DOI : 10.5392/JKCA.2011.11.3.084

정보시스템 감리에서 개인정보 영향평가를 통한 개인정보 보호

Personal Information Protection by Privacy Impact Assessment in Information System Audit

김희완*, 유재성**, 김동수***
삼육대학교 컴퓨터학부*, (주) IBK시스템**, (주)키삭***

Hee-Wan Kim(hwkim@syu.ac.kr)*, Jae-Sung Ryu(rjs3star@ibksystem.co.kr)**,
Dong-Soo Kim(dskim@kisac.co.kr)***

요약

정보 시스템 고도화로 인한 정보의 집적화, 대량화가 점차 확대됨에 따라 개인 정보의 유출 가능성은 날로 높아지고 있다. 이에 따라 개인정보 침해 요소를 사전에 분석하고 최소화 할 수 있는 개인정보 영향평가(PIA)의 필요성이 대두 되고 있다. 그러나, 대부분의 정보시스템 감리에서 시스템 아키텍쳐 영역의 물리적, 관리적, 기술적 보안 항목을 감리하여 일반적인 항목만을 체크하고 있어서 실질적인 개인정보보호를 위한 감리는 제대로 이루어 지지 않고 있다. 이에 따라 본 논문에서는 개인정보 침해를 사전에 최소화하기 위해 개인정보영향을 평가하고 그에 따른 개인정보보호 감리 절차 및 방법을 제시하였다. 본 논문에서 제시한 방법을 프로젝트에 적용한 결과 개인정보 보호를 위한 개선사항이 도출되었음을 확인할 수 있었다.

■ 중심어 : | 개인정보영향평가 | 개인정보보호 | 정보보호 감리 |

Abstract

As the integrated and large-scale information is extended due to an advanced information system, a possibility of leaking out privacy increases as the time passes by. As a result, the necessity of using a privacy impact assessment (PIA) is emphasized because it can analyze and minimize the element of invasion of privacy. However, an essential audit for personal information protection is not fulfilled because most of the information system audit supervises over physical, managerial, and technical security items of system architecture area so that general items are the only things being checked. Consequently, this paper proposes that in order to minimize the invasion of personal information, the privacy impact assessment should be done. It also presents a procedure and method of personal information protection audit according to the result of the assessment. After applying the suggested method to two projects, it was confirmed that the improvements for protecting personal information were drawn from this paper.

■ keyword : | Privacy Impact Assessment | Personal Information Protection | Information Protection Audit |

I. 서 론

개인정보는 과거부터 다양한 형태로 존재하고 있으며 최근 들어 세상의 이목이 더욱 집중되고 있다. 이는 현대 자본주의의 발전, 시민 사회의 성장, IT 기술의 눈부신 진보에 기인한다. 현대의 기업들은 고객 정보가

접수번호 : #110207-003
접수일자 : 2011년 02월 07일
심사완료일 : 2011년 03월 08일
교신저자 : 김희완, e-mail : hwkim@syu.ac.kr

기업 활동의 중요 요소라는 것을 알게 되었으며 많은 관심을 기울이게 되었다. 국민은 국가와 기업에 의해 자신들의 사생활이 쉽게 감시 당할 수 있다는 사실을 알게 되었으며 이러한 침해 위험성은 자신의 개인정보와 프라이버시에 대한 침해가 그 어느 시대보다 높은 우려감을 나타내게 되었다. 또한 급격히 발전하는 새로운 유비쿼터스 기술은 특정영역이 아닌 사회 전반에 급속도로 파급되어지고 정보 유통이 점차 확대되고 있어 개인정보의 유출 가능성도 그만큼 증대하고 있다.

개인정보를 제3자에게 제공 또는 자체 보관 할 경우 개인정보영향 평가를 통해 침해요소를 사전에 점검해야 하나 본 연구의 설문 및 선행논문 확인 결과 개인정보 침해요소를 사전 평가하고 권고하는 감리 결과는 찾아보기 힘든 실정이며 대부분 시스템 아키텍처 영역의 물리적, 관리적, 기술적 일반적인 보안 항목을 감리하고 있으며 범위도 너무나 폭 넓게 분포되어 실질적인 개인정보보호를 위한 감리는 제대로 이루어지지 않고 있다.

따라서 본 논문에서는 개인정보 침해를 사전에 최소화하기 위해 정보시스템 분석 및 설계단계에 개인정보 영향을 평가하고 그에 따른 개인정보보호 감리 절차 및 방법을 구축하여 개인정보보호 방법을 제시하였다.

II. 관련 연구 및 개인정보보호 영향평가

1. 관련 연구

현재 「공공기관의 개인정보보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「보건의료기본법」, 「의료법」, 「교육기본법」 등 개인정보의 처리를 규율 하는 개별 이법들이 존재하나, 이러한 개별 법률들로는 나날이 발전하는 정보통신기술에 의한 새로운 개인정보침해 상황에 대해 대다수의 공공기관이 모든 법에 대응하기 어려운 실정이다[1].

또한, 전자정보 고도화에 따른 전자적 행정서비스 활성화 및 효율적 업무수행을 위한 정보 공동이용의 확산과 정보 집적과 통합 처리가 가능해짐에 따라 공공기관에서 수집·보유하고 있는 개인정보에 대한 체계적이고 안전한 보호관리의 필요성이 강조되고 있다.

선행논문의 경우「개인정보보호 측면에서의 보안감리 방법에 관한 연구」[2], 「 차세대 전자정부서비스의 개인정보보호 아키텍처 설계 방안에 관한 연구」[3] 등 정보 시스템 운영 시 개인정보 유출에 대한 보안감리 방법을 ISO27001, ISMS, 개인정보 아키텍처 프레임워크를 이용하여 개인정보 수집·이용·파기·보관 감리방법을 제시 했으나, 본 논문에서는 개인정보보호를 위한 감리 절차 및 방법을 구축하여 개인정보보호 방법을 제시하고자 한다.

2. 개인정보보호 영향평가(PIA : Privacy Impact Assessment) 프로세스

2.1 개인정보보호 영향평가 개요

개인정보보호 영향평가(PIA)는 새로운 정보시스템 도입이나 개인정보 수집에 앞서 시스템의 구축과 운영이 고객 및 국민의 프라이버시에 미치는 영향을 평가하는 체계적인 절차를 의미한다. 미국의 「전자정부법」(e-Government Act of 2002)에서는 IT도입 시 반드시 고려해야 할 사항으로 명시 할 만큼 그 주요성이 커지고 있으나 아직 방법론이 크게 발전되어 있지는 않다. 캐나다는 공공 부문과 민간부분으로 구분되어 PIA를 실시할 것을 법제화하고 있다. 고객이나 국민의 프라이버시권을 보호하기 위해 프라이버시 법률과의 부합성과 잠재적인 프라이버시 위험을 관리하는 것을 도와주는 역할을 한다[2][4].

PIA 수행시기는 [그림 1][5]과 같이 시스템 소유자와 개발자가 개발의 초기 단계부터 프라이버시를 평가하도록 설계되어 있으며 PIA의 실시시기는 정보시스템 개발 초기 단계인 요구사항 분석 시부터 시스템 설계 등의 기획기간에 최초로 실시되며 시스템 개발주기(Life Cycle)의 전 과정에서 실시된다[6].

PIA의 수행주체는 시스템 소유자(Owner) 및 개발자(Developer)로서 시스템 소유자는 정보의 소유자와 일치한다. 또한 개발자는 해당정보자산에 미치는 위협요소와 취약성의 발생 가능성 및 정보를 평가한다.

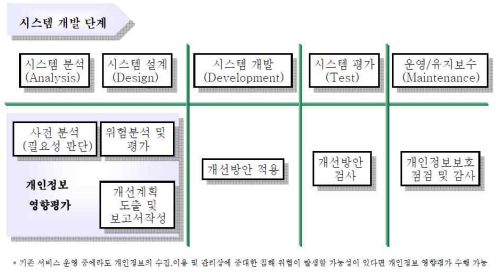

그림 1. 정보시스템 개발 단계별 PIA 수행시기

2.2 개인정보 영향 평가 절차

개인정보영향평가는 총 7영역으로 구성되어 있으며, 영역별 절차에 대한 내용은 [그림 2]와 같다[5].

그림 2. 개인정보 영향평가 절차

2.2.1 사전분석

개인정보 영향 평가 절차 중 사전분석 분석을 통해 시행 또는 변경하고자 하는 사업에 대한 개인정보 영향평가의 필요성 여부를 결정하고 제공하는 서비스의 특성을 고려하여 당해 사업의 개인정보 침해 가능성을 기준으로 영향평가의 필요성을 검토해야 한다.

2.2.2 영향평가 수행 주체의 선정

내부 인력 혹은 외부 인력을 활용하여 개인정보 영향평가를 수행할 평가팀을 구성해야 하며 개인정보 영향평가를 수행하는 자는 정책·전략수립 지식, 기술·시스템 분석 지식, 위험평가 및 프라이버시 관련 지식, 운영 프로그램 및 사업계획 지식 등이 필요하며 개인정보 영향평가를 수행할 수 있는 능력이나 경험이 있는 내부 직원의 존재 여부 등을 파악하여 자체 평가팀을 구성할 것인지 외부 인력을 활용할 것인지 여부를 판단해야 하며 영향 평가팀을 구성한 후 영향평가 수행에 대한 총책임자를 선정하고 구성원에게 역할 및 책임사항을 배분할 수 있다[7].

2.2.3 개인정보 관련 정책, 법규 및 사업내용 검토

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

- ○ 개인정보 관련 내부 정책 및 조직 체계 검토
  - 현재 조직 내의 개인정보관리 절차·방법 및 개인정보보호정책
  - 개인정보관리책임자 및 담당자의 역할과 책임
  - 개인정보 관련 조직 체계 등
- ○ 개인정보 관련 법률·지침 및 가이드라인 등 조사
  - 시행 또는 변경하고자 하는 사업에 적용되는 각종 개인정보보호 관련 법률·지침·가이드라인 및 기관 내부 규정 등에 대한 조사를 실시
- ○ 시행 또는 변경하고자 하는 사업 내용 검토
  - 시행 또는 변경하고자 하는 사업이 구체적으로 어떠한 방법을 통하여 개인정보를 수집·이용·보관·파기 등의 업무를 수행하는지 확인
- ○ 개인정보 영향평가의 시행 대상 사업이 개인정보 이용, 저장, 보관, 파기시 취약한 부분과 위협이 될 만한 사항을 파악하기 위해 개인정보 영향평가 점검표의 작성 및 회수를 통해 개인정보보호 현황을 파악한다.
- ○ 정보화 사업기획 점검, 개인정보 수집 • 이용 • 제공, 개인정보 처리 위탁, 개인정보의 이용기간 및 파기, 권리보장, 기술적 • 관리적 조치사항의 7개 영역으로 나뉘어진다[8].

2.2.4 개인정보 흐름 분석

대상 사업에서 취급하는 개인정보 및 이를 포함하는 자산을 확인하고 개인정보의 흐름을 한 눈에 파악할 수 있도록 도표화 할 수 있으며 시행 또는 변경 하고자 하는 사업에서 취급하는 개인정보 및 이를 포함하고 있는 자산을 확인하고 개인정보 자산의 종류 및 처리단계, 개인정보에 대한 통제 및 접근권한, 제3자 제공 여부 등을 한눈에 볼 수 있도록 도표화해야 하며 각종 보안장치를 포함한 정보시스템구조도 만들 수 있다.

○ 개인정보의 분류
- 수집하는 개인정보를 종류별로 분류

○ 업무 프로세스 작성
- 다양한 배경지식을 가진 담당 실무자들이 사업과 개인정보의 흐름에 대한 이해를 쉽게 하고, 의사소통을 원활

○ 개인정보 흐름 분석
- 각 업무절차 단계에서 수집·이용·보관·파기 및 제3자에게 제공되는 개인정보를 분석

○ 시스템 구조도(보안 메커니즘 포함) 분석
- 시스템 설계상 원천적으로 내재된 개인정보 자산의 위험을 분석 활용하기 위한 시스템 구조도
- 시스템 구조도는 보안 메커니즘을 포함하여야 하고, 이를 통하여 개인정보보호를 위한 기술적•물리적•관리적 보안 메커니즘의 타당성 검토

2.2.5 개인정보 침해요인 분석 및 위험 평가

시행 또는 변경하고자 하는 사업과 관련된 주요 개인정보자산에 대하여 주어진 영향평가 기준을 바탕으로 침해요인을 분석하며 영향평가 기준에 의해 침해요인에 대한 위험평가를 실시하고 위험평가표를 작성한다[8].

○ 개인정보 자산의 식별
- 개인정보를 포함하고 있는 모든 자산 목록을 작성하는 단계로서 자산 목록 양식을 작성한 후 자산관련 부서들로부터 자산 목록을 수령

○ 자산 그룹핑
- 각 자산의 중요도를 고려하여 그룹핑
- 자산의 소유자(Owner)가 그룹핑을 실시

○ 개인정보 자산의 민감도 평가
- 개인정보 자산의 민감도는 정보의 기밀성(C), 무결성(I), 가용성(A)이 결여되었을 경우에 발생하는 민감도(Impact)로 정의되며, 개인정보가 유출되어 접근권한이 없는 사람이 정보를 열람했을 경우 발생하는 영향의 잠재 정도를 의미
- 평가는 해당 정보의 소유자만이 가능하며, 평가는 사전에 등급과 각 등급의 판단기준을 명시
- 평가 결과는 유효성(Effectiveness)을 확보하기 위하여 현실과의 일치성을 검토

○ 개인정보 자산의 위협요소 도출
- 대상 정보가 존재하는 물리적·논리적 공간의 특성을 파악하고 출연할 수 있는 위협요소를 출연빈도와 함께 DB화하여 각 개인정보들과 매핑
- 위협요소가 이미 발생한 경우 이력 정보를 바탕으로 통계적 분석을 통하여 빈도를 측정하고, 아직 발생하지 않은 위협은 기존 발생 위협과 비교하여 빈도를 추정

○ 개인정보 자산의 취약성 도출
- 취약성은 단순한 기술적인 요인에서부터 사회공학적인 요인에 이르기까지 다양하며, 특히 전자적 공간에서만 가질 수 있는 취약성은 정보유통 및 이전 속도의 증가에 따른 위협과 관계
- 기술적 요인보다는 80% 이상이 접근권한의 불확실성, 권한 관리자의 이해부족, 오동작, 실수, 관리 절차의 미비, 규정·절차의 미 준수 등 사람에 의한 것이 대부분을 차지
- 취약성은 위협요소와 연계되어 하나의 시나리오를 이루기 때문에 이러한 시나리오가 현실에서 가능한 것인지를 검토

○ 위험도 산출
- 위험이란 개인정보 자산에 대한 위협과 취약성으로 말미암아 자산에 발생할 수 있는 부정적 영향
- 개인정보 자산의 민감도와 위협의 정도, 취약성의 정도를 평가하여 위험도를 산출

※ 위험도 산출(Risk Value) = 개인정보 자산의 민감도(Asset Value) + 위협의 정도(Threats Value) + 취약성의 정도(Vulnerability Value)[6]

○ 위험 평가표 작성
- 영향평가팀은 상기의 위험평가 방법에 따른 평가 결과를 기초로 최종 위험 평가표를 작성

2.2.6 개선계획 수립 및 위험관리

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

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

○ 개선계획 수립
- 위험 요소를 제거/최소화할 수 있는 대처 방안
- 위험 요소 해결을 위해 유사 사례의 벤치마킹
- 담당자들이 취약 사항을 시정하기 위해 취해야 할 조치 사항과 책임 사항 등을 마련
- 위험요소 제거 및 개선을 위한 총괄계획표 마련

2.2.7 보고서 작성 및 제출

영향평가의 사전 준비 단계에서부터 프로젝트 개요 및 위험관리까지 모든 절차의 내용과 결과를 정리하여 문서화 한다. 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 해야 하며 잔존 위험이나 관계자들의 의사충돌이 있는 경우 최종 의사결정자를 토론에 참여시킴으로써 사업수행 및 프라이버시에 대한 합의 도출 및 최종적 의사결정 수행한다. 회의 결과를 통해 최종 개선안이 도출되면 시스템 구축 및 변경 단계에 반영해야 한다[8].

3. 개인정보보호 감리 프로세스

3.1 정보시스템 개발 단계별 보안감리 요구사항

새로운 정보시스템을 개발할 때, 개발 단계별로 정보보호에 관한 제반 문제를 분석, 평가하고 개선사항을 도출하여 개발시스템에 반영함으로써, 정보시스템의 개발 이후 발생할 수 있는 문제점들을 사전에 식별하여 예방 할 수 있으며, 시스템의 안전성과 신뢰성을 보장할 수 있게 된다. 개발 보안감리는 4단계로 구분된 각각의 개발 단계별 정보보호 활동이 적절하게 이루어지고 있는지 점검하게 된다.

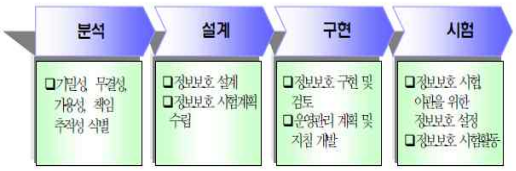

그림 3. 정보시스템 개발 보안 감리

분석단계에서 정보보호 요구사항은 기밀성, 무결성, 가용성, 책임 추적성 등의 관점에서 도출된다. 기밀성 요구사항은 정보시스템 내 비밀정보 분류, 정보시스템 기능의 제한 등을 포함한다. 무결성 요구사항은 정보시스템 내 정보를 변경할 수 있는 개인/업무 식별, 정보시스템 자체의 무결성, 정보시스템의 변경 기능에서의 무결성 보장 등을 포함한다. 가용성 요구사항은 모든 구성요소의 가용성 요구사항을 식별할 필요가 있으며, 정보시스템 구성 요소간의 의존성 및 상호작용을 파악하고 네트워크 등 인프라의 가용성 요구사항을 식별해야 한다. 책임 추적성 요구사항은 사용자 식별 및 인증과 정보보호 사고 조사 시 필요한 정보를 제공하기 위해 감사에 대한 요구사항을 포함한다.

분석, 설계, 구현, 시험단계의 개발보안 및 감리 요구사항 및 활동 / PIA 절차를 이용하여 [표 1]과 같이 프로젝트 / 정보보호 / 개인정보활동 간의 비교 분석 하였다[7][9][10].

표 1. 프로젝트 / 정보보호 / 개인정보보호 연관관계

개발 단계	프로젝트 주요활동	정보보호 활동	개인정보보호
분석	-프로젝트 수행계획 수립, 환경분석 -업무환경분석 -정보시스템의 요구사항 분석 -응용시스템/데이터 현황 분석 -IT 인프라 현황분석 -IT 관리 현황분석	-프로젝트 수행계획 내 정보보호 반영 -시스템 개요 식별 -정보보호 요구사항 분석 -위험평가 -정보보호 대책 선택 -정보보호 계획 수립	-개인정보보호 필요성 분석 -개인정보 관련정책 및 법규 / 사업내용 검토 -개인정보 침해요인 분석 위험 평가 -개인정보 개선계획 수립 및 위험관리
설계	- 기본 설계 ·IT인프라 아키텍처 ·응용/데이터 아키텍처 ·IT관리 아키텍처 -상세설계 -시험계획 수립	-정보보호 아키텍처 개발 ·IT 인프라 보안 ·응용/데이터 보안 -정보보호 시험계획 수립	-개인정보 아키텍처 개발 ·개인정보 인프라 보안 ·개인정보 응용/데이터 보안 -개인정보보호 시험계획
구현	-하드웨어/S/W 도입 -코딩 및 단위 시험 -교육/훈련 계획 수립 -운영계획 수립	-정보보호 솔루션 도입 -정보보호 모듈 개발 -정보보호 교육/훈련 계획 수립 -정보보호 운영계획 및 지침 수립	-개인정보보호 솔루션 도입 -개인정보보호 모듈 개발 -개인정보 교육계획 수립 -개인정보 운영계획 및 지침 수립
시험	-통합 시험 -인수 시험 -평가 및 승인	-계층별 정보보호 취약성 시험 -침투시험 -정보보호 평가/승인	-개인정보 취약성 시험 -평가 및 승인

3.2 개인정보보호 점검항목

구체적인 개인정보보호 세부 점검항목을 정립하기 위해서 ISMS[11], ISO27001[12], 정보시스템 구축가이드[13] 등 정보시스템 도입 및 개발 단계 점검 프로세스의 비교 분석을 통해 최적의 개인정보보호 감리 점검항목 요소를 도출하고자 한다.

3.2.1 정보보호관리체계(ISMS) 분석

정보보호관리체계에서는 정보보호에 관련된 위험을 통제하기 위한 대책을 수립하고 관리하는 체계이다. 인증심사기준에서는 15개 통제분야에 대하여 120개 통제사항을 제시하고 있으며, 아래 [표 2]와 같다[14].

표 2. ISMS 통제분야별 정의

Domain	항목수	분야별 정의
정보보호 정책	5	정책의 승인 및 공표, 정책의 체계, 정책의 유지관리
정보보호 조직	4	조직의 체계, 책임과 역할
외부자 보안	4	계약 및 서비스 수준협약, 외부자 보안
정보자산 분류	4	정보자산의 조사 및 책임할당, 정보 자산의 분류 및 취급
정보보호 교육 및 훈련	4	교육 및 훈련프로그램 수립, 교육훈련의 시행 및 평가
인적보안	5	책임할당 및 규정화, 직원의 적격심사, 주요직무 담당자관리, 비밀유지
물리적 보안	12	물리적 보호구역, 물리적 접근통제, 데이터 센터보안, 장비보호, 사무실 보호
시스템 개발 보안	13	분석 및 설계, 구현 및 이행, 변경관리
암호통제	3	암호정책, 암호사용, 키 관리
시스템 개발 보안	14	접근통제 정책, 사용자 접근 관리, 접근통제 영역
접근통제	14	접근통제 정책, 사용자 접근관리, 접근통제 영역
운영관리	22	운영절차와 책임, 시스템운영, 네트워크 운영 및 문서관리, 악성소프트웨어 통제, 원격 컴퓨터 및 원격 작업
전자거래 보안	5	교환합의서, 전자거래, 전자우편, 공개서버의 보안관리, 이용자 공지사항
보안사고관리	7	대응계획 및 체계, 대응 및 복구, 사후관리
검토, 모니터링 및 감사	11	법적 요구사항 준수 검토, 정보보호정책 및 대책 준수 검토, 모니터링, 보안감사
업무 연속성 관리	7	업무 연속성 관리체계 수립, 업무 연속성 계획 수립과 구현, 업무 연속성 계획시험 및 유지관리

ISMS 통제항목 중 시스템 개발 보안 항목인 분석 및 설계 보안관리 (접근통제, 사용자접근관리 등) 10개 항목을 이용하여 정보시스템 설계단계 개인정보보호 감리 프로세스 항목을 도출하고자 한다.

3.2.2 ISO27001

ISO27001는 총 11개 도메인과 133개 통제항목으로 구성되어 있으며 인증체계의 도메인은 [표 3]과 같다[15][16].

표 3. ISO27001의 도메인별 정의

Domain	항목수	분야별 정의
정보보호 정책	2	정보보호에 대한 경영진의 방향성 및 지원을 제공
정보보호 조직	11	조직 내에서 정보보호 조직과 제3자 보안 제공
자산관리	5	자산 보호를 위한 책임 할당 및 자산분류를 통한 적절한 수준으로 보호
인적자원관리	9	임직원의 입사, 재직, 퇴직 시 고려해야 할 보안사항
물리적 / 환경적 보안	13	운영 절차 및 책임사항, 제 3자 서비스 공급관리, 시스템 계획 및 인수, 악성 및 모바일 코드에 대한 대응 방안, 백업, 네트워크 보안관리, 미디어관리, 정보교환, 전자상거래 서비스, 모니터링에 대한 보안사항

접근제어	32	접근제어를 위한 비즈니스 요구사항, 사용자 접근 관리, 사용자 책임, 네트워크 접근제어, 시스템 접근 제어, 어플리케이션 및 정보 접근제어, 모바일 컴퓨팅 및 텔레워킹 등에 대한 보안사항
정보시스템 도입, 개발, 유지	25	정보시스템의 보안 요구사항, 어플리케이션에서의 정확한 처리, 암호관리, 시스템 파일 보안, 개발과 지원 프로세스에서의 보안, 기술적인 취약점 관리 등에 대한 보안 사항
정보보안 사고 관리	5	보안 취약성과 사고에 대한 보고서, 보안사고 개선 관리 등에 대한 보안사항
사업 연속성 관리	5	재난이나 사고, 고장에 의한 주요한 비즈니스의 중단을 방지하기 위하여 업무영향 평가 및 위험평가, 복구계획 등을 수립하여 이행하고 테스트하여야 함.
준거성	10	법적 요구사항 준수, 정보보호 정책, 표준 및 기술적 사항에 대한 준수, 정보시스템 감사 준수사항 등에 대한 보안사항

ISO27001 통제항목 중 정보시스템 도입, 개발, 유지 항목 정보시스템 보안요구사항, 어플리케이션 내 처리 정확성, 암호통제, 응용시스템 파일의 보안을 이용하여 정보시스템 설계단계 개인정보보호 감리 프로세스 항목을 도출하고자 한다.

3.2.3 정보시스템 개발 구축 가이드

정보시스템 개발 구축 가이드 개발 단계별 정보보호 점검항목은, [표 4]와 같이 4단계 구분된 정보보호 활동에 대하여 총 172개를 도출하였다.

표 4. 정보시스템 개발 구축 가이드 도메인별 정의

Domain	항목수	분야별 정의
분석 단계	27	프로젝트 수행계획, 시스템 개용 및 특성정의, 정보보호 현황분석, 정보보호 요구사항분석, 위험평가, 정보보호 계획수립
설계 단계	115	정보보호설계, 네트워크, 서버, Application, DB, 클라이언트, 통합관리, 물리적 통제 설계
구현 단계	14	정보보호 구현 및 점검, 운영관리계획/지침 개발
시험 단계	16	정보보호시험, 정보보호설정, 이관 후 정보보호 시험, 정보보호 시험 계획 수립

지금까지 ISMS, ISO27001, 정보시스템 구축 가이드를 점검해 보았다. [표 5]는 분석 및 설계단계 세부 점검 항목을 비교를 통해 정보시스템 구축단계별 개인정보보호 감리 세부점검 항목을 비교 분석하였다.

표 5. 정보시스템 개발 주기 세부항목 비교 분석

구분	ISMS	ISO27001	정보시스템 구축
분석 단계	보안요구사항정의	보안 요구사항 분석 및 명세화	– 정보보호 현황 분석 – 정보보호 요구분석, – 위험 평가,정보보호 계획수립
설계 단계	– 입력 데이터 검증 – 내부 처리의 검증 – 출력 데이터 검증 – 인증 및 암호 – 보안기록 관리	– 입력데이터 확인 – 출력 데이터 확인 – 내부처리 통제 – 메시지 무결성 – 암호통제의 적응 정책 및 Key – 응용 파일의 보안	– 식별/인증,접근 통제 – 로깅 및 감사 – 통신 보호/암호화 – 침입탐지, 무결성
구현 단계	– 구현 및 시험 – 소스프로그램의 접근보안	– 프로그램 소스코드 접근 통제 – 운용 S/W 통제	– 정보보호 구현 및 검토 – 운영관리 계획/지침 개발
시험 단계	운영환경 이행 보안 – 시험 데이터의 보안	시스템 시험 데이터 보호	– 정보보호 구현 시험 – 운영 계획 및 지침 – 정보보호 시험 – 정보보호 설정 – 이관 후 정보보호 시험

[표 5]와 같이 ISO27001, ISMS는 경우 정보 자산을 효율적으로 보호하기 위한 조직의 정보보호 인증체계로 너무 포괄적으로 담고 있으며, 정보보호정책 수립에서부터 사후관리까지 조직의 전반적인 범위를 포함하고 있다.

3.3 개인정보보호 감리 프로세스

3.3.1 분석단계 개인정보보호 감리 프로세스

정보시스템 개발 분석단계 주요활동은 개발될 시스템에 대해 정의하고, 시스템 개요 및 특성 정의, 정보보호 현황분석, 정보 보호 요구분석, 위험평가, 정보보호 계획 수립한다. 분석단계에서 개인정보를 보호하기 위해서 개인정보보호 위험 요소를 분석할 수 있는 프로젝트 사전분석 산출물(시스템 구축 제안서, N/W 구성도, 사업계획서 등)과 PIA 7단계 프로세스를 이용하여 [그림 4]와 같이 각 절차별 산출물(영향평가 타당성 보고서, 영향평가 업무 분장도, 개인정보 평가표, 개인정보 흐름표, 개선계획, 위험개선 총괄표 등)을 구축하였다.

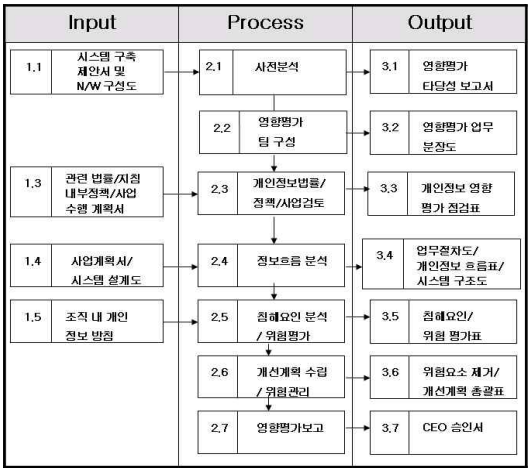

그림 4. 분석단계의 개인정보 보호활동 및 산출물

분석단계의 개인정보보호 활동 기능 및 산출물 분석 / PIA 수행 단계별 요구사항을 통해 [표 6]과 같이 개인정보보호 감리 항목 7단계통제항목과 21개 세부 점검항목이 도출되었다.

표 6. 분석단계 PIA 개인정보보호 감리 통제 항목

절차	내 용	점검항목
사전분석	-시행 또는 변경하고자 하는 사업에 대한 개인정보 영향평가의 필요성 여부 결정하는 단계	4개
영향평가 수행 주체의 선정	-내/외부 개인정보영향평가 수행 능력과 경험이 있는 직원 또는 전문가로 영향평가팀 구성·운영 -영향평가 총 책임자 선정 및 구성원에게 역할과 책임사항 배분	4개
개인정보 관련 정책, 법규 및 사업내용 검토	-개인정보 관련 내부 정책 및 조직 체계 검토 -개인정보 관련법률·지침 및 가이드라인 등 조사 -시행 또는 변경하고자 하는 사업 내용 검토	3개
정보 흐름 분석	-개인정보 자산의 종류 및 처리단계, 개인정보에 대한 통제 및 접근권한, 제 3자 제공여부 등을 도표화 -각종 보안장치를 포함한 정보시스템 구조도 분석	2개
개인정보 침해요인 분석 및 위험평가	-주요 개인정보 자산에 대하여 주어진 점검표를 바탕으로 침해 요인 분석 -점검표에 의해 드러난 침해요인에 대한 위험 평가를 실시하여 위험평가표 작성	5개
개선계획 수립 및 위험관리	-보장수준에 따라 관리되어야 할 위험과 잔여 위험으로 분리하고 관리되어야 할 위험에 대한 통제방안 마련 -위험에 대한 통제방안 마련 과정에서 의견충돌이 생기는 경우 최고 관리자가 참여하여 의사결정	2개
영향평가 보고서 작성 및 제출	-사전 준비단계부터 프로젝트 개요 및 위험관리까지 모든 절차의 내용과 결과를 정리하여 문서화	1개

[표 7]은 [표 5] 및 PIA 개인정보보호 감리의 7단계 프로세스[그림 2]를 이용하여 각 통제항목별 세부점검항목 및 검토문서를 산출하였다.

표 7. 분석단계 PIA 개인정보보호 감리 세부 점검항목

감리점검항목	세부검토항목	검토문서
사전분석 단계 도입의 필요성 검토	1.1 개인정보 수집 / 파기 / 보관절차 구현 전 개인정보보호 필요성을 검토하였는가?	구축 제안서
	1.2 다른 시스템과 개인정보 연동 시 개인정보보호 필요성을 검토하였는가?	구축 설계서
	1.3 제 3자와 개인정보 공유할 경우 개인정보보호 필요성 검토하였는가?	
	1.4 기존 보안 및 개인정보 체계에 영향을 줄 경우 개인정보보호 필요성을 검토하였는가?	네트워크 구성도
개인영향 평가팀 구성의 적정성	2.1 사업 주관부서, 개인정보 소유부서, 시스템 운영 부서, 개인정보관리 책임자, 최고 의사 결정자 또는 외부 전문가 등으로 영향평가팀이 적절하게 구성되었는가?	영향 평가팀 업무 배분도
	2.2 법률 검토 및 조언이 가능한 담당자가 포함되어 있는가?	
	2.3 기관의 사업흐름과 내용을 분석하는 담당자가 포함되어 있는가?	
	2.4 정보보안 기술적 구조와 데이터 흐름을 분석하는 담당자가 포함되어있는가?	
개인정보 관련 정책, 법규 및 사업평가의 적정성	3.1 영향평가 수행 이전에 현재 조직 내 개인정보 관련 주요 사항에 대해 검토 되었는가? - 조직 내의 개인정보관리 절차•방법 및 개인정보보호정책 - 개인정보관리책임자 및 담당자의 역할과 책임 - 개인정보 관련 조직 체계 등	관련법률 지침 / 가이드라인
	3.2 신규 구축하는 사업에 적용되는 각종 개인정보보호 관한 법률 지침 가이드라인 및 기관 내부 규정 등에 대한 조사가 실시되었는가?	개인정보 관련내부 정책
	3.3 신규 구축하고자 하는 사업이 개인정보를 수집•이용•보관•파기 업무를 수행하는지 확인하기 위하여 사업개요 및 사업절차가 검토되었는가?	사업수행 계획서
정보흐름 분석의 적정성	4.1 개인정보 자산의 종류 및 처리단계, 개인정보에 대한 통제 및 접근권한, 제3자 제공 여부 등을 한눈에 볼 수 있도록 도표화 작성되었는가?	시스템 관련사업 계획서
	4.2 각종 보안장치를 포함한 정보시스템 구조가 분석이 되었는가?	시스템 설계도
개인정보 침해요인 분석 및 위험평가의 적정성	5.1 개인정보 침해요인 분석 및 평가를 위해 위험평가표가 적절하게 도출되었는가?	관련법률 / 보안 가이드라인
	5.2 기관 내 정보화 사업 기획 점검 및 기관내 개인정보보호 체계를 검토 되었는가?	
	5.3 개인정보의 수집단계에서 발생할 수 있는 위험 요소를 분석 및 도출하였는가?	
	5.4 개인정보 이용 및 저장 기간을 검토하고 파기 절차가 존재하는가?	조직 내 개인정보 보호방침
	5.5 침해 발생시 조치사항 및 내부절차가 검토되고 위험 평가표에 반영되었는가?	
개선계획 수립 및 위험관리 적정성	6.1 개인정보 위험관리를 위한 관리위험 / 잔여위험/통제 방안이 수립되었는가?	개인정보 침해요인 점검표
	6.2 개인정보 위험관리를 위한 관리위험 / 잔여위험 및 통제 방안이 수립되었는가?	
영향평가 보고서 적정성	7.2 개인정보 영향평가 결과를 최종적으로 검토 또는 승인할 수 있는 최고의사 결정권자(CEO)에게 보고서를 제출 되었는가?	영향평가 최종 보고서

3.3.2 설계단계 개인정보보호 감리 프로세스

설계 단계는 분석 단계에서의 요구사항이 정보시스템으로 구현되기 위해 해석되고 구체화되는 과정으로 개인정보보호 설계, 개인정보보호 시험계획 수립 활동이 수행된다. [그림 5]의 개인정보보호 분석 단계에서 산출된 침해요인 및 위험평가표, 위험요소제거 및 개선계획 총괄표, 개인정보 영향 평가 점검표 등을 이용하여 개인정보보호 설계서 및 테스트 계획서 산출물이 생성되었으며 한국정보보호 진흥원의『정보시스템 구축 단계별 정보보호 가이드라인』및 ISMS / ISO27001을 기반으로 점검항목이 도출되었다.

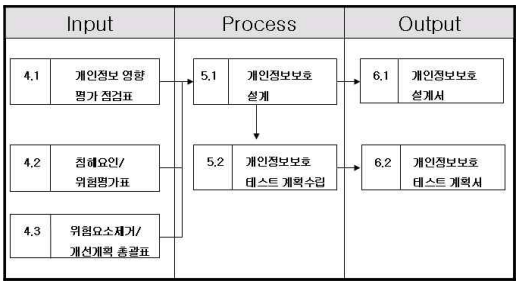

그림 5. 설계단계의 개인정보 보호활동 및 산출물

개인정보보호 설계 및 개인정보보호 테스트 계획 수립 프로세스와 산출물분석 / 과 ISO27001 정보시스템 도입, 개발, 유지 프로세스를 이용하여 [표 8]과 같이 개인정보보호 감리 항목 4단계(8개 통제항목)과 24개 세부 점검항목이 도출되었다.

표 8. 설계단계 개인정보보호 통제 항목

절차		내 용	점검 항목
개인정보보호 설계	공통사항 (서버,N/W,응용,DB)	- 개인정보 식별 및 인증, 접근통제 설계, 로깅 및 감사 설계, 통신보호 및 암호화 설계, 무결성 설계, 침입탐지 설계, 복구설계 세부항목	12개
	응용프로그램설계	- 입력 값 및 파라미터값 검증 설계 - XSS, SQL Injection 대책 설계 - 쿠키 암호화 방안 설계 등	4개
	물리적 설계	- 출입통제 방안을 설계 - 장비에 대한 물리적 정보보호 방안을 설계	4개
개인정보 테스트 계획 수립		- 시험의 목적을 정의 - 시험대상, 범위, 가정, 제약조건, 준비사항을 정의 - 시험 절차 / 일정계획을 정의 - 시험을 위한 팀 구성 및 역할을 정의	4개

[표 9]는 [표 5]와 PIA 개인정보보호 분석 산출물 및 정보시스템구축단계별 정보보호 방법론 이용하여 각 통제항목별 세부점검항목 및 검토문서를 산출하였다.

표 9. 설계단계 PIA 개인정보보호 감리 세부 점검항목

감리점검 항목	세부검토항목		검토문서
공통사항 (N/W, DB, 서버 응용프로그램) 설계의 적정성	식별 및 인증	8.1 접근 위험을 분석하여 이에 따른 식별 인증 방안이 설계 되었는가?	시스템 구축 설계도
		8.2 계정 설정 및 패스워드 관리 정책을 수립하였는가?	
	접근 통제	8.3 최소한 접근 통제 정책을 기반으로 설계 안을 작성하였는가?	네트워크 구성도
		8.4. 개인정보 시스템은 내부망과 분리하여 설치하며 침입차단 시스템 등에 의해 보호되도록 설계하였는가?	침해요인 위험분석 평가표
		8.5 개인정보 시스템은 네트워크간 관리 정책이 설계되었는가?	
		8.6 침입차단시스템 등의 보호장비를 우회한 인터넷 접속이 불가능하도록 설계되었는가?	위험요소 개선/ 위험 총괄표
	로깅 및 감사	8.7 불법적인 침투시도를 기록 할 수 있는 로깅 방안이 설계되었는가?	
		8.8 비인자가 개인정보 로그 기록에 접근할 수 없도록 설계되었는가?	
		8.9 개인정보 접속 로그를 일정기간 저장하고 분석할 수 있도록 설계되었는가?	
	암호화	8.10 개인정보 데이터에 대해 안전한 통신을 보장하도록 암호화 설계(SSL) 되었는가?	
	침입 탐지	8.11 개인정보 접근 시 비인가자나 의심스러운 사용자의 접근 행위를 모니터링, 탐지하고, 추적하는 방안이 설계 되었는가?	
		8.12 바이러스 진단, 색출, 예방, 퇴치를 등을 위한 방안을 설계에 반영 했는가?	
응용프로그램 설계의 적정성	입력 검증	9.1 개인정보 입력 값 및 파라미터 값, 모듈간 전달되는 파라미터값 등이 정확하게 들어오는지에 대한 검증이 이루어 지도록 설계되었는가?	시스템 구축 설계도 및 제안서
		9.2 개인정보 웹 어플리케이션 설계 시 대표적인 입력공격(XSS, SQL Injection 등)에 대한 대책이 설계되었는가?	
		9.3 쿠키를 사용한 개인정보 인증의 경우 인증값 보호를 위한 암호화 방안을 설계에 적용했는가?	네트워크 구성도
		9.4 개인정보 어플리케이션의 환경변수 등 구성 설정 내용의 안전한 저장 방법을 설계에 반영했는가?	침해요인 위험분석 평가표
물리적 통제 설계의 적정성		10.1 개인정보 전산실은 잠금 장치를 설치하도록설계 했는지를 점검하였는가?	
		10.2 개인정보 전산실 출입기록을 녹화하고 기록 할 수 있는 장치를 설계에 반영 했는가?	
		10.3 개인정보 전산실 천장을 통하여 외부와의 왕래가 불가능하도록 설계되었는가?	위험요소 개선/ 위험 총괄표
		10.4 개인정보 전산실의 주요창문은 강화유리를 사용하고 개폐가 되지 않도록 설계되었는가?	
정보보호 시험 계획수립		11.1 개인정보보호 기능 시험의 목적, 대상 및 범위, 가정, 제약조건, 준비사항을 정의되었는가?	
		11.2 개인정보보호 영역 및 구성 요소 별 시험 항목을 정의했는가?	
		11.3 개인정보보호 시험방법 및 절차를 정의하고, 이 관후 침투시험을 수행할 경우 침투 시나리오를 수립했는가?	
		11.4 개인정보보호 시험을 위한 조직의 구성 및 책임과 역할을 정의했는가?	

IV. 분석/설계 단계에서 개인정보보호 감리 프로세스 검증

본 설문은 공공기관 정보화 사업의 정보시스템 분석 및 설계단계에서 개인정보보호감리 프로세스 실효성을 점검하기 위한 목적으로 작성되었으며 정보시스템 역할별 담당자 50명을 기준으로 설문 조사를 실시하였다. 통계 분석은 SPSS 10을 이용했으며 PIA 인식 수준 및 프로젝트 수행여부 / 각 검증항목 설문은 빈도분석을 통해 각 항목별 점유율을 추출하였다.

4.1 통제항목 및 주요점검사항 검증 결과

설문 내용은 아래의 [표 10]과 같이 도출되었으며 분석 단계의 경우는 개인정보영향평가(PIA) 모델을 이용하여 7개의 통제항목과 21개의 주요 세부점검 항목을 도출했으며 설계 단계의 경우는 정보시스템 설계 단계별 정보보호 요구사항을 토대로 1개의 통제항목과 7개의 주요 통제점검 항목을 도출하였다. 답변항목 <매우필요, 필요, 보통, 필요없음, 전혀필요없음>의 5개 항목은 <매우필요, 필요>는 적합으로, <보통>은 보통으로, <필요없음, 전혀필요없음>은 부적합으로 3단계로 줄였다.

[표 10]과 같이 개인정보 사전분석 단계 도입의 필요성(92.4%), 개인영향 평가팀 구성의 필요성(77.2%), 개인정보 관련 정책, 법규 및 사업평가 필요성(86.5%), 개인정보흐름 분석의 필요성(74.6%), 개인정보 침해요인 분석 및 위험평가의 필요성(91.3%), 개선계획 수립 및 위험관리 필요성(91.3%), 영향평가보고서 작성 및 승인의 적정성(80%), N/W, DB, 서버 응용프로그램, 물리적 보안 설계 적정성(92.5%)의 8개의 통제항목이 적합하다는 결과가 도출되었다.

대부분의 항목은 90%이상 적합하다는 결과가 도출되었지만 개인 영향평가팀 구성의 필요성, 개인정보흐름 분석의 필요성, 영향평가보고서 작성 및 승인의 적정성 통제항목의 경우 상대적으로 낮은 동의를 보이고 있어 감리 개선 권고의견 작성 시 의무적 도입보다는 권고사항으로 판단되며 프로젝트 이해 관계자와 지속적이고 탄력적인 협의가 필요하다.

표 10. 개인정보보호 감리 설문 검증

구분	통제항목 및 주요점검 사항	점검항목 타당성 검증			소계
		적합	보통	부적합	
개인정보분석단계	1. 개인정보 사전분석 단계도입 필요성	47	3		50
	1.1 개인정보 수집 / 파기 / 보관절차 구현 전 개인정보보호 필요성 점검	45	5		
	1.2 다른 시스템과 개인정보 연동시 개인정보보호 필요성 점검	47	3		
	1.3 제 3자와 개인정보 공유 할 경우 개인정보보호 필요성 점검	49	1		
	1.4 기존 보안 및 개인정보체계에 영향을 줄 경우 개인정보보호 필요성	43	7		
	통제항목 응답률	92.4 %	7.6 %		100%
	2. 개인영향 평가팀 구성의 필요성	39	10	1	50
	2.1 개인정보보호 영향도 분석을 위한 개인정보보호 각 분야별 담당자가 적절하게 구성되어 있는지를 점검	39	9	2	
	2.2 개인정보보호 관련 법률검토 및 조언이 가능한 담당자포함 여부 점검	37	12	1	
	2.3 기관의 사업흐름과 내용을 분석하고 사업계획과 절차 흐름도 작성 담당자 포함 여부를 점검	40	10		
	2.4 정보보안 기술적 구조와 데이터 흐름 등에 관한 기술적 및 시스템적 담당자포함 여부를 점검	38	10	2	
	통제항목 응답률	77.2 %	20.4	2.4%	100%
	3. 개인정보 관련 정책, 법규 및 사업평가 필요성	46	4		
	3.1 현재 조직 내 개인정보 관련 주요 사항에 대해 검토 여부를 점검	40	9	1	
	3.2 개인정보보호 관한 법률·지침·가이드라인 및 기관 내부 규정 등에 대한 조사를 실시 했는지를 점검	41	8	1	
	3.3 개인정보를 수집·이용·보관 · 파기 등의 업무를 수행하기 위한 사업 개요표 및 사업절차도 검토 점검	46	3	1	
	통제항목 응답률	86.5 %	12%	1.5%	100%
	4. 개인정보흐름 분석의 필요성	38	12		50
	4.1 개인정보 흐름 분석(이동 및 관리/저장) 및 접근통제, 제 3자 제공여부 등을 볼 수 있는 도표화(업무절차도 및 개인정보 흐름도) 작성여부 점검	33	17		
	4.2 각종 보안장치를 포함한 정보시스템 구조도 분석여부를 점검	41	8	1	
	통제항목 응답률	74.6 %	24.6	0.8%	100%
	5. 개인정보 침해요인 분석 및 위험평가의 필요성	49	1		50
	5.1 개인정보 침해요인 분석 및 평가를 위해 위험 평가표가 적절하게 도출되었는지 점검	47	3		
	5.2 정보화 사업 기획 점검 및 개인정보 보호 체계 검토	43	7		
	5.3 개인정보의 수집단계에서 발생	45	5		

		할 수 있는 위험 요소를 분석 및 도출				
	5.4	개인 정보의 이용 및 저장기간을 검토하고 해당 정보의 파기 절차 존재 여부를 점검	43	7		
	5.5	침해 발생 시 조치사항 및 내부절차가 검토되고 위험평가표에 반영되어 있는지를 점검	47	3		
		통제항목 응답률	91.3 %	8.7 %		100%
	6.	개선계획 수립 및 위험관리 필요성	47	3		50
	6.1	개인정보 위험관리를 위한 관리위험 /잔여위험 및 통제 방안이 수립되었는지를 점검	44	5	1	
	6.2	개인정보 위험관리를 위해 위험 순위에 따른 평가 및 조치가 수립 되었는지를 점검	46	3	1	
		통제항목 응답률	91.3 %	7.3 %	1.3%	100%
	7.	영향평가보고서 작성 및 승인의 적정성	40	9	1	50
		통제항목 응답률	80%	18%	2%	100%
개인정보 설계 단계	8.	N/W, DB, 서버 응용프로그램, 물리적 보안 설계 적정성	46	3	1	50
	8.1	개인정보 식별 및 인증을 고려한 설계 적정성 점검	46	3	1	
	8.2	개인정보 데이터 보호를 위한 암호화 설계의 적정성 점검	45	5		
	8.3	개인정보 수집·이용·보관·파기로깅 및 감사 설계의 적정성 점검	44	5	1	
	8.4	개인정보 침해 방지를 위한 침입차단 설계의 적정성 점검	47	3		
	8.5	개인정보 입력 정보의 위·변조 방지 설계의 적정성 점검	47	3		
	8.6	개인정보 시스템 출입 및 물리적 장비 보호 통제 설계의 적정성 점검	48	2		
	8.7	개인정보 접근통제를 고려한 설계의 적정성 점검	47	2	1	
		통제항목 응답률	92.5%	6.5 %	1%	100%

4.2 분석/설계단계 개인정보보호 감리 사례 검증

[표 11]은 본 논문에서 도출된 PIA 개인정보보호 감리 프로세스에 대해여 그 실효성을 검증하고자 현 정보시스템 감리 기준으로 과거 프로젝트를 선정하였다.

표 11. 프로젝트별 감리 내용

구분	A프로젝트 감리내용	B프로젝트 감리내용
사업명	○○○○○○ 유통지원시스템 구축사업	통합○○관리시스템 구축사업
사업기간	6개월	15개월
사업금액	10억 5천6백만원 (지원도구 포함)	25억 9천만원 (지원도구 포함)
감리방법	중간/최종감리 진행	중간/최종감리 진행
사업내용	– 유통지원시스템 구축 – 수급안정지원관리 시스템 구축	– 경영계획 / 예산관리시스템 구축 – BPM기반의 사업관리시스템 구축 – 해외사무소 운영관리시스템 재구축 – 봉사단파견관리시스템 연동작업

4.2.1 A 프로젝트 검증

4.2.1.1 개인정보보호 감리항목과 A프로젝트 점검항목 비교

A 프로젝트는 2007년 6월에 수행한 RFID 기반의 생산유통지원시스템 구축 및 수급안정지원관리 시스템 구축 사업이다. 2007년 9월 정보시스템 기반정립 및 분석 / 설계 단계의 중간감리와 생산유통지원시스템 구현 및 개선 단계의 최종감리로 총 2회의 감리를 실시하였다. 아래의 [표 12]는 본 논문에서 제안한 개인정보보호 감리 점검항목과 감리 사례로 선정한 A프로젝트 감리 점검항목을 비교하였다.

표 12. PIA 개인정보보호 항목과 A 프로젝트별 점검항목

구분	PIA 감리 점검항목	A 프로젝트 감리 점검항목
분석단계	PIA 사전분석 단계 도입의 필요성 검토	_
	개인영향 평가팀 구성의 적정성	_
	개인정보관련 정책,법규 및 사업 평가의 적정성	개인정보 관련 법률 점검 – 정보통신망 이용촉진 및 정보 보호 등에 관한 법률
	개인정보흐름 분석의 적정성	_
	개인정보 침해요인분석 및 위험 평가의 적정성	개인정보 침해 요인 분석 및 위험평가의 적정성 – 주민등록번호 도용에 따른 위험(해커의 침입으로 자료 누출, 스니핑, 기타 인터넷상의 개인 신상 공개 위험)
	개인정보 개선계획수립 및 위험관리 적정성	개선계획수립 및 위험관리 적정성 – 개인보호정책 확대에 따라 주민등록번호에 의한 인증 방식을 아이핀 또는 E-Mail 주소 인증 방식의 적용 검토를 권고
	개인정보 영향 평가보고서 적정성	_
설계단계	N/W, DB, 서버 응용프로그램, 물리적 보안 설계 적정성	– 응용시스템 접근권한 및 통제 설계를 적정하게 수행하였는지 여부 – 시스템 아키텍처에 대한 정의 및 설계를 적정하게 수행 여부 – 보안의 상세설계의 적정성 여부

[표 10]에서와 같이 본 논문에서 제안한 정보시스템 분석 및 설계단계의 개인정보보호 감리 통제항목 8개 항목 중에 A프로젝트 감리에 재 적용하여 나타난 감리

점검 항목은 4개이다. 그러므로 감리 영역에 포함되지 않은 4개의 항목에 대해서 문제점이 발생될 수 있으며, 신규 개인정보보호 감리 프로세스의 항목을 통해 이러한 문제점의 개선을 기대할 수 있다.

4.2.1.2 A 프로젝트 감리 결과

[표 13]은 본 논문에서 제안한 개인정보보호 감리점검항목에서 도출한 중간감리의 개선권고사항 중에서 A 프로젝트의 개선권고사항과 종합의견에 대한 감리 내용 중 일부 발췌하였다.

표 13. 기존 A 프로젝트 감리 결과

개선권고사항	개선권고유형	개선시점	중요도	주관기관협조필요
(1) 개인보호정책 확대에 따라 주민등록 번호에 의한 인증 방식을 아이핀 또는 E-Mail 주소 인증 방식의 적용 검토를 권고함	협의	장기		
(2) 안전정보 웹 서비스 시스템의 분석설계 산출물에서의 일부 설계 누락된 내용의 추가 및 미흡한 산출물의 보완 필요함	필수	단기	○	
(3) 사용자 접근/통제의 완전성을 위하여 기정의된 사용자의 역할 정립과 현재 프로그램별 접근 권한이 필요함	협의	단기		

<종합의견>

안정정보 WEB 시스템 설계가 누락되었으며, 설계는 되었으나 운영 방안이 확정되지 않은 커뮤니티 운영자에 대한 운영계획의 보완이 필요하고, 개인정보 보호정책에 따라 주민등록번호를 이용한 회원 인증에 대해 정통부에서 고시된 정보통신망법에서 제시하는 주민등록번호 대체 수단인 아이핀이나 다른 대체 수단인 E-Mail 인증 등의 적용 검토를 권고하며 현재 프로그램 별 정의된 사용자 역할 정립과 접근 통제의 권한이 필요함.

4.2.1.3 PIA 개인정보보호 감리와 A프로젝트 감리 비교

[표 10]의 점검항목 비교에서 도출된 내용을 근거로 PIA 개인정보보호감리 항목 중 A프로젝트의 감리 점검항목의 영역에 포함되지 않는 4개의항목에 대해서 본 논문에서 제안한 감리항목으로 A프로젝트 감리를 수행하였다. 그 결과 아래의 [표 14]와 같이 추가개선권고사항이 도출되었다.

표 14. PIA 개인정보보호 감리를 통한 A프로젝트 감리 결과

개선권고사항	개선권고유형	개선시점	중요도	주관기관협조필요
(1) 개인정보 수집·이용·파기·보관 영향평가를 위해 PIA 사전 검토가 필요함.	협의	단기		
(2) 개인정보 수집·이용·파기·보관 영향평가를 위해 법률적, 기술적, 업무적 전문가 의견이 포함을 권고함.	협의	장기		○
(3) 개인보호정책 확대에 따라 주민등록 번호에 의한 인증 방식을 아이핀 또는 E-Mail 주소 인증 방식의 적용 검토를 권고하며 해당 시스템 구축 불가 시 최소한의 암호화가 필요함.	필수	장기		
(4) 안전정보 웹 서비스 시스템의 분석설계 산출물에서의 일부 설계 누락된 내용의 추가 및 미흡한 산출물의 보완 필요함.	필수	단기	○	
(5) 개인정보 흐름 분석(이동 및 관리/저장) 및 접근통제, 제 3자 제공여부 등을 볼 수 있는 도표화(업무절차도 및 개인정보 흐름도) 작성이 필요함.	협의	장기		
(6) 사용자 접근/통제의 완전성을 위하여 기 정의된 사용자의 역할 정립과 현재 프로그램 별 접근 권한이 필요함.	필수	단기	○	
(7) 개인정보 영향평가 보고서가 기관장 승인 및 행안부와 보유파일에 대한 사전 협의를 했는지 점검이 필요함.	필수	장기	○	○

<종합의견>

개인정보의 수집·이용·보관·파기 영향평가 및 타당성 검토를 위해 개인영향평가(PIA)의 도입의 필요성을 검토해야 하며 PIA를 실행 할 경우 법률적, 기술적, 업무적 조언이 가능한 내부 및 외부 전문가의 역할이 업무 배분도에 포함을 권고하며 개인정보 보호정책에 따라 주민등록번호를 이용한 회원인증에 대해 정통부에서 고시된 정보통신망법에서 제시하는 주민등록번호 대체 수단인 아이핀이나 다른 대체 수단인 E-Mail 인증 등의 적용 검토를 권고하며 해당 시스템 구축 불가 시 최소한의 암호화 정책이 필요하다. 개인정보 취약점 및 위험을 분석하기 위한 개인정보 흐름 도표화가 필요하며 현재 프로그램 별 정의된 사용자 역할 정립과 접근 통제의 권한이 필요하다. 개인정보 파일을 보유하기 위해서는 행정안전부와 사전 협의해야 하며 최종적으로 안전한 시스템 인증을 위해 국가정보원의 승인이 필요하다.

위의 [표 10]과 같이 신규 개인정보보호 감리 프로세스를 적용함으로 실제감리시 확인되지 못한 A기관의 추가 개선 권고사항을 도출하여 개인정보 안정화에 기여할 수 있었다.

4.2.2 PIA 개인정보보호 감리를 이용한 B 프로젝트 검증

4.2.2.1 개인정보보호 감리항목과 B 프로젝트 점검항목 비교

B프로젝트는 2005년 12월에 수행한 통합○○관리시스템 구축사업으로 전략경영체계 구축, 사업관리시스템 구축, 지식정보시스템 구축, 고객서비스시스템 구축 사업을 위한 프로젝트이다. 이에 따라 2006년 9월 정보시스템 기반정립 및 분석 / 설계 단계의 중간감리 및 최종감리를 실시하였다. 아래의 [표 15]는 본 논문에서 제안한 개인정보보호 감리 점검항목과 감리 사례로 선정한 B프로젝트 감리 점검항목을 비교하였다.

표 15. PIA 개인정보보호 항목과 B 프로젝트별 점검항목

구분	PIA 감리 점검항목	B 프로젝트 감리 점검항목
분석단계	PIA 사전분석 단계 도입의 필요성 검토	_
	PIA평가팀 구성의 적정성	–
	개인정보관련 정책,법규 및 사업평가의 적정성	_
	개인정보흐름 분석적정성	–
	개인정보 침해요인분석 및 위험평가의 적정성	_
	개인정보 개선계획수립 및 위험관리 적정성	_
	PIA 평가보고서 적정성	–
설계단계	N/W, DB, 서버 응용프로그램, 물리적 보안 설계 적정성	– 패키지 사용자 접근통제 및 보안 분석을 적정하게 수행하였는지 여부 – DB 데이터에 대한 접근통제 및 보안에 대한 분석, 설계의 적정성 – 시스템 보안요건분석 및 보안 설계의 적정성 – DB 및 응용프로그램 감사 설계의 적정성

[표 10]과 같이 본 논문에서 제안한 정보시스템 분석 및 설계단계 개인정보보호 감리 통제항목 8개의 개선작업 중에 B기관 감리 시 나타난 감리점검 항목의 감리영역은 1개이다. 그러므로 감리 영역에 포함되지 않은 7개의 항목에 대해서 문제점이 발생될 수 있으며, 신규 개인정보보호 감리 프로세스의 항목을 통해 이러한 문제점의 개선을 기대할 수 있다.

4.2.2.2 B 프로젝트 감리 결과

[표 16]은 본 논문에서 제안한 개인정보보호 감리점검항목에서 도출한 중간감리의 개선권고사항 중에서 보안감리 내용 중 일부 발췌한 내용이다.

표 16. 기존 B 프로젝트 감리 결과

개선권고사항	개선권고유형	개선시점	중요도	주관기관 협조필요
(1) 응용시스템의 업무요건에 맞는 접근통제 정의가 필요함.	필수	장기		
(2) 시스템 아키텍처 보안체계의 분석 및 설계가 미흡함.	필수	장기		
(3) 싱글사인온 시스템 (SSO) 구축 방안과 그 시험 계획이 미흡함	협의	단기		
(4) 개발환경의 보완과 구축되는 시스템의 가용성을 제고할 수 있도록 적절한 장애 복구 및 백업 대책의 설계서 반영이 필요함	필수	단기	○	

<종합의견>

응용시스템 및 데이터베이스부문은 데이터의 접근통제 및 보안, 백업 및 복구 방안의 미흡하며 신규 시스템에서 요구되는 응용시스템 및 데이터 보안 요구사항 도출이 미흡하였다. 싱글 사인 온 시스템 (SSO)의 구체적인 계획과 실행과정이 미흡하며 DBA, 통합전문가의 투입이 조속히 필요함.

4.2.2.3 PIA 개인정보보호 감리와 B 프로젝트 감리 비교

[표 10]의 점검항목 비교에서 도출된 내용을 근거로 분석 및 설계단계 개인정보보호 감리 항목 중 A프로젝트의 감리 점검항목의 영역에 포함되지 않는 7개의 항목에 대해서 본 논문에서 제안한 감리항목으로 A프로젝트 감리를 수행하였다. 그 결과 아래의 [표 17]과 같이 추가개선 권고사항이 도출되었다.

표 17. PIA 개인정보보호 감리를 통한 B프로젝트 감리 결과

개선권고사항	개선권고유형	개선시점	중요도	주관기관 협조필요
(1) 개인정보 수집·이용·파기·보관 절차 존재 여부 사전 검토 필요함	협의	단기		
(2) 개인보호정책 확대에 따라 주민등록번호에 의한 인증 방식에 대한 검토가 필요함	필수	장기	○	
(3) 기관 및 정부의 개인정보보호 법률적 최소 가이드라인 및 내부 규정의 조사가 필요함	필수	단기	○	○
(4) 개인정보 흐름 분석 및 접근통제를 확인할 수 있는 도표화 작성이 필요함	협의	장기		
(5) 시스템 아키텍처 보안체계의 분석 및 설계가 미흡함.	필수	단기	○	

<종합의견>

WEB 서비스 제공에 따른 개인정보의 수집·이용·파기·보관 절차 존재여부를 사전에 검토해야 하며 개인정보 보호정책에 따라 주민등록번호를 이용한 회원 인증에 대해 정통부에서 고시된 정보통신망법에서 제시하는 주민등록번호 대체 수단인 아이핀이나 다른 대체 수단인 E-Mail 인증 등의 적용 검토를 권고하며 해당 시스템 구축 불가 시 최소한의 암호화 정책이 필요하다. 기관 및 정부의 개인정보보호를 위한 최소한의 법률적 가이드라인 및 내부규정에 대한 조사가 필요하며 개인정보 취약점 및 위험을 분석하기 위한 개인정보 흐름 도표화를 권고하며 현재 프로그램 별 정의된 사용자 역할정립과 접근 통제의 권한이 필요하다. 응용시스템 및 데이터베이스 부문은 데이터의 접근통제 및 보안, 백업 및 복구 방안의 미흡하며 신규 시스템에서 요구되는 응용시스템 및 데이터 보안 요구사항 도출이 미흡하였다.

4.2.3 PIA 개인정보보호 감리 프로세스 실효성 검증 결과

본 논문에서 제시한 PIA 개인정보보호 감리 프로세스를 설문을 통해 [표 10]과 같이 타당성을 입증했으며 모든 설문 항목이 필수 또는 권고 항목을 도출되었다. A, B 프로젝트를 PIA 개인정보보호 프로세스로 감리한 결과 [표 18]과 개선사항을 도출할 수 있었으며 개인정보를 보호하기 위한 사전 프로세스가 미흡한 것으로 나타났다.

표 18. PIA 개인정보보호 사례 비교 분석

구분	PIA 개인정보보호 감리 프로세스	A 사례	B 사례	비고
개인정보분석단계	개인정보 사전분석 단계 도입의 필요성	X	X	개인정보 수집, 이용, 파기, 보관절차 존재 시 사전검토 필수
	개인영향 평가팀 구성의 필요성	X	X	개인정보 이용 시 각 분야별 전문가 의견 포함 권고
	개인정보관련 정책, 법규/사업 평가 필요성	○	X	B기관 최소 법률 / 정부가이드 검토 필요
	개인정보보호 흐름 분석의 필요성	X	X	개인정보 흐름분석 도표화 권고
	개인정보 침해요인 분석/위험 평가의 필요성	○	X	B기관 개인정보 침해 요소 분석 필요
	개선계획 수립 및 위험관리 필요성	○	X	B기관 개인정보보호를 위한 암호화 필수 및 아이핀 인증 권고
	영향평가보고서 작성 및 승인의 적정성	X	X	기관장 승인 및 행안부 사전 협의 필요
설계단계	N/W, DB, 서버 응용프로그램, 물리적 보안 설계 적정성	○	○	

B 프로젝트의 경우 WEB 서비스를 운용 및 연동해야 하나 개인정보를 위한 장치가 전혀 없으며 시스템 아키텍처의 접근 통제로만 개인정보를 보호하고 있어 추가적인 개인정보보호 장치 마련이 절실히 필요하다는 것을 알 수 있었다. 이처럼 PIA 개인정보보호 감리 프로세스를 이용하여 사전에 개인정보영향 평가 검토를 하며 최소한의 개인정보보호를 위한 사전프로세스가 마련할 것으로 판단된다.

V. 결론

본 논문은 본 연구는 정보시스템 분석 및 설계 단계의 개인정보를 보호하기 위해 PIA 및 정보시스템 설계 단계 정보보호활동을 이용하여 정보시스템 분석 및 설계단계의 개인정보보호 감리 프로세스를 구축하고 연구하였다.

본문의 3, 4장을 통해 PIA 개인정보보호 감리 프로세스는 분석 단계 7개 통제항목을 이용하여 21개 세부점검항목을 도출하였으며 설계 단계의 경우 4단계(7개 통제항목)을 이용하여 24개 세부 점검항목을 도출하였다. 개인정보보호라는 목표를 달성하기 위해서 정보시스템의 개인정보보호 감리 프로세스를 제시하였으며, 개인

정보보호 감리 프로세스의 실효성을 확인하기 위해서 두 프로젝트에 개인정보보호 프로세스를 적용하여 기존 감리 프로세스와 대비하여 검증하였다. 특히 도출된 감리 점검항목을 기존 프로젝트에 재 적용하는 방식의 감리를 통하여 실효성을 검증하였다.

앞으로 지속적으로 발전하는 유비쿼터스 및 U-City에 사용 될 유·무선 장비간 통합 개인정보보호 감리 연구가 필요하며 본 연구에서 다루지 않았던 시험 및 구현단계에서의 개인정보보호 감리 프로세스의 정립에 대한 연구와 개인정보보호를 위한 보안 서버 구축 및 운영에 따른 감리방법에 대한 연구가 수행되어야 한다.

참 고 문 헌

[1] 남현수, 개인정보보호의 공법적 실현에 관한 연구,숭실대학교 대학원 석사논문, 2008.

[2] 심봉권, 개인정보보호 측면에서의 보안감리 방법에 관한 연구, 건국대학교 대학원 석사논문, 2008.

[3] 서석배, 차세대 전자정부 서비스의 개인정보보호 아키텍처 설계 방안에 관한 연구, 건국대학교 대학원 석사논문, 2008.

[4] Ontario, A user's Guide - Privacy Impact Assessment, 2001.

[5] 한국정보보호진흥원, 개인정보 영향평가(PIA) 교육 교재, 한국정보보호진흥원, 2006a.

[6] 송세현, 개인정보보호를 위한 프라이버시 영향평가 (PIA) 모델, 경기대학교 대학원 석사논문, 2004.

[7] 박순희, 이동통신사를 위한 개인정보 영향평가(PIA) 적용 방안에 관한 연구, 동국대학교 대학원 석사논문, 2006.

[8] 한국정보보호진흥원, 기업의 개인정보 영향평가 수행을 위한 가이드, 2005a.

[9] 한국정보보호진흥원, 정보시스템 구축단계별 정보보호 가이드라인, 2004.

[10] ISO/IEC, International Standard ISO/IEC 17799 Information technology Code of practice for information security management, 2000.

[11] 한국정보보호진흥원, 정보보호 거버넌스 개념 도입을 위한 정보보호 관리체계(ISMS) 발전 방안 연구, 2009.

[12] ISO/IEC 27001, International standard - Information technology - Security techniques - Information security management systems - Requirements, 2005.

[13] 한국정보보호진흥원, 정보시스템 구축단계별 정보보호 가이드라인, 2004.

[14] 문승준, 내부정보유출 통제를 위한 보안수준 평가방법 개발에 관한 연구, 조선대학교 경영대학원 석사논문, 2009.

[15] 서세일, 웹상에서 신원도용 및 프라이버시 보호를 위한 사례 연구, 남서울대학원 석사논문, 2007

[16] British Standard Institute, BS ISO/IEC 27001:2005, 2005.

저 자 소 개

김 희 완(Hee-Wan Kim) 정회원

- 2002년 2월 : 성균관대학교 정보공학과(공학박사)
- 정보관리기술사
- 정보시스템 수석감리원
- 2001년 2월 ~ 현재 : 삼육대학교 컴퓨터학부 교수

<관심분야> : 정보시스템 감리, 프로젝트 관리, 데이터베이스, 소프트웨어 공학

유 재 성(Jae-Sung Ryu) 정회원

- 2009년 8월 : 건국대학교 정보통신대학원(공학석사)
- 현재 : IBK시스템 네트워크 운용

<관심분야> : 정보시스템 감리, 프로젝트 관리, 정보시스템 보안

김 동 수(Dong-Soo Kim) 정회원

- 1981년 2월 : 광운대학교 전자계산학과(이학사)
- 2001년 2월 : 서울산업대학교 전자계산학과(공학석사)
- 2005년 2월 : 국민대학교 경영정보학과(경영학박사)
- 전자계산기조직응용기술사, 정보통신기술사, 정보시스템 수석감리원
- 현재 : (주)키삭 대표컨설턴트, 건국대학교 정보통신대학원 겸임교수

<관심분야> : 정보시스템 감리, u_city 감리, 프로젝트 관리, 소프트웨어공학