인터넷 입학원서 접수 시스템의 개인정보보호

정갑규*, 이경현**
*부경대학교 전산정보학과
**부경대학교 전자컴퓨터정보통신공학부
e-mail:jungkk@pknu.ac.kr

Privacy Protection for Internet-Based Real-Time Admission Application System

Kap-Kyu Jung*, Kyung-Hyune Rhee**
*Dept of Computer Information, Graduate School of Industry, Pukyong National University
**Div of Electronic, Computer and Telecommunication Engineering, Pukyong National University

요 약

본 논문에서는 인터넷 상에 공개된 정보를 기반으로 대부분 대학에서 대행업체에 위탁하고 있는 인터넷 원서접수 업무에 있어서 개인정보보호 문제점을 다룬다. 개인정보보호와 관련된 정책, 시스템 검토, 개인정보 흐름 분석, 개인정보침해요인 분석과 위험평가 및 개선 계획 도출 등 일련의 프로세스 관점에서 개인정보영향평가를 모의 수행함으로써 동 시스템이 가지고 있는 개인정보 관련 문제점 및 개선 방안을 도출한다.

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.

본 연구는 현재 대부분 대학에서 대행업체에 위탁하여 처리하고 있는 대학 입학원서 접수 업무를 개인정보영향평가제도 기법을 이용하여 분석하고 개인정보 보호방안을 제시하고자 한다.

Ⅱ. 인터넷 원서접수 시스템의 개인정보영향평가

1. 개인정보 영향평가 개요

개인정보영향평가[2]는 새로운 시스템을 구축하거나, 기시스템을 변경하는 경우에 발생할 수 있는 개인 정보 침해요인을 사전에 분석하는 것으로, 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.

따라서 본 연구에서는 현재 대부분의 대학에서 위탁하여 처리되고 있는 인터넷 원서 접수 시스템이 불가피하게 다수의 개인정보를 다루고 있으므로 인터넷 상에 공개된 정보를 기반으로 개인정보영향평가를 모의 수행한다.

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

2. 접수 시스템에 대한 개인정보 영향평가 수행

개인정보영향평가 절차는 ①사전분석 ⇒②영향평가 수행 주체의 선정 ⇒③개인정보 관련 정책,법규 및 사업내용 검토 ⇒④개인정보흐름 분석 ⇒⑤개인정보 침해요인 분석

---

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)

2)**개인정보영향평가(PIA: Privacy Impact Assessment)**

PIA란 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 개인정보 보호 대책 수립·적용, 고객의 개인정보 보호를 위한 제도적 장치(조직·역활·책임) 구축 등의 결과물을 도출한다.(KISA, 개인정보영향평가, 2007)

및 위험평가 ⇒⑥개선계획 수립 및 위험관리 ⇒⑦보고서 작성 및 제출 순으로 진행된다.

인터넷 원서 접수 시스템은 운영 중에 있어 사전분석 단계는 생략하고 영향평가 수행 주체는 본 연구 제안자가 수행하는 것으로 한다.

2.1 개인정보 관련 정책, 법규 및 사업내용 검토

본격적인 영향평가 수행이전에 대행업체의 개인정보보호 관련 법규, 조직 및 사업내용을 검토한다. <표 1>은 검토한 결과이다.

<표 1> 개인정보보호 관련 정책, 법규 및 사업내용 검토

구분 \ 대행업체	A, B사 공통
법규	『정보통신망이용촉진 및 정보보호에 관한 법률』, 『개인정보취급방침』
정책	『개인정보취급방침』, 『이용약관』의 개인정보보호 조항
사업내용	인터넷 원서접수 대행
개인정보보호 전담 인력(조직)	『개인정보취급방침』에 명시적인 전담부서가 없고 개인정보관리 책임자만 지정되어 있음

2.2 개인정보흐름 분석

개인정보 흐름분석 단계는 개인정보 자산의 종류, 처리 단계, 통제 및 접근권한, 제3자에 제공여부 등을 분석한다.

<표 2>는 업체별로 수집하는 개인정보 항목을 필수와 선택으로 구분하여 정리하였다

.

<표 2> 수집되는 개인정보 목록

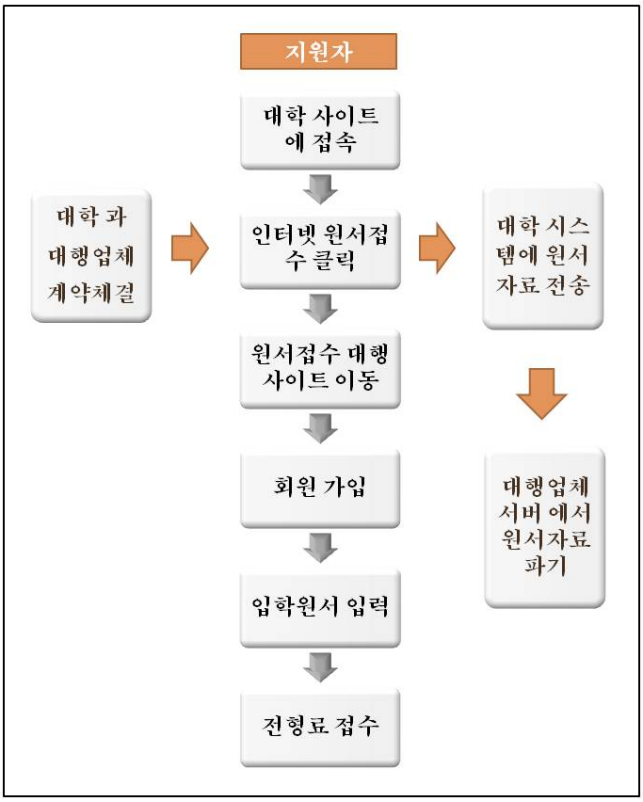
구분		항목	
		필수	선택
가입자정보	A사	성명, 주민등록번호, 로그인ID, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, 생년월일, 회원 구분, 학교, 희망대학 ※만14세 미만자 : 법정대리인의 주민등록번호, 성명, 연락처	학년,반,희망계열,학생성적
	B사	성명, 주민등록번호, 로그인ID, 비밀번호, 주소, 전화번호, 휴대폰번호, 이메일, 생년월일 ※만14세 미만자 : 법정대리인의 주민등록번호, 성명, 연락처	회원구분,학교,학년,반,희망계열,희망대학
원서접수정보		연락처, 학력사항, 성적, 보호자 관련 사항 등 대학(교)에서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

<표 3>은 개인정보 자산의 종류, 소유자, 접근 권한, 이용목적, 제3자 제공여부 및 보관장소 등을 조사하여 분석한 결과이다.

<표 3> 개인정보 자산 종류, 접근 권한 및 제3자 제공여부

개인정보 자산	소유자	접근권한	이용목적	제공처	보관장소
가입자 정보	대행업체	대행업체 담당자	가입고객 확인	제휴사	대행업체 서버
원서자료	해당대학	대행업체 담당자	원서접수	해당대학	대행업체 서버

[그림 1]은 현재 대부분 대학에서의 인터넷 원서접수 업무 흐름도이다. 계약체결 → 원서입력 → 전송 및 파기 순으로 진행된다



[그림 1] 인터넷 원서접수 업무 흐름도

2.3 개인정보 침해요인 분석

개인정보 침해요인 분석 단계에서는 주요 개인정보 자산에 대하여 영향평가 기준(점검표)을 바탕으로 침해 요인을 분석한다.

<표 4>는 작성한 영향평가 기준(점검표)을 요약한 영향평가 점검 및 분석 결과이다. 자세한 세부점검 항목은 생략하고 분석결과 나타난 문제점을 요약·기술하였다.

<표 4> 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
개인정보 주체의 권리 보장	이상 없음
개인정보보호를 위한 기술적·관리적 조치 사항	접수 마감시간에 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

2.4 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 5>는 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 5> 개인정보 자산의 민감도

개인정보 자산	민감도[3]		
	기밀성	무결성	가용성
원서접수정보	3	3	3

원서접수정보는 위와 같이 민감도가 매우 높으므로 <표 6>에서 예상되는 위협/취약성 내용들에 대한 위험도를 산출하였다.

<표 6> 위협/취약성 도출 및 위험도 산출

민감도			위협/취약성		위험도[5]		
기밀성	무결성	가용성	예상 내용	정도[4]	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 공식[5] = 민감도 + 위협/취약성 * 2

2.5 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.

<표 6>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 7>은 대행업체가 수립할 것으로 예상되는 위험관리방안이다.

3)민감도는 업체 신뢰도가 실추되는 정도를 표시
3 치명적인 손실 발생/ 2 약간의 손실이 있으나 복구가 가능한 경우/ 1 무시할만한 경우

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

5)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

<표 7> 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 원서접수 개시 전
DOS공격으로 인한 서비스 중단	2	7	7	7	Dos공격 탐지 및 차단솔루션 도입	〃	〃
대학에 원서접수정보를 온라인 전송할 경우	2	7	7	7	전송 자료 암호화	〃	〃

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 8>은 이용자 요구가 예상되는 위험관리방안이다.

<표 8> 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 원서접수 시스템 구축 또는 대학 별 시스템 구축	국가 관련 기관 및 대학	장기사업

Ⅲ. 결론

지난 2002년부터 시작된 인터넷 접수는 학생들의 이용 편의와 학교의 부담 감소라는 장점 때문에 2003년에 200만건을 넘었으며 2005년에 인터넷 접수 시스템 마비로 상당수 대학이 원서접수기간을 연장하는 초유의 사태도 발생하였다. 정시모집의 경우 몇 만명의 학생들이 원서를 제출하기 때문에 이를 감당할 수 있는 서버를 자체적으로 구축하기 힘들어 대부분 대학에서 인터넷 원서 접수를 대행업체에 맡기고 있다.

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 개인정보누출에 대한 불안은 항상 존재하고 있다.

이를 해소하기 위하여, 대행업체에서는 해킹 방지를 위하여 웹 방화벽, DB보안, 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 대책으로 대행업체에서 목적 외 이용할 가능성은 희박하나 이익을 추구하는 기업의 특성상 유혹이 있을 수 있으므로 제도적인 보완을 통하여 국가에서 통합 원서접수 시스템 구축·운영 또는 대행업체에서의 개인정보 유출의 원천적인 방지를 위한 대책을 강구해야 할 것이다.

결론적으로, 본 연구에서는 대학에서의 인터넷 원서접수 대행에 따른 개인정보 유출 가능성에 대한 문제점을 개인정보영향평가제도 기법을 이용하여 분석한 후 몇 가지 개인정보보호방안을 제시하였다.

참고문헌

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

[2] (주)유웨이중앙교육 홈페이지, http://www.uway.com

[3] (주)진학사 홈페이지, http://apply.jinhak.com

[4] 이기혁·윤재동, 민간 기업의 개인정보 유출 위험에 대한 측정 방법과 그 사례에 대한 연구, 정보보호학회지, 2008 .6.

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