특집 08

병원 전자차트시스템에 대한 개인정보 영향평가 실시

신상규 · 세토 요이치 (산업기술대학원대학), 타카사카 사다무 ((주)메딕총연),
세키즈카 에이치 (국립 사이타마 병원)

목 차 »

1. 서 론
2. 개인정보 영향평가의 개요
3. 개인정보 영향평가의 실시 절차
4. 새 전자차트시스템의 개인정보 영향평가
5. 결 론

1. 서 론

현재, 독립행정법인 국립병원기구 사이타마 병원(이하, "사이타마 병원")은, 전자차트시스템 갱신을 계획하고 있다. 새로운 전자차트시스템의 도입에 따른 개인정보 유출에 대한 리스크를 관계자들이 사전에 인식하고 그에 대한 정보를 공유하며, 유출 리스크를 줄이는 것을 목적으로 한다. 이에 전자차트시스템의 기본 설계서에 대한 개인정보 영향평가를 실시했다.

해외에서는, 개인정보 유출을 미연에 방지하기 위한 수단으로서, 프라이버시 영향평가(Privacy Impact Assessment)가 주목받고 있다[1,2].

캐나다와 호주의 정부 기관이나 주 정부에서는, 개인정보를 취급하는 시스템을 구축할 때, 프라이버시 커미셔너(Privacy Commissioner)가 PIA를 실시하여 개인정보의 안전성을 사전에 평가하는 것이 예산 승인의 조건이며, 미국에서는 개인정보를 다루는 행정시스템을 구축할 때, 전자정부법 제208조에 의한 PIA 실시가 의무화되어 있다[3]. 일본에서도 번호법 제15조에 의해, 행정 기관 등이 특정 개인정보보호 평가를 실시하여 국민의 의견을 구한 후, 평가서를 작성, 특정 개인정보보호 위원회에 승인을 받고 보고서를 공개하게 되어 있다[4]. 특정 개인정보보호 평가는 프라이버시 영향평가와는 다르지만, 사전에 리스크를 평가한다는 공통점을 가지고 있다. 특정 개인정보보호 평가대상은 번호법에 관련된 행정 분야를 대상으로 하며, 민간 분야는 대상으로 하지 않았다. 일본의 민간 분야에서는 ISO22307에 부합하는 개인정보 영향평가가 실시되고 있다. 미국에서는 프라이버시 영향평가라 불리는데, 프라이버시 영향평가의 대상은, 기밀정보뿐만 아니라 일반적인 개인정보도 평가대상이다. 따라서 일본에서는 개인정보 영향평가라고 부른다. 본 논문에서는, 해외 사례 소개를 제외하고는 "개인정보 영향평가 (Personal information Impact Assessment, 이하 PIA)"를 사용한다. 본 논문에서는 기획 단

계의 전자차트시스템에 관해서 사이타마 병원이 작성한 “병원 정보시스템 기술 시방서(안)”에 대하여 산업기술대학원대학이 PIA를 실시하고, 그 결과를 정리한 것이다.

2. 개인정보 영향평가의 개요

개인정보 영향평가(Privacy Impact Assessment)란, 개인정보를 수집하는 정보 시스템을 도입 또는 변경할 경우 이에 따른 개인정보 유출에 관한 리스크를 명확히 하고, 개인정보 유출로 인해 이해 관계자들 사이에 미치는 영향을 “사전”에 평가하는 리스크 관리 방법이다. 개인정보에 관한 영향을 평가할 뿐만 아니라, 리스크의 회피 또는 감소를 위한 기술적인 변경·운용, 법 제도 정비를 촉진하는 것을 목적으로 한다[1-3,10,11]. 1990년대, 개인정보의 전자화가 진행됨에 따라 정보시스템의 프라이버시 문제가 대두되면서 PIA가 검토되기 시작했다.

PIA를 실시하는 목적은 예산 절감과 이해 관계자들 사이의 신뢰 구축에 있다. PIA는 실시 결과를 바탕으로, 필요에 따라 구축 시스템에 대한 사양의 변경을 요구할 수도 있다. 시스템 가동 전에 필요한 변경사항을 반영함으로써 가동 후 발생할 수 있는 개인정보보호 문제로 인한 시스템 중지나 그에 따른 비즈니스 상의 리스크, 시스템 보수비용을 줄일 수 있다. 또한, 실시 기관이 PIA 보고서를 공표함으로써 사생활과 개인정보 취급과 관련된 실시 기관, 개인, 매스컴의 3자가 함께 논의하는 자리를 제공할 수도 있다. 즉, PIA는 일종의 리스크 커뮤니케이션 수단인 셈이다.

영국에서는 PIA가 사회 제도로서 실시되고 있는 반면, 미국과 한국에서는 법으로 규정해 실시하고 있다[3,7]. PIA는 각 국의 사정에 따라 실시 방법이 다르다. 따라서 국제 표준화 위원회는 2008년에 TC68에 PIA 요구사항을 규정했다.

ISO 22307 Financial services--Privacy Impact Assessment는 국제 표준화 위원회 ISO TC68/SC7 (금융 서비스)에 의해 2008년 4월에 규정된 프라이버시 영향평가에 관한 국제 표준 규격으로[8], 사생활 보호 목적을 금융업계에 한정하지 않고, 다른 업종에도 적용할 수 있다.

ISO 22307은 “① PIA계획, ② PIA평가, ③ PIA보고, ④ 충분한 전문 지식, ⑤ 독립성과 공공성, ⑥ 대상 시스템의 의사 결정시 이용”이라는 6가지 항목을 PIA 실시 요구사항으로 규정하고 있다. 이 중에서 앞의 3가지가 PIA 실시 절차이며, 뒤의 3가지가 실시 체제이다.

3. 개인정보 영향평가의 실시 절차

3.1 개인정보 영향평가의 절차

(그림 1)은 개인정보 영향평가(Personal information Impact Assessment) 절차이다[9].

3.1.1 예비평가 및 실제 PIA 평가 실시 계획서 작성

대상 시스템의 실제평가를 실시하기 전에 예비평가를 실시한다. 예비평가에서는 실시 스케줄 및 체계 (인원) 확보, 실시 형태 등을 보고서로 정리한다. 다만 예비평가는 평가 의뢰기관 책임자의 판단에 따라 생략할 수도 있다. 예비평가 실시 후, 실제 평가 실시 계획을 정하고 PIA 프로젝트를 추진하기 위한 실시 체제를 정비한다. 또한, PIA의 대상 범위, 참조해야 할 법령, 규칙, 가이드라인, 조직 내부규정 등을 조사한다. 실시 의뢰기관은 평가 팀의 협력을 얻어 이러한 사항들을 프로젝트 계획서에 해당하는 PIA 실시 계획서로

	평가 실시 계획서 작성	평가 실시			보고서 작성
	프로젝트 계획	평가 준비	프라이버시 리스크 식별	프라이버시 리스크 분석	프라이버시 리스크 평가	보고
평가절차	평가 실시 체제의 정비	평가 관련 자료 수집	개인정보 식별	영향도 평가	필요한 리스크 대응방안 검토	보고서 작성
	대상 범위 확정	대상 시스템 분석	리스크 시나리오 식별	발생 가능성 평가	개인정보 영향평가	
	참조 법령·규칙, 가이드라인, 사내 규정, 계약서 등 조사	데이터 흐름도 작성	기존 또는 계획된 대책 식별			
	PIA 실시 계획서 작성	평가표 작성				
성과물	·PIA 실시 계획서	·시스템 분석서 ·데이터 흐름 분석서 ·평가표	·개인정보 관리대장 ·리스크 분석표	·리스크 분석표	·리스크 분석표 ·평가표	·PIA 보고서

(그림 1) 개인정보 영향평가 절차

정리한다.

3.1.2 PIA 평가

평가 대상 시스템의 프라이버시 리스크(개인정보 유출)를 평가하기 위해 평가 팀은, 대상 시스템을 이해(시스템 분석, 데이터 흐름 분석)한 후, 개인정보 유출 리스크를 식별하고 분석한다. 관할 부처가 지정하는 가이드라인이나 개인정보 보호에 관한 법령, 사내 규정 등을 근거로 평가의 기준이 되는 평가표를 작성한 후 그 평가표를 이용해 영향평가를 실시한다.

3.1.3 PIA 보고서 작성 및 공개

평가 팀은 프라이버시 리스크 영향평가 결과를 바탕으로 PIA 보고서를 작성한다.

3.1.4 보고서 작성 및 제출

PIA 보고서는 정보 보호 감사 보고서의 모델을 따라 다음 3가지 부문으로 구성된다.

(가) 도입 부문 : 목적, 기간(스케줄), 대상 범위, 체제(PIA 평가 팀, PIA 시행 의뢰 책임자)

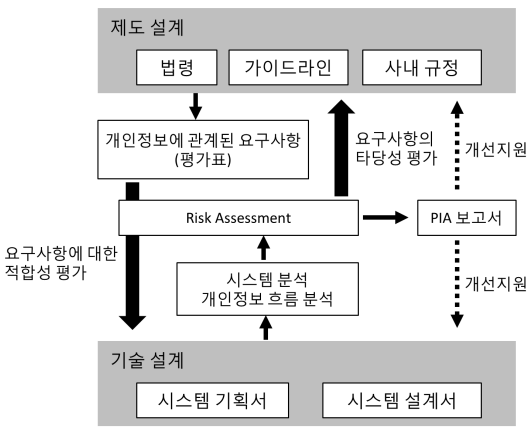
(나) 개요 부문 : 대상 시스템에 관한 기술(시스템 구성, 취급하는 개인정보 등), 리스크 평가 실시 절차 및 리스크 평가 기준, 실시 시 사용한 전문 지식.

(다) 의견 부문 : 대상 시스템이 계획하고 있는 안전 관리 조치에 대한 평가, 법령이나 가이드라인, 사내 규정 정비 등에 관한 평가.

실시 의뢰기관에 시스템 설계서에 대한 개인정보 유출 문제 발생 유무를 지적하고 시정 사항에 대한 조언을 한다. 보고 후에 실시 의뢰기관의 책임자는 Chief Privacy Officer의 조언을 받아 PIA 보고서를 승인하여 정식으로 발행한다.

3.2 개인정보 영향평가의 리스크 분석

일반적인 시스템 감사는 규칙으로 정한 요구사항을 평가 대상 시스템이 충족하고 있는지 여부를 일방적으로 평가한다. 이에 비해 규칙 자체의 평가와 연계해 실시한다는 점이 PIA의 특징이다[9].



(그림 2) 양방향 차이 분석 개요

제도 설계와 기술 설계를 동시에 평가하기 위해서 본 평가에서는 양방향 차이 분석이라는 리스크 평가 방법을 개발해 평가를 실시했다(그림 2)[12,13].

3.2.1 요구사항에 대한 적합성 평가

평가 대상 시스템의 기술 설계 문서(시스템 규격서나 설계서 등)가 요구사항을 충족하고 있는지 여부를 확인해야 한다는 점은 기존 평가 방법과 같지만, 리스크 평가를 실시하고, 기술 설계 문서에 계획된 안전 관리 조치 방안이 어떤 리스크와 관련되어 있는지를 밝힌다는 점은 기존 평가 방법과 다르다. <표 1>은 요구사항에 대한 적합성 평가의 판정 패턴을 나타낸다.

3.2.2 요구사항의 타당성 평가

요구사항의 타당성 평가에서는 검출된 리스크에 대한 대책 요구사항이 마련되어 있는지 여부를 확인한다. 대상 시스템이 가진 리스크에 대해 대책 요구사항이 없을 경우에는 부족한 부분을 검증한 후에 규칙을 정비하고, 운용 리스크 경감 대책을 강구하는 등의 대책을 마련하여 제도 설계 개선을 촉구한다.

〈표 1〉 요구사항에 대한 적합성 판정 패턴

No.	리스크	안전관리조치	판정
①	검출	충분	문제없음
②	검출	없음·불충분	기술설계 불충분
③	미검출	있음	비용의 적정 여부 검증필요
④	미검출	없음	문제없음

4. 새 전자차트시스템의 개인정보 영향평가

4.1 평가 대상 시스템 개요

시스템 분석 대상은 <표 2>에 나타낸 것과 같이 전자차트시스템으로, 전자차트시스템·의사회계시스템 및 문서관리시스템과 병원진료연계시스템(C@RNA)과 문서관리시스템(Yaghee)으로 구성된다.

사이타마 병원은 진료 부문, 검사 부문 등으로 구성되어 있으며, 각 부문의 업무에 대응되는 정보시스템이 존재한다. 그 중에서 병원시스템의 핵심을 이루는 처방시스템 및 전자차트시스템과 의사회계시스템이 이번 평가의 대상 범위가 된다. 병원진료연계시스템은 외부 병원과 연계되어 있지만 병원진료연계시스템과 전자차트시스템 간의 정보 교환 부분까지를 대상 범위로 하며, 외부 연계 기능에 대해서는 대상 범위에서 제외했다.

〈표 2〉 평가 대상 시스템 목록

No.	시스템	사용 목적
1	전자차트시스템	진료 기록, 처방, 간호 지원
2	의사회계시스템	의사 청구, 회계, 의료비 청구서, Diagnosis Procedure Combination
3	문서관리시스템(Yaghee)	문서 작성 지원 관리
4	병원진료연계시스템 (C@RNA)	지역 의료 시설과 진료 예약 연계
5	새 클라이언트시스템	새 클라이언트 및 서버

4.2 평가 실시 계획 작성 및 자료 수집

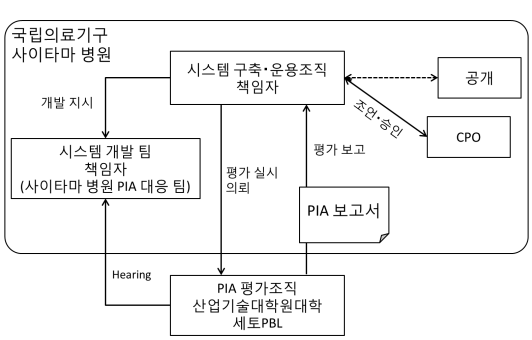
PIA에 의해 대상 시스템에 잠재하는 프라이버시 리스크를 밝혀내고 시스템 이용자의 프라이버시를 보호할 목적으로, PIA의 대상 범위, 작업 기간의 설정, 필요한 전문 지식 및 건강진단 종합시스템에 적용되는 법령이나 규칙을 조사하고 실시 체제를 구성했다. 이 결과를 PIA 실시 계획서로 작성했다.

4.2.1 평가의 실시 체제 구축

(그림 3)과 같은 실시 체제를 구축했다. 평가팀은 시스템 구축 운용조직과 영향평가를 실시하는 대학을 합동으로 구성했다.

팀의 멤버는, PIA에 관한 지식, 개인정보보호법에 관한 지식, 정보 보안 기술에 관한 지식, 정보시스템(예를 들면, 데이터베이스, 네트워크, 시스템 설계 등에 관한 지식), 전자차트시스템에 관한 지식을 갖춘 인재로 구성된다.

평가를 수행한 인원은, 5명×5개월(25명, 월 900시간)이다. 실제 평가 작업은 교원 1명과 학생 5명, 변호사(조언) 1명, 의료정보시스템 전문가(조언) 1명으로 실시했다. 학생은 PIA에 관한 지식을 학습하면서 대응했다.



(그림 3) PIA 실시 체제도

4.2.2 평가 자료 수집

평가를 위한 자료로 관련 법령·규칙, 대상 시스템 해당 문서, 실시 조직의 내부 정책 문서 등을 수집했다.

4.3 개인정보 영향평가 실시

평가 대상 시스템의 기본 설계서에 기재된 시스템 구성 확인 및 개인정보의 취득, 이용, 보관, 폐기까지의 데이터 흐름 분석을 실시했다.

4.3.1 시스템 분석

시스템 구성을 네트워크, 하드웨어, 소프트웨어 분야로 구분했으며, 리스크를 의도적인 것과 우발적인 것으로 나누어 정리했다. 분석의 방법은 일반적으로, ISMS (JIS Q 27002:2006)에서 활용되고 있는 ISO/IEC TR13335 (GMITS: Guidelines for the Management of IT Security)의 베이스 라인 어프로치, 비형식 접근, 상세 리스크 분석을 조합한 방법을 사용했다.

4.3.2 개인정보 흐름 분석

업무 분석은 사이타마 병원의 전자진료기록카드·의사시스템이 취급하는 개인정보를 대상으로 하고, 아래 순서로 실시했다.

(가) 사이타마 병원에서 받은 운용절차를 바탕으로 업무 프로세스에서 개인정보의 흐름을 업무 흐름도로 작성했다.

(나) 작성한 업무 흐름도를 바탕으로 업무별 작업 내용을 명확히 하고, 각각의 업무에서 취급되는 개인정보를 추출하여 개인정보관리대장을 작성했다. 또한, 추출한 개인정보의 중요도를 평가하여 정보자산대장을 작성했다.

(다) 개인정보관리대장, 정보자산대장을 이용하여 개인정보에 대한 리스크를 분석해 평가

했다.

진찰시 환자가 병원에 제공한 개인정보의 흐름에 따라, 업무 흐름도를 작성했다. 여기서 말하는 업무는 환자 개인정보를 전자진료기록카드·의사 시스템에 등록, 예약·진찰·검사·처방·입원 기록, 진료기록 작성, 회계업무 등의 작업을 가리킨다.

4.3.3 개인정보에 관한 리스크 분석

시스템 구성 및 개인정보 흐름을 바탕으로 개인정보 리스크를 분석했다. 병원 의료 업무에서 취급되는 개인정보는 개인을 특정할 수 있는 기본적인 정보부터, 검사 결과, 병력 등 민감한 정보까지 포함하고 있다.

개인정보관리대장에서 각 정보를 취급할 때마다 발생할 수 있는 예상 리스크 대책 상황에 대하여 병원에서 받은 운용관리규정 등의 자료를 토대로 분석을 실시했다. 운용절차나 운용관리규정 등에서 이미 리스크 대책이 마련되어 있는 경우를 제외하고, 개인정보 유출 가능성이 있는 리스크 항목을 추출했다.

4.4 평가 대상 시스템 평가기준 마련

관련 법령 및 규칙을 바탕으로 평가 항목의 체크 리스트를 기술한 평가표를 작성했다. 평가표는 OECD8원칙에 따라 항목을 분류한 후에, 각 항목에 관한 구체적인 체크 항목을 중분류, 소분류와 같이 계층적으로 구성해, 34개 항목을 작성했다. <표 3>에 평가 항목의 개요를, <표 4>에 평가 항목의 분류와 항목 수를 나타낸다.

〈표 3〉 평가표의 항목

항 목	설 명
대분류 (OECD8원칙)	OECD에서 정한 개인정보 기본원칙을 항목 분류에 사용
평가 항목	평가 대상 시스템에 대한 요구사항을 질문 형식으로 기재
법령·규칙	요구사항의 근거가 되는 법령이나 규칙, 가이드라인 등
평가 결과	평가 항목에 대해 확인한 사실
지적·권장사항	평가 결과가 부적합 또는 평가 거부의 경우, 지적사항과 권장사항을 기재
참고 자료	검증 결과의 근거가 되는 자료와 공청회 결과를 기재

〈표 4〉 평가 항목의 분류와 문항 수

대분류	내용	항목
목적 명확화 원칙	이용 목적을 분명히 기재	1
이용 제한의 원칙	목적 외 이용 동의, 제3자 제공의 공동 이용	2
데이터 내용의 원칙	데이터의 정확성을 확보	23
안전 원칙	위탁처의 감독, 안전 관리 조치	7
공개의 원칙	데이터 취득에 있어서 이용 목적의 통지 등	1
합계		34

4.5 평가 결과

평가표는 각 항목별 질문에 대해 기본 설계서를 참조하여 평가를 실시했으며 적합, 부적합, 평가 거부(평가 시점에서는 미확정인 것들)의 3가지로 구분했다.

평가 구분에는 정보 보안 감사에서 이용하는 3분류(중대한 미비, 미비, 경미한 미비)평가 방법을 사용했다. 상세한 평가 구분을 <표 5>에 나타낸다.

4.5.1 리스크 대책의 적합성 평가

본 평가의 결과 총 34개 평가 항목 중에서 부적합 1건, 경미한 부적합 1건으로 판정되었다. 지적된 항목 내용과 지적사항을 <표 6>에 나타낸다.

4.5.2 대상 시스템의 리스크 분석표에 따른 요구사항에 대한 미비성 평가

"시스템 분석서", "개인정보에 관한 업무 흐름 분석서"에서 검출된 리스크 중, 평가표에 기재되

〈표 5〉 평가 구분

리스크 대책의 적합성	요구사항에 대한 미비성	구분 설명
중대한 부적합	중대한 미비	개인정보 유출에 직접 관련되는 경우에 해당하며, 발생할 가능성이 높다.
부적합	미비	개인정보 유출에 직접 관련되는 경우이지만 발생할 가능성이 낮다.
경미한 부적합	경미한 미비	개인정보 유출에 직접적으로 관련되지 않는 경우이다.

〈표 6〉 부적합 항목 목록

평가 항목	지적사항	평가 결과
2-1 목적 외 이용 동의	본 건은 부적합에 해당한다. 본래의 이용 범위를 넘어서 사용하는 경우, 환자의 동의 없이 개인정보를 제공하지 않는 것으로 규정되어 있다. 하지만, "L1_001_개인정보 보호방침"의 개인정보보호 책임자" 부분이 공란이고, 실제로 책임자, 운용 담당자, 감사 책임자, 기기 책임자 안전 관리자가 정해져 있지 않다. 시급히 조직 체제를 갖출 필요가 있으며 운용 관리 규정 안에 명시해야 한다.	× 부적합
5-4 시스템 관련 용역 업체의 관리	본 건은 경미한 부적합에 해당한다. 의사시스템의 운영 등 준비 작업에 관한 개인정보 취급이 동반되는 업무를 위탁하는 경우, 업무 위탁 계약서에 개인정보의 안전 관리에 관한 조항을 포함하도록 해야 한다. 배상 책임에 관해서도 기술되어 있다. 시스템 유지보수 업무에서 원격 관리는 유지보수 계약을 체결한 시스템벤더에 국한한다고 규정되어 있지만 유지보수 계약 중에 개인정보의 안전한 취급에 대한 규정은 없다. 원격 관리 계약에 개인정보 취급에 대한 규정을 넣어야 한다. 또한 원격 관리, 사무 처리 용역 업체 회사의 선정 기준을 미리 마련해 두고 위탁 업체 선정 시의 평가에 포함시켜야 한다.	× 부적합

〈표 7〉 지적·조언 건수

리스크 대책의 적합성		요구사항에 대한 미비성		조언 사항
중대한 부적합	0	중대한 미비	0	8
부적합	1	미비	1	
경미한 부적합	1	경미한 미비	1	

지 않은 사항을 추출했다. 현시점에서의 가이드라인 등의 미비를 지적한 것이다. 지적·조언 건수는 <표 7>과 같다.

5. 결 론

본 영향평가에서는 사이타마 병원의 새로운 전자차트시스템에 대해 34개 항목에 대한 개인정보 영향평가를 실시했다. 사이타마 병원의 전자차트 시스템은 의료정보시스템의 안전 관리에 관한 가이드라인의 요구사항을 만족하도록 설계되어 있었다. 그러므로 기획 단계의 설계서로 이 기술사양서를 이용해 적절한 시스템을 충분히 구축할 수 있다고 평가할 수 있다. 다만, 개인정보보호 관리책임자의 부재, 시스템 관련 용역업체 선정 기준 미비라는 부적합이 있었다. 개인정보보호에 충실하기 위해서는 이들의 부적합 사항에 대한 조속한 대응이 필요하다. 의료정보시스템의 안전 관리에 관한 가이드라인에는 암호화 방법 및 새로운 클라이언트 환경에 관한 요구사항이 부족하다는 지적이 있었다. 가이드라인이 보안 관점에서 부족했으며 이에 대한 빠른 시정이 요구된다. 시스템 발주자는 보안에 관한 요구 사양을 정리하여 시스템벤더에 요구사항을 제시할 필요가 있

다. 요구사양의 작성은 공적 기관에 의한 보안 기준이나 가이드라인을 이용할 것을 권장했다. 사이타마 병원에는 이러한 이유로 ISO/IEC15408 인증이나 전자정부 권장 암호 리스트 등에 제시된 요구사항을 참고하도록 했다. 특히 의료시스템에서 취급하는 개인정보는 민감한 정보가 많으므로 안전에 대한 충분한 배려가 필요하다. 이번 지적 사항이 평가 대상 시스템에 반영되는 것을 확인하기 위해서 상세 설계 시 개인정보 영향평가를 다시 실시할 것을 권장했다.

감사의 말

본 연구는 산업기술대학원대학의 Project Based Learning 교육의 일환으로 실시되었다. 오카자키 미치야, 오카모토 나오코, 카와구치 하루유키, 사카모토 마코토, 나가노 마나부의 협력으로 이루어 졌다. 또한 독립행정법인 국립병원기구 사이타마 병원에 본 연구의 기회를 준 것에 대해 여기에 감사의 뜻을 표한다.

This work was supported by JSPS KAKENHI Grant Number 25240017.

참 고 문 헌

[1] 세토 요이치 외, 프라이버시 영향평가 PIA와 개인정보보호, 중앙경제사, 2010.
[2] David Wright, Paul De Hert, “Privacy Impact Assessment,” Springer Verlag, 2nd ed, 2012.
[3] 세토 요이치, “프라이버시 영향평가의 평가 방법에 관한 조사 연구,” 산학 전략적 연구 포럼, 2007.
[4] 번호법 실무 연구회, 번호법 시행으로 바뀌는 지자체 업무, 교우 세이, 2013.
[5] 신영진 저, 세토 요이치, JIPDEC역, 정보화 사회의 개인정보보호와 영향평가, 게이소쇼보, 2014.
[6] 안전행정부, KISA(한국 인터넷 진흥원), 개인정보 영향평가 수행 가이드, 2012.
[6] 신상규, 세토 요이치, “한국에서의 프라이버시 영향평가 제도와 실시 상황,” SCIS2014, 2014.
[8] ISO22307 Financial services -- Privacy impact assessment, 2008.
[9] 세토 요이치, “스마트 시티에서의 프라이버시 영향평가 적용,” IEEJ Tran.EIS, Vol.133, No.7, pp.1427-1435, 2013.
[10] 세토 요이치, 실천적 프라이버시 리스크 평가기법, 근대 과학사, 2014.
[11] 세토 요이치, “개인정보 영향평가 PIA의 생각과 실시 절차 － 디자인에 의한 프라이버시로서 PIA－,” 법과 컴퓨팅학회 제3회 소그룹 연구회, 2013.
[12] 와타나베 신타로, 세토 요이치 외, “프라이버시 영향평가의 건강진단종합시스템에 적용,” CSS2012, 2012.
[13] 마에시마 하지메, 세토 요이치, “프라이버시 영향평가 실시에 있어서의 리스크 평가 검토,” 일본정보처리학회, 2013.

저 자 약 력

신 상 규

이메일 : shin@aiit.ac.jp

- 2010년 게이오대학 박사(공학)
- 2010년~2011년 게이오대학 방문연구원
- 2011년~현재 산업기술대학원대학 조교수
- 관심분야 : 데이터베이스, 정보시스템, e-Learning, 개인정보 영향평가

세토 요이치

이메일 : seto.yoichi@aiit.ac.jp

- 1979년~2006년 (주) 히타치 제작소 시스템 개발 연구소 보안 연구센터 센터장, 보안 비즈니스 센터 센터장, 주관 연구원 역임
- 2006년~현재 산업기술대학원대학 교수
- 관심분야 : 정보보호, 개인인증, 개인정보 영향평가

세키즈카 에이치

이메일 :
esekizuk@wakho.hosp.go.jp

- 현재 국립 사이타마 병원 병원장
- 의학 박사, 일본 소화기병학회 전문의 · 지도의

다카사카 사다무

이메일 :
s.takasaka@medical-ict.com

- 1978년~2006년 NEC 소프트(주)
- 2012년 산업기술대학원대학 정보시스템학(석사)
- 2006년~현재 (주)메딕총연