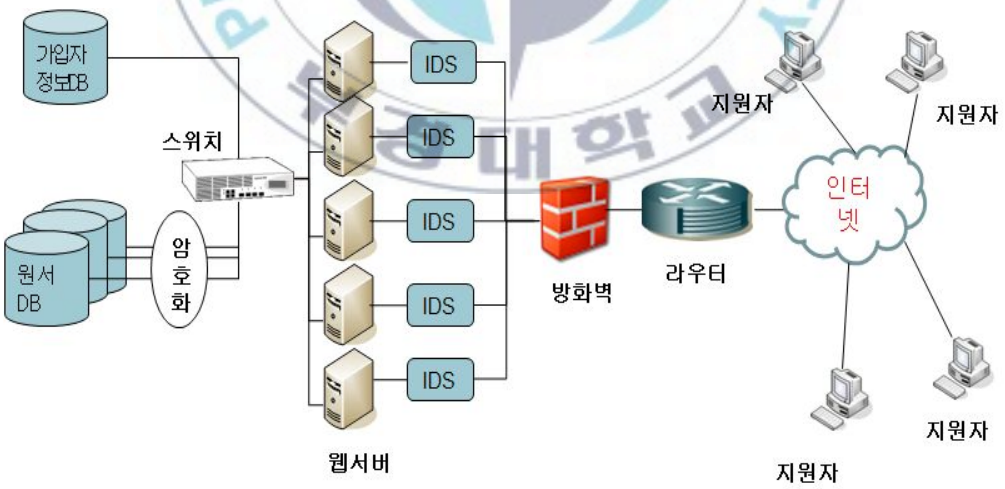
구분		항목	
		필수	선택
가입자 정보	A사	성명, 주민등록번호, 로그인ID, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, 생년월일, 회원 구분, 학교, 희망대학 ※만14세 미만자 : 법정대리인의 주민등록번호, 성명, 연락처	학년,반,희망계열,학생 성적
	B사	성명, 주민등록번호, 로그인ID, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, 생년월일 ※만14세 미만자 : 법정대리인의 주민등록번호, 성명, 연락처	회원구분,학교,학년,반, 희망계열,희망대학
원서접수정보		연락처, 학력사항, 성적, 보호자 관련 사항 등 대학(교)에서 접수와 전형에 필요로 하는 정보	

[표 15]은 개인정보 자산의 종류, 소유자, 접근 권한, 이용목적, 제3자 제공여부 및 보관장소 등을 조사한 결과이다.

[표 15] 개인정보 자산 종류, 접근 권한 및 제3자 제공여부

개인정보 자산	소유자	접근권한	이용목적	제공처	보관장소
가입자 정보 DB	대행업체	대행업체 담당자	가입고객 확인	제휴사	대행업체 서버
원서자료DB	해당대학	대행업체 담당자	원서접수	해당 대학	대행업체 서버

[그림 7]은 대행업체의 개인정보보호방침에 기재된 기술적 보호대책을 해석하여 재구성한 인터넷 원서접수 시스템 구성도(추정)이다[3][4]. 전형료 및 이용수수료 결재 시 입력하는 계좌번호, 신용카드번호 및 기타 관련 정보는 수집하지 않으므로 결재시스템 부분은 제외하였다. 중요 데이터는 별도의 보안기능을 통해 보호되고 있으며 각 웹서버 별로 침입탐지시스템(IDS: Intrusion Detection System)이 설치되어있고 방화벽이 외부로부터의 불법 침입을 차단하고 있음을 알 수 있다. 하지만 기술적 보호대책에 최신 보안기술을 적용한 웹방화벽, 침입방지시스템(IPS : Intrusion Prevention System), DOS공격 탐지/차단 시스템 등 최신 해킹 및 DOS공격을 대비한 장비에 대한 언급이 없어 설치가 되었다면 개인정보보호방침을 수정하여 알리는 것이 바람직하며 만일 없으면 차기 원서접수 전까지 설치하여 기존 보안시스템으로는 막을 수 없는 불법 공격에 대비하여야 할 것이다.



[그림 7] 인터넷 원서접수 시스템 구성도(추정)

4. 개인정보 침해요인 분석

개인정보 침해요인 분석 단계에서는 주요 개인정보 자산에 대하여 영향평가 점검표를 만들고 이를 바탕으로 침해 요인을 분석한다. 본 논문에서는 영향평가용 점검표를 작성하는 대신 한국정보보호진흥원의 '기업의 개인정보 영향평가 수행을 위한 가이드'에 있는 영향평가 기준(점검표)를 활용하여 점검을 실시하였다.

[표 16]은 작성한 영향평가 기준(점검표)을 요약한 영향평가 점검 및 분석 결과이다. 자세한 세부점검 항목은 생략하고 분석결과 나타난 문제점을 요약·기술하였다.

[표 16] 영향평가 점검 및 분석 결과 요약

점검 사항	분석 결과
정보화 사업 기획 점검	운영 중인 시스템이므로 생략
개인정보보호 체계 검토	개인정보취급방침 고지, 개인정보관리책임자 지정 등 관련 법률에 부합하지만 개인정보보호 전담부서/담당자별 업무 등의 구체적인 내용이 부족
개인정보 수집	목적에 필요한 최소한의 정보를 수집하는 것으로 보이나 '생년월일' 등은 목적이 분명치 않으며 선택항목을 입력하도록 유도
개인정보의 이용·제공·공유 등	이상 없음
개인정보처리 위탁 등	위탁업체에 대한 보안 교육 실시 여부 언급 없음
개인정보의 이용기간 및 파기	이상 없음
개인정보 기입서류 등의 보관 및 파기	이상 없음

[표 16] 계 속

점검 사항	분석 결과
개인정보 주체의 권리 보장	이상 없음
개인정보보호를 위한 기술적·관리적 조치 사항	접수 마감시간 대에 DOS공격등의 대량의 유해 패킷 유입 시 가용성 확보를 위한 차단 대책이 미흡
개인정보보호를 위한 인적 통제	비인가자에 대한 접근 제한이 되고 있으나 인가자에 대한 업무별 특성을 고려한 개인정보 접근 권한부여가 요구 됨
개인정보 침해사고 발생 시 사후 구제 체계	침해사고 발생 시 이를 감지하고 대응하는 사후 절차 등의 대책이 미흡

5. 위험평가

영향평가 기준(점검표)을 바탕으로 침해 요인 분석 후 드러난 침해요인에 대한 위험평가를 실시하고 위험평가표를 작성한다. 위험평가는 개인정보 유출 시 큰 피해가 우려 되는 원서접수정보에 대해서만 수행하였다.

[표 17]은 원서접수정보에 대한 민감도를 기밀성・무결성・가용성 측면에서 분석한 결과이다.

원서접수정보는 주민등록번호, 성적 등 학부모 및 지원자의 중요한 개인정보가 포함되어 있어 높은 기밀성이 요구되며, 접수마감 시간 직전에 지원자가 한꺼번에 접속하여 입력함으로 완벽한 무결성 및 고 가용성을 보장해야 한다.

[표 17] 개인정보 자산의 민감도

개인정보 자산	민감도		
	기밀성	무결성	가용성
원서접수정보	3	3	3

※민감도는 업체 신뢰도가 실추되는 정도를 표시

1 : 무시할만한 경우

2 : 약간의 손실이 있으나 복구가 가능한 경우

3 : 치명적인 손실 발생

원서접수정보는 위와 같이 민감도가 매우 높으므로 [표 18]에서는 예상되는 위협/취약성 내용들에 대한 위험도를 산출하였다.

[표 18] 위협/취약성 도출 및 위험도 산출

민감도			위협/취약성		위험도[2]		
기밀성	무결성	가용성	예상 내용	정도[3]	기밀성	무결성	가용성
3	3	3	해킹으로 인한 유출	2	7	7	7
			DOS공격으로 인한 서비스 중단	2	7	7	7
			대학에 원서접수정보를 온라인 전송할 경우	2	7	7	7
			접근권한 불확실성, 취급 부주의 등으로 내부 직원으로 인한 유출	1	5	5	5
			목적 외 이용	1	5	5	5

※ 위험도 산출 공식[4] = 민감도 + 위협/취약성 * 2

2) KISA의 기업의 개인정보 영향평가 수행을 위한 가이드의 위험도 산출(Risk Value)공식은 『민감도(Asset Value) + 위협의 정도(Threads Value) + 취약성의 정도(Vulnerability Value)』 이나 취약성은 위협요소와 연계되므로 위협과 취약성을 한번에 등급을 산정하여 2를 곱하였음

3)위협/취약성 정도: 3 반드시 발생 2 가능성 있음 1 가능성 희박

6. 개선계획 수립 및 위험관리

개선계획 수립 및 위험관리 단계에서는 보장수준(DOA: Degree of Assurance)을 결정한다. 더 이상 조치를 취할 대상 위험이 아닌 수용할 만한 위험이라고 판단되면 그 정도를 보장수준으로 정의한다. 보장수준이 높을수록 관리해야할 위험요소는 적어지므로 관리하는 측에서는 비용은 줄어든다.

[표 18]에서 예상되는 위협/취약성 내용들에 대하여 산출한 위험도를 대행업체 관점에서 볼 때 7미만은 수용할 만한 위험이라고 판단할 것으로 예상됨으로 보장수준은 7로 결정할 것으로 보여 진다. [표 19]은 대행업체가 수립할 것으로 예상되는 위험관리방안이다.

[표 19] 위험관리방안(대행업체)

위협/취약성		위험도			위험관리방안		
내용	정도	기밀성	무결성	가용성	검토의견	담당	완료 예정일
해킹으로 인한 유출	2	7	7	7	인터넷 접속점 및 서버존 앞단에 웹방화벽 각각 설치, DB보안솔루션 도입	시스템 운영 부서	차기 원서접수개시 전
DOS공격으로 인한 서비스 중단	2	7	7	7	Dos공격 탐지 및 차단솔루션 도입	시스템 운영 부서	차기 원서접수개시 전
대학에 원서접수 정보를 온라인 전송할 경우	2	7	7	7	전송 자료 암호화	시스템 운영 부서	차기 원서접수개시 전

다음으로 서비스 이용자로서 접수 주체나 대학 입장에서는 가능성이 희박하지만 내부 직원으로 인한 유출, 목적 외 이용 등에 대한 우려로 5정도의 보장수준을 요구할 것으로 간주된다.

[표 20]은 이용자 요구가 예상되는 위험관리방안이다.

[표 20] 위험관리방안(이용자 요구)

위협/취약성		위험도			위험관리방안		
내용	정도	기밀성	무결성	가용성	검토의견	담당	완료 예정일
접근권한 불확실성, 취급 부주의 등으로 내부 직원에 의한 유출	1	5	5	5	개인정보 취급자 별 접근권한 세분화 및 최소 권한 부여	시스템 운영 부서	차기 원서접수 개시 전
					국가 관련 기관에서 유출 여부 감사 실시	국가 관련 기관	
목적 외 이용	1	5	5	5	국가에서 통합 원서 접수 시스템 구축 또는 대학 별 시스템 구축	국가 관련 기관 및 대학	장기 사업

Ⅴ. 인터넷 원서접수 시스템에 대한 개인정보보호 방안

1. 기술적 대책

가. 보안시스템 고도화

침해요인 분석과정에서 도출된 기술적인 위협/취약성인 해킹으로 인한 유출, DOS공격으로 인한 서비스 중단 및 원서접수정보 전송 등을 관리하기위한 대책 즉 기밀성, 무결성, 가용성을 보장하기 위하여 기본적인 보안장비인 침입탐지 및 차단시스템 외에 웹방화벽, DB보안솔루션, 안티DDOS 장비를 설치하고, 정상 트래픽과 구분이 안 될 정도로 점점 지능화되고 있는 고도의 해킹 방지를 위하여 지속적으로 장비 및 인력을 고도화하여야 하며 원서자료 전송 시 암호화하여 접수 주체 외에는 내용을 알 수 없도록 기밀성을 보장 하여야 한다.

나. 가입 시 본인 확인 절차 다양화

주민등록번호 대체 수단을 이용하여 가입자가 원할 경우 주민등록번호를 남기지 않도록 하는 대체수단을 제공하여야 한다.

대체 수단 예시	- 아이핀(Internet Personal Identification Number) - 공인인증서 - 신용정보회사를 통한 본인 확인 서비스

다. 개인정보노출 차단 및 점검 시스템 운영

혹시 있을지 모를 게시판 등 홈페이지 상에서의 개인정보 노출 방지를 위하여 실시간으로 입력되는 모든 게시글 및 첨부파일에 있는 개인정보와기 저장되어 있는 방대한 자료에 대한 개인정보 노출 여부를 직접 모니터링 하는 것은 불가능에 가까우므로 자동으로 점검할 수 있는 개인정보 노출 차단 및 점검시스템을 도입하여 효율적으로 차단 및 점검하는 것이 필요하다.

2. 관리적 대책

접근권한 불확실성, 취급 부주의 등 대행업체 내부 직원에 의한 유출 방지를 위하여서는 개인정보 접근 및 관리 절차 수립·실천, 최소한의 개인정보 취급자 지정 및 취급자 별 접근권한을 세분화하여야 한다.

목적 외 이용을 방지하기 위하여 대행업체는 접수주체(본인, 학부모, 대학, 고교)가 아닌 전달자 역할이므로 원서접수정보를 직접 열람하여서는 안 될 것이다. 이를 위하여 정부에서는 원서접수시스템에 대한 실시간 모니터링, 로그분석 및 수시 감사 실시 등 여러 수단과 방법을 통해서 대행업체가 원서접수정보를 이용 할 수 없도록 하는 대책이 필요하다.

마지막으로 지원자 개인의 관리 대책으로는 가입 시 대행업체의 개인정보보호방침 사전 검토, iPIN 등 주민등록번호 대체수단을 활용하며 학교, PC방 등 개방된 환경에서 원서접수를 할 경우 접수 후에는 반드시 로그아웃을 하고 열린 모든 웹 브라우저의 창을 닫아주어야 한다.

Ⅵ. 결론

과거 대학에 직접 방문·접수하여 막대한 인력과 비용을 발생하였던 대학입학원서 업무가 인터넷과 전자상거래 기술의 발전으로 온라인 처리됨으로써 대단한 정보화 효과를 누리고 있다. 대행업체를 통한 인터넷 원서접수방식은 개인정보 유출, 추가 비용부담 등의 문제만 없다면 대학 및 지원자에게 모두 좋은 제도이다. 하지만, 지원자의 동의여부와는 상관없이 수익을 추구하는 제3자(대행업체)를 거쳐야만 대학에 원서접수가 되는 방식 외에 대학 자체 원서접수시스템 구축(대학 부담을 줄이기 위하여 정부의 대폭적인 예산지원이 필요), 우편접수, 접수 창구 운영 등 다양한 원서접수 방식을 제공하여 지원자가 자율적으로 선택할 수 있는 권리는 보장해야 할 것이다.

단기적 대책으로는 대행업체에서는 해킹 방지를 위하여 웹 방화벽, DB보안, 고도로 지능화한 Dos공격 탐지 및 차단솔루션 도입 등의 시스템 도입을 고려하여야 하고 대학 등 외부에 원서자료를 암호화하여 전송해야 할 것이며, 개인정보 취급자 별 접근권한 세분화 및 최소 권한 부여를 통한 관리적인 대책을 수립해야한다.

장기적인 대책으로는 국가에서 직접 통합 원서접수 시스템 구축·운영 또는 제도적인 보완을 통하여 대행업체에서의 개인정보 유출의 원천적인 방지를 위한 대책을 강구해야 할 것이다.

본 연구에서는 대학에서의 인터넷 원서접수 대행에 따른 개인정보 유출 가능성에 대한 문제점을 전국 대학 입시요강, 인터넷원서 접수 대행업체의 정보시스템, 개인정보 보호방침 및 이용약관을 분석하고 개인정보 영향평가 기법을 통하여 개인정보 위협 요소 도출 및 그에 따른 몇가지 개인정보 보호 대책을 제시하였다.

참 고 문 헌

[1] 한국정보보호진흥원, "개인정보영향평가(PIA)", 2007. 5.

[2] 한국정보보호진흥원, "기업의 개인정보 영향평가 수행을 위한 가이드", 2006. 1.

[3] (주)유웨이중앙교육 홈페이지, http://www.uway.com, 개인정보취급방침, 이용약관

[4] (주)진학사 홈페이지, http://apply.jinhak.com, 개인정보취급방침, 이용약관

[5] 안준모, 개인정보 영향평가 제도 최근 동향 및 활성화 방안, 한국정보보호진흥원, 2006. 12.

[6] 행정안전부, 개인정보보보법 제정법률안, 행정안전부 공고 제2008-115호, 2008.8.

[7] 행정자치부, 2007년 하반기 공공기관 홈페이지 개인정보 노출실태 점검 결과, 2008.1

[8] 2009학년도 전국 4년제 대학 입시 요강

[9] 공공기관의 개인정보보호에 관한 법률

[10] 권헌영, 전자정부시대 개인정보보호법제의 쟁점, 정보화정책 제11권 제3호, 2004년 가을

[11] 행정안전부, 2009년도 공공기관 개인정보 영향평가 추진계획, 2009.2.

[12] 이기혁, 윤재동, 민간 기업의 개인정보 유출위험에 대한 측정 방법과 그 사례에 대한 연구, 정보보호학회지, 2008.6.

감사의 글

늦은 나이에 할 수 있을까 하는 의구심으로 시작한 산업대학원 석사과정을 무사히 마치면서 지나간 시간들을 되돌아봅니다. 입학하여 같은 과 선배 김영주, 김정삼, 박성만, 박원옥, 서민성, 심혜인, 이옥란, 정현군 선생님과 동기 서미영 선생님, 후배 김무경, 김태현, 박봉준, 조혜정, 최은희 선생님들과 같이 수업을 받으면서 세미나 발표 등 서로를 도와가며 보낸 시간들이 생각납니다. LISIA연구실은 항상 연구하는 분위기가 정착되어 있어 논문을 작성하는데 자극제가 되었습니다. 퇴근 후 연구실에 가면 몸은 피곤하였지만 교수님과 연구실 학생들의 한결같은 성실한 모습에 동화되어 열중할 수 있었습니다. 같은 연구실에 있었던 것에 자부심을 느낍니다.

특히 저를 지도해주신 이경현 교수님 감사합니다. 능력 부족으로 논문 과제 선정 및 논문작성에 고민 할 때 애정 어린 지적과 관심으로 이끌어 주셨고, 바쁜 시간에도 불구하고 많은 시간을 할애하여 아낌없이 지도하여 주셨습니다.

논문 수정 시 상세하게 검토하여 마무리에 많은 도움을 주신 김창수 교수님, 신상욱 교수님 그리고 전산정보학과 교수님, 논문을 준비하면서 많은 도움 받았던 LISIA연구실 서철 선생님을 비롯한 학생들, 함께 다녔던 산업대학원 학생들, 직장 동료, 학교당국 등 모든 분들께 감사드립니다.

마지막으로 어려운 과정에서도 항상 미소를 잃지 않고 뒷바라지 해준 사랑스런 아내 김미경님과 커갈수록 믿음직한 두 아들 정상빈, 정상진에게 “사랑해요” & “고마워요”란 말을 전하고 싶습니다.

2009년 8월 정 갑 규