情報保護學會論文誌
第16卷 第3號, 2006. 6

유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임워크 적용 방안*

홍 승 필,[1†] 이철수[2‡]

[1]성신여자대학교 컴퓨터정보학부 [2]경원대학교 소프트웨어 대학

Privacy Framework in Ubiquitous Computing Environments*

Seng-phil Hong,[1†] ChulSoo Lee [2‡]

[1]Sungshin Woman's University, [2]Kyungwon university

요 약

정보사회에서는 사회 구성원 개개인의 욕구를 충족시키는데 정보가 핵심적 역할을 하고 있다. 특히 유비쿼터스 컴퓨팅 환경에서는 개인 활동이 증가함에 따라 개인정보의 노출이 심해지고 개인정보 불법 취득도 점차 많아지고 있다. 이에 본 논문에서는 안전하고 효과적인 개인정보 관리체계와 기술적 구현이 용이하도록 개인정보 프레임워크를 제시하고, 시스템 개발자나 개인정보를 다루는 사업자 측면에서 개인정보 시스템을 설계하고 구현하기에 용이하도록 5단계의 구체적인 방법론을 제시하였다. 특히 제시된 방법론이 실 환경에 효과적으로 활용될 수 있도록 체계적인 개인정보 보호 시스템 개발 방안을 시스템 아키텍처 측면에서 소개함으로써, 본 논문의 활용 방안을 제시하였다. 본 논문에서 제시된 개인정보보호 프레임워크와 방법론은 실제 유비쿼터스 내 점점 중요시 되어가고 있는 개인정보 보호 측면에서의 방향성 제시 및 실제 엔지니어나 개발자 측면에서 이론위주의 설명보다는 실제 활용이 가능한 새로운 접근방안을 제시 할 수 있다고 사료된다.

ABSTRACT

Information is playing a key role in sufficing the needs of individual members of the society in today's rapidly changing environment. Especially, the cases of illegal gathering of privacy information will increase and the leakage of privacy information will grow as the individual activities in the ubiquitous computing environment. In this paper, we suggested the privacy framework in order to make design and implementation of secure and effective privacy management system. And, we also introduced the methodology which is represent to 5 specific stages in order to suggest to the privacy system development guideline from the standpoints of the privacy system operator or developer. Especially, we tried to determine whether the suggested methodology can be effectively used in the real computing environment or not by making necessary investments in management (privacy policy) and technical (system architecture) sides. We believe that the privacy framework and methodology introduced in this research can be utilized to suggest new approach for showing direction from the privacy protection perspective, which is becoming more important in ubiquitous environments, and practical application rather than providing conceptual explanation from the views of engineer or developer.

Keywords : *Privacy, Ubiquitous Computing, Security Policy, Framework, Architecture, Methodology*

Ⅰ. 서 론

유비쿼터스 컴퓨팅(Ubiquitous Computing)이란 다양한 종류의 컴퓨터가 사람, 사물, 환경 속으로 스며들고 서로 연결되어 언제 어디서나 컴퓨팅을 구

접수일: 2006년 4월 17일; 채택일: 2006년 5월 30일
* 본 연구는 성신여자대학교 학술연구조성비 지원에 의하여 수행하였습니다.
† 주저자, philhong@sungshin.ac.kr
‡ 교신저자, csl100@kyungwon.ac.kr

현할 수 있는 환경을 말한다. 유비쿼터스(Ubiquitous)는 라틴어에서 유래한 것으로 '도처에 널려 있다', '언제 어디서나 동시에 존재 한다'라는 의미로 사용 한다.[1]

유비쿼터스 환경에서는 다양한 비즈니스 환경에 준하는 개인 활동이 증가함에 따라 개인정보의 노출이 심해지고 개인정보 불법 취득도 점차 많아지게 될 것이며, 이러한 관련 서비스를 활용하기 위하여 각 단계마다 ID와 비밀번호, 인증 등을 필요로 한다. 현재도 주민등록번호만으로 휴대전화기를 타인명의로 구매하고, 타인명의의 전자우편을 가지고 상거래를 성사시킬 수 있다. 유비쿼터스 컴퓨팅 환경은 외지에서 집안의 각종 가전과 디바이스를 작동 시킬 수 있어 정보의 가용성이 더 넓어지고 있으나, 그와 더불어 개인정보 침해 및 정보의 역공학 측면에서 그 문제점이 점점 더 대두되어지고 있는 현황이다. 이렇듯 개인정보의 부적절한 사용으로 인한 침해 문제는 유비쿼터스 컴퓨팅이 가져다 줄 긍정적 파급효과를 가리는데 결정적인 요인이 될 수 있기에 개인정보의 보호는 중요하다.[2,3]

이에 본 논문에서는 개인정보 시스템 설계 및 개발 측면에서 안전하고 체계적으로 사용할 수 있는 개인정보 프레임워크와 개발방법론을 제시하고, 이를 효과적으로 관리하고 구현할 수 있도록 관리적, 기술적 측면에서의 활용방안을 제안하였다.

본 논문은 1장에서 본 논문 구성에 대한 간략한 소개와, 2장에서는 개인정보 관련 연구 및 개인정보 이슈를 정리해 보고, 3장에서는 개인정보 프레임워크를 제시하고, 설명하였다. 4장에서는 개인정보 개발 시스템을 방법론 측면에서 5단계로 나누어서 제시하였다. 5장에서는 제시된 개인정보 프레임워크 기반의 개인정보 시스템 구현 및 활용 방안을 개인정보 정책 설정 및 역할 기반의 접근제어측면과 개인정보 시스템 아키텍처측면에서 제안하였고, 6장에서는 결론과 향후 연구 방안을 소개하였다.

II. 개인정보 관련 연구

개인정보는 학자마다 또는 관련 규범에 따라 다양하게 정의되고 있어 웩스(Wacks)처럼 개인의 건강상태, 신체적 특징, 사상이나 신념과 같은 정신세계, 학력·경력·재산상태, 사회적·경제적 지위 등 개인에 관한 사실·판단·평가를 나타내는 모든 정보를 개인정보로 넓게 파악하는 학자가 있는가 하면 특별히 민감한 정보만을 개인정보로 보는 견해도 있다[4-6].

개인정보란 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"를 말한다.[7,8]

1. P3P (Platform for Privacy Preference)

P3P는 W3C(the World Wide Web Consortium)에서 개발한 프라이버시보호 표준기술 플랫폼으로써 구체적인 목표는 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자 측면에서 정보공개 수준과 비교하여 정보를 선별적으로 제공하는 것이다. 실제적으로 P3P는 웹 환경 내 HTTP를 통해 사용자 개인정보 정책을 전송하는데 필용한 메커니즘(데이터의 표준 스키마, 개인 정보 공개 표준, 웹 페이지 및 쿠키와 관련된 개인 정보 정책 수단, 개인 정보 정책을 표현하는 XML 형식 등)을 정의하고 있다[10].

2. OECD(Organization for Economic Co-operation and Development) 가이드라인 기준

개인정보의 국제법적·제도적 측면에서 중요한 연구 방향 중 한 가지는 OECD에서 제시하는 "프라이버시 보호 및 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)" 부분이다[9]. OECD 기준은 주로 정보주체의 동의 절차에 대한 명시가 중요한 내용으로 포함되어 있다. 즉 개인정보에 대한 관리가 정보주체의 동의절차와 수집경로 그리고 이용목적에 대한 고지가 어떻게 이루어지고 있는가 하는 점이 중요한 문제이다. 이에 대한 기준으로는 아래와 같은 8가지(수집 제한, 정확성 확보, 목적명시, 이용제한, 안전성, 공개, 개인참여, 책임) 원칙이 중요시 되어 지고 있다.

OECD가이드라인의 8대 원칙과 비교한 국내 개인정보보호 현황에 대해 간략히 요약하면 다음과 같이 개인적으로 분석하여본다.[11,12]

개인정보 보호에 대한 공공기관의 개인정보 보호의 범위가 제한적이고 모호하다. (OECD 기준으로

보면 보호의 범위가 제한적일 뿐만 아니라 목적 명확화의 원칙에 미달한다고 보여 진다.)

표 1. OECD의 개인정보 보호원칙

원칙	내 용
수집제한	개인데이터의 수집에 제한을 두어야 한다. 어떠한 개인 정보도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.
정확성확보	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적명시	개인정보는 수집 시 그 수집목적이 명확히 제시하고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다.
이용제한	개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전상확보	개인데이터는 그 분실 또는 불법적인 엑세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.
공개	개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 하낟.
개인참여	자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다.
책임	데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

개인정보 수집의 원칙이 모호하게 운영되고 있어 국제적 기준에 미치지 못하고 공공부분의 경우 예외가 많아 기본권을 침해할 우려가 있다고 보여 진다.

개인정보 데이터베이스 등의 공고 및 게시가 형식적이고 부실하다.

3. 유비쿼터스 환경 내 개인정보 이슈

빠르게 발전하고 있는 유비쿼터스 컴퓨팅 기술은 점점 고도화, 분업화 되면서 사용자의 편의성을 증대하고 있지만, 그와 관련 된 역기능 측면에서도 우려의 목소리가 커지고 있다. 무엇보다 유비쿼터스의 기본개념인 '어디에서나 컴퓨팅을 이용한다'는 것은 곧 어디에서든지 정보가 누출되고 왜곡될 위험이 있다는 것을 의미한다. 한 예로 유비쿼터스 환경 내 개인정보의 대표적인 적용 방안을 고려 해 보면, 현재 주민등록번호체계를 기준으로 개인정보의 개인화 경향(개인프로파일링)이 급속하게 확산되고 있고 이로부터 발생하는 인권침해 및 범죄 등에 활용될 가능성이 커지고 있다. 더욱이 현행의 정보사회로부터 이러한 침해가 발생하고 있는바 향후 유비쿼터스 컴퓨팅 환경하에서는 더욱 확대되고 전면적인 개인정보침해 또는 유해의 가능성이 농후하다고 보여 지며, 개인정보 보호 측면에서 고려하여 할 주요 사항은 아래와 같이 정리될 수 있다.

- 익명성(Anonymity) 또는 아호(Pseudonymity): 사용자 정보는 불법적 또는 악의적 목적으로서의 인용 측면에서 보호 하는 측면에서, 사용자 정보에 대한 책임추적성(Accountablity)이 보장되어야 하며, 적용되는 목적에 따라 다른 등급 차원에서의 익명성이 보장 되어야 한다.
- 사용자 동의(Notice): 유비쿼터스 환경 내 점점 개인정보가 분업화, 다각화 되어 지면서, 한번 입력 된 개인정보가 필요한 곳에 효과적으로 사용되어지는 방법과 정보가 필요한 곳에서만 사용자의 동의아래 사용되어질 수 있는 방안이 필요하다.
- 정보의 수집 및 제어(Information gathering and Access): 사용자는 필요시 자기 정보에 대하여 접근 및 변경이 용이하여야 한다. 혹 사용자의 동의 없이 개인정보를 접근하고, 수집하려 할 때를 고려하여 제도적, 기술적 측면에서 개인정보를 보호하기 위한 접근 제어 방안은 매우 중요한 개인정보 해결방안 중의 하나이다.
- 정보보안(Security): 개인정보를 활용(수집 및 관리·운영) 측면에서 기술적, 제도적, 관리적 측면에서 혹 발생 될 수 있는 위협 요소에 대하여 그 피해를 최소화하기 위한 예방이 필요하며, 모니터링·교정 측면에서 정보보안 기술 및 정책, 절차 및 지침 등을 활용 하여야 한다.

위의 사례를 기반으로, 개인정보에 대한 침해유형은 크게 다음 6가지로 구분해 볼 수 있다. 1) 부적절한 접근과 수집, 2) 부적절한 모니터링, 3) 부적절한 분석, 4) 부적절한 이전, 5) 원하지 않은 영업행위, 6) 부적절한 저장 등이 있으며, 이는 지식정보사회의 발달과 더불어 점점 증가하는 유비쿼터스 환경내 사용되는 개인정보들은 개인적으로나 사회적으로 1)개인의 사적 공간, 2)개인의 안전성, 3)사회적 배제(Social Exclusion) 초래, 4)기업과 소비자 사이에 힘의 불균형 측면에서 중대한 위협이 될 수 있다[11].

다음 장에서는 제시된 개인정보 이슈에 대하여 개인정보 프레임워크(Privacy Framework)을 통한 해결 방안을 제시하고자 한다.

Ⅲ. 개인정보 프레임워크

개인정보 프레임워크는 정보보안의 3대 원칙인 기밀성(Confidentiality), 무결성(Integrity), 그리고 가용성(Availability) 외 개인정보에 대한 권한(Privilege)을 보장하는 것을 목표로, 이러한 전략목표를 성취하기 위해 제공되어야 하는 개인정보 메커니즘은 OECD 에서 제시하는 원칙(정보수집 및 활용의 제한, 정보의 정확성, 사용목적, 공개정도, 개인 참여도)을 참조로 고려하였으며, 이는 개인정보 적용영역 또는 대상에 따라 관리적 측면, 서비스 측면, 그리고 기술적 측면으로 크게 세 영역으로 나누어 볼 수 있다.

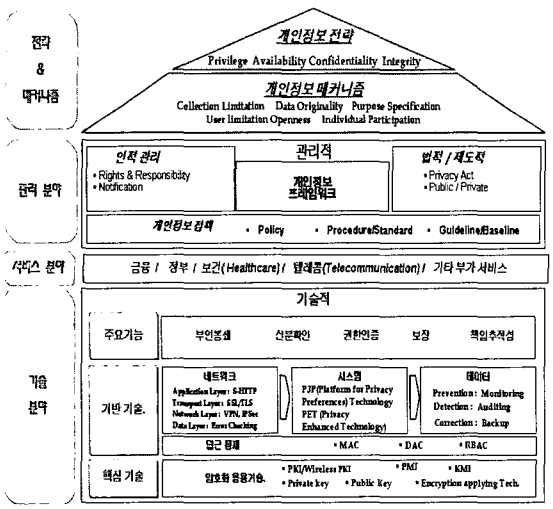

그림 1. 개인정보보호 프레임워크

관리 측면은 개인정보 관련 인적·관리적·제도적 측면을 고려하여 개인정보의 예방 측면에서 혹 발생될 수 있는 개인정보 오·남용에 대비하여야 한다. 즉, 악의적 목적을 대상으로 개인 동의 없이 개인 금융정보, 주민정보 등이 사용되었을 때 처벌을 위한 명확한 법적 대응 방안을 제시하고 아울러 기술적 측면과 연동하여 개인정보의 오남용을 증명 할 수 있는 절차(procedure)나 기술적 가이드라인이 구체적으로 제시 되어야 한다.

서비스 영역은 개인 사용자 측면에서 접할 수 있는 영역별 특성을 고려하여 정부차원에서 공개되어 사용되어지는 영역과 상업적 측면에서 사용될 수 있는 공개 정보의 정도를 고려하여 제시되어야 한다. 이는 향후 개인정보 관리 측면에서 개인정보 정책, 지침, 절차를 적용하는 기준을 제시하고, 그에 준하는 개인정보의 접근 통제 규정을 만들고 실행할 수 있도록 지정한다. 특히 고객정보를 활용한 서비스 분야는 향후 개인정보영향 평가와 같은 제3의 신뢰 할 수 있는 기관이나 조직으로부터의 개인정보 구축 시스템에서 가용 서비스 분야에 대한 정기적인 감시 모니터링 제도를 도입하여 개인정보 서비스에 대한 보장성(Assurance)을 유지 할 수 있도록 해야 할 것이다. 새로 구축되는 신규 서비스나 시스템, 또는 기 구축된 개인정보 시스템 측면에서도, 궁극적으로 안전한 개인정보 서비스를 제공하기 위하여서는 관련 정보보호 메커니즘을 간과 할 수 없으며, 이런 이유로 기업의 업무지속성 계획(Business Continuity Planning), 재난복구 계획(Disaster Recovery Planning), 전사적 개인정보시스템 관리(Enterprise Privacy Information Management)라는 세 가지 관점에서 관리적 측면(정책수립, 인적보안 관리, 물리적 보안 관리)이 강조되며, 기술적 정보보호 분야와도 유기적인 결합이 이를 뒷받침되어야 한다.

개인정보 기술영역을 분류함에 있어서는 수직으로는 기술의 쓰임새에 따라 세 가지 계층별 분류(요소기술·기반기술·응용기술)를 수평적으로는 각 계층 내에서 기술의 적용범위나 적용대상에 따라 영역별(Network, System, Data, Access Control) 분류와 상세 계층별(복합/단일/기반응용, 네트워크 4계층 모형) 분류를 병행하였으며, 특히 사용자 측면에서 주워진 개인정보 정책을 쉽게 적용하고 웹의 브라우저 환경에서 쉽게 개인정보의 보호 방안을 지향하는 P3P(Platform for Privacy Preferences)

기술과 PET (Privacy Enhanced Technology) 기술을 지원 할 수 있도록 설계하고 구현 되어져야 한다.

요소기술은 정보기술시스템의 기반을 형성하는 기술로, 만일 이러한 기술이 밑받침되지 않는다면 현실세계를 Cyber상에 그대로 재현할 때 반드시 전제되어야 할 안전성과 신뢰성을 유지할 수 없다. 기반기술은 요소기술을 바탕으로 물리적인 정보인프라를 건설하기 위해 요구되는 기술로서 정보의 생성과 처리(System 영역), 정보의 저장(Data 영역), 정보의 공유(Network 영역)를 담당하는 인프라를 구축한다.

응용기술은 정보인프라를 바탕으로 현실세계의 사회경제활동을 디지털화하여 신뢰성, 편이성, 생산성 향상을 도모하며, 개인정보보호 측면에서 적용된 요소·기반·응용 기술은 아래와 같이 개인정보 관련 상세 기술표를 참고 할 수 있다.

표 2. 개인정보관련 상세 기술 분류표

대분류	중분류	소분류	솔루션
응용 기술	복합응용기술	전자지불	■ e-Payment (Credit Card, E-Cash/E-Check)
		컨텐트 보안 개인정보응용기술	■ 바이러스 ■ 전자메일
			■ Digital Right Management (DRM) ■ PET (Privacy Enhanced Technology)
	단일응용기술	IC카드	■ Smart Card
		개인정보보호	■ P3P (Platform for Privacy Preferences)
	인프라 기술	공개키기반구조 (PKI)	■ PKI/PMI (CA/SSO, Directory /LDAP, Attribute CA / RBAC, KMI)
		권한관리구조 (PMI)	
		커버리	
기반 기술	네트워크	응용계층	■ 방화벽(Firewall) ■ 침입탐지시스템(IDS)-N/W기반 ■ 가상사설망(VPN)
		전송계층	
		네트워크계층	
		데이터계층	
	시스템	소프트웨어	■ 침입탐지시스템(IDS)-Host기반 ■ 취험분석관(RAT)
		하드웨어	
	데이터	예방(Prevention)	■ DB접근제어, 그룹통제
		탐지(Detection)/ 교정(Correction)	■ DB Backup
	접근제어	강제 접근제어	■ Access Control (Access Control List, Access Control Matrix, Security labeling, Constraint, User Privilege, Delegation)
		임의 접근제어	
		역할기반의 접근제어(Role-Based Access Control)	
요소 기술	암호화	비밀키, 공개키	■ Crypto Toolkit
		암호화 알고리즘	

이러한 개인정보 보호를 위해 적용되는 정보보호 관련 메커니즘은 · 사용자 인증(Authentication), 사용자 권한허가(Authorization), 거래의 부인방지(Non-repudiation), 정보기술 시스템의 보안인증(Assurance), 보안감사를 통한 책임추적성(Accountability)의 기능을 들 수 있다.

Ⅳ. 개인정보 보호 개발 방법론

앞서 제시한 개인정보 프레임워크는 개인정보의 기본 목적과 메커니즘을 통한 개인정보의 보호 측면에서 해야 할 추진 방안을 정의하고, 관리적 기술적 측면에서 개인정보가 적용되는 비즈니스나 서비스 영역을 대상으로 필요한 요소를 제시해 보았다. 이번 절에서는 개인정보보호 프레임워크를 기반으로 실제 어떻게 개인정보 시스템을 분석 설계하고 개발되어야 하는 방향성을 제시해 주는 개인정보보호 시스템 개발관련 방법론을 제안한다.

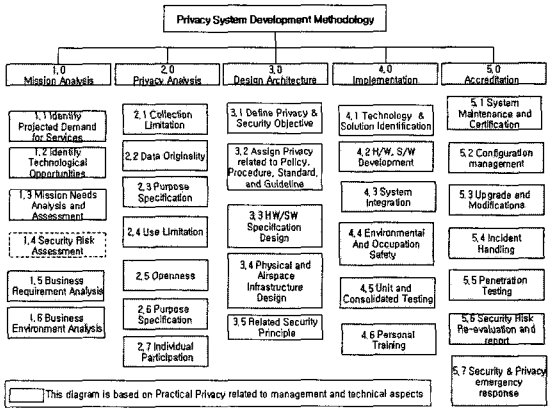

그림 2. 개인정보 보호 시스템 구축 방법론

개인정보 시스템 개발 방법론은 크게 5가지 단계로 구분하고, 그 중에서도 개인정보관련 수행하여야 할 중요한 미션은 흰색으로 표기하였으며, 각 미션에 관련 된 그 주요 역할과 세부 절차는 다음과 같다.

1. 환경 분석(Mission Analysis): 개발하고자 또는 적용하고자 하는 시스템이나 비즈니스 환경에 대한 이해와 그에 관련된 기술적, 환경적 분석을 그 목표로 하고 있다.
2. 개인정보 영향 분석(Privacy Analysis): 개인정보 보호 및 활용 측면에서 OECD에서 제시하는 개인정보 관련 주요 원칙을 고려하여 1단계 파악된 환경 측면에서 개인정보에 대한 수집 제한, 정확성 확보, 목적명시, 이용제한, 안전성, 공개정도, 개인참여 정도, 책임성 등을 파악하고 그 현황을 분석하며, 이때 개인정보 관련 정량적·정성적 위험을 정의하는 단계가 필수적이다. 또한 개인정보 관리적, 제도적 측면에서 가용성 대비 개인정보 활용 관련 안전성에 대한 고려가 필요한 단계이다.
3. 개인정보 시스템 설계 (Design Architecture): 환경 분석을 기반으로 개인정보 현황 분석을 기반으로 개인정보 정책, 지침, 가이드라인을 정의하

고, 시스템 구축에 필요한 방법이나 구축방안을 H/W, S/W 측면에서 설계하는 단계이다.

4. 구현(Implementation): 개인정보 정책에 준한 필요한 기술 및 개발 환경을 파악한 후 개발 일정에 준하여 단계별 개발을 실시한 후 단일 테스트, 통합 테스트 단계를 통하여 개발을 완료하는 단계이다.
5. 보장성(Accreditation): 개발 완료 후 구축된 개인정보 시스템의 안정성을 보장하는 단계로, 관련 운영자, 관리자에 대한 교육, 시스템 수정 및 변경 후 형상관리, 수집된 개인정보에 대한 접근제어 및 주기적인 백업 등이 이루어지는 부분이다.

V. 개인정보 프레임워크 활용방안

개인정보 프레임워크를 실 환경에서 시스템 엔지니어(System Engineer)나 개발자가 용이하게 사용 할 수 있도록, 개인정보 관리 측면에서, 향후 관련 시스템 설계 및 구현, 운영의 기본이 되는 개인정보 정책(Privacy Policy) 설정에서 논리적 접근제어 방향성 제시에 이르기까지의 3가지의 순차적 추진 방안으로 실제 적용이 가능한 방안을 제시 한다.

1단계: 개인정보보호 정책은 정보보호의 중요도에 따라 5등급으로 분류하여 사용자 측면(단계별 분류의 상위부분)과 개인정보를 사용하는 정부나 회사 측면(단계별 분류의 하위부분)으로 구분하여 그 기본 구성을 그림 3과 같이 가이드를 제시 한다.

아래 그림 4는 정의 된 5단계 기준의 개인정보보호 정책이 실제 개인정보 서비스에 활용되는 정보를 나열하여 적용이 가능한 예를 표시한 것이다.

보안 정도 높음 ↑ ↓ 낮음

보안 등급	분류
P1 (Privacy_ 1 : Strict) (반드시 공개해야 하는 경우 외 기본적으로 통제하는 정책)	개인정보 관련 기밀 정보
	기업/기관 정보 관련 기밀 정보
P2 (Privacy_ 2: Cautious)	개인정보관련 취급시 주의를 요하는 정보
	기업/기관 관련 취급시 주의를 요하는 정보
P3 (Privacy_3 :Moderate)	개인정보관련 적절한 통제(사용자 등의) 기능아래 공개 가능여부가 가능한 정보
	기관/업체 적용시 적절한 통제 기능 아래 공개 가능여부가 가능한 정보
P4 (Privacy_4 :Flexible)	개인정보관련 어느정도 공개가능한 정보
	기관,업체 관련 어느정도 공개가능한 정보
P5 (Privacy_5 : Casual) (꼭 필요한 정보만 통제 후 기본적으로 공개하는 정책)	대 국민 공개 가능 정보
	기관/업체 공개 가능 정보

그림 3. 개인정보보호 정책 설정 기준표

2단계: 개인정보 정책 설정이 완료된 후, 개인정보 정책에 준한 세부 준수 사항인 절차(procedure), 가이드라인을 구성하고, 사용자, 운영자, 관리자 측면에서 개인정보를 다루는 역할별 주요 업무 수행 분야를 지정하고, 향후 개인정보 활용 시 접근제어 측면에서, 실제 가이드가 될 수 있도록, 정보의 제한(Constraint) 및 허가(Permission) 부분을 명시하는 부분이다.

표 3. 개인정보 정책, 절차, 가이드라인 생성 표

분 류	설 명
개인정보 정책	- 개인정보를 위한 중심축으로서 전반적이고 선언적인 내용으로 본 논문에서의 개인정보 정책은 목적, 적용 및 책임 범위 등을 고려하여 아래와 같이 5단계로 구분하여 정의하였다. -예) P1, P2, P3, P4, P5
개인정보 절차	- 개인정보 정책에서 정의 된 세부 사항을 달성하기 위해 관련 분야를 세부적으로 명시 한다. 예) - P_100: 개인정보보호 관련 부서의 역할과 책임 - P_200: 개인정보보호에 관련된 자들의 역할과 책임 - P_300: 개인정보보호 사고 시 대응 절차 - P_400: 개인정보보호 서비스 제공시 고려 절차 - P_500: 개인정보관련 사용자 인증 관리 규정 - P_600: 접근 권한 관리
개인정보 가이드라인	- 개인정보 시스템을 다루는 운영자, 관리자 측면에서 역할 대비 실행 할 수 있는 가이드를 절차에 준하여 제시 한다 예) - P_100_A_001: 사용자 개인정보 발급/신청/폐기 절차 - P_100_A_002: 개인정보 입력 발생 시 처리 절차 - P_100_A_003: 사용자 정보 공유 및 2중 사용 시 확인 절차
역할 정립 (Role Assignment)	- 조직 내 업무에 대하여, 수행가능한 권한과 책임을 기반으로 조성 된 구성원들에 대한 관련 업무를 정립 한다 예) 사용자, 관리자, 개발자, 운영자 등
역할기반의 접근제어	- 관리자, 운영자 측면에서 사용자 개인정보에 대하여 누가, 언제, 어디에서, 어떤 행동에 대하여 개인정보 이용 관련 사용자 배정, 역할 할당, 권한 배정, 세션(Session)등에 따른 제한 및 접근 가능한 지에 대한 규정을 제시 한다 예) 제약(Constraint)적 기능 - R_100_C_001 : 사용자 주민번호 제공기능 제한 - R_100_C_002 : 사용자 신용정보 제공기능 제한 - R_100_C_003 : 사용자 자산정보 제공기능 제한 - R_100_C_004 : 개인정보보호 오류시 세션 종제 기능 - R_100_C_005 : 개인정보 제공시 역할별 제한 서비스 제공 - R_100_C_006 : 개인정보 중요도에 따른 제공 서비스 제한 기능 예) 허락(Permission) 기능 - R_100_P_001 : 개인정보보호 요청시 사용자 정보 제공 허가 기능 - R_100_P_002 : 개인정보보호 사용자 사전통보 기능 - R_100_P_003 : 개인정보보호 사용자 사후통지 기능

사용자 정보	의미	개인정보 정책 지정 및 상세 내역
이름	사용자 이름	한글(일반정보:P4) 영문/한자(P3)
성별	남/여 구분	P4 / P5
나이	사용자 나이	10-20, 20-30,30-40 (P4 / P5) 정확한 나이(P3)
주소	사용자 주소	지역구 구분-서울,경기(P4 / P5) / 정확한 나이(P3 / P2)
직업	사용자 직업	직업 일반:학생,전문직등 (P4 / P5) 상세정보 직책, 직장주소, 연락처 (P3 / P2)
학벌	사용자 교육 정도	교육 일반 : 석사이상/대졸/고졸 (P4 / P5) 상세:학교명,전공, 학점등 (P3 / P2)
전화번호	사용자 연락처	집전화 / 핸드폰 / 직장전화 / 비상연락처 (P5 / P2)
주민번호	사용자 신분정보	(P1/P2)
자산정보	사용자 자산정보	신용카드/직불,후불카드 번호, 만료기간, 카드 타입 (P1)
의료진료정보	사용자 진료정보	병명/진료기관,처방정보,감염성여부 (P1/P2)
구매정보	사용자구매 정보	구매상품종류, 구매 비용, 횟수, 구매장소, 구매방식등(P2/P3)
재산여부	사용자재산정도	자동차,토지,주식등 (P1/P2/P3)
전과 여부	사용자범죄여부	범죄유형, 구속여부, 구속시 복역기간등 (P1/P2)

그림 4. 개인정보보호 정책 적용 가이드라인 예제

3단계: 개인정보 시스템, 서비스를 대상으로 환경 분석을 통한 적절한 개인정보 정책, 절차, 가이드라인 설정 후 사용자 측면, 운영자 측면, 관리자 측면에서 적절한 개인정보 접근 방안

과 통제 기준이 구성 되면, 실제 다양한 정보의 흐름 분석 (Information-flow)을 기반으로 논리적 기반의 접근제어 체제를 수립한다. 접근제어 체제 확립이란 개인 정보의 입출력 및 수정 사항에 대하여 효과적이고 안전한 접근통제 기능을 수립한다. 아래 그림 5는 능동적인 개인정보의 흐름을 기반으로 운영자, 관리자 측면에서의 적절한 제약(constraint) 및 허락(permission) 기능을 고려하여 설계 된 "역할기반의 접근제어 흐름도(flow)를 설명이 보여주고 있다. 그림 6은 실제 개인정보 시스템 측면에서 개인 사용자가 개인정보를 저장하고 활용하는 방안(개인정보 정책 설정 및 저장, 접근제어, 개안정보 배포 시스템 등)을 시스템 측면에서 보여주는 개인정보 아키텍처를 보여준 것이다.

Ⅵ. 결 론

인터넷과 더불어 IT 관련 빠른 기술의 발달과 더불어, 개인정보에 대한 신뢰적인 사용 방안에 대한 필요성이 점점 증가되고 있다. 이에 본 논문에서는 개인정보의 보호를 위하여 기술적, 관리적, 환경적 측면에서의 유기적인 연결을 통해, 개인정보 보호 방안을 체계적으로 보여 줄 수 있는 개인정보 프레임워크를 개발하였다. 또한 실제 개인정보 시스템을 새로이 설계하고 개발하거나 운영하는 측면에서 효과적인 개인정보 시스템 구축이 가능하도록, 제시된 개인정보 프레임워크 기반의 방법론을 개인정보 환경, 위험분석에서 개발, 사후 관리 차원까지의 적용 가능한 방안을 5단계로 상세히 제시하였다. 또한 제시된 개인정보 방법론 활용 측면에서, 개인정책 수립에서 개인정보 통제, 개인정보 시스템 아키텍처 설계 측면까지를 단계적 적용방안을 제시함으로써, 본 논문의 개인정보 프레임워크의 활용 방안을 소개하였다. 향후 개인정보 프레임워크와 방법론을 전자정부, e-비즈니스와 같은 웹 기반의 분산 환경 내 신뢰할 수 있는 개인정보 시스템 설계 및 구현 메커니즘 측면에서 적합한 개인정보 모델링이나 아키텍처를 개발하여 제시할 예정이다.

참 고 문 헌

[1] P. W. Warren, "From Ubiquitous Computing to Ubiquitous Intelligence", *BT Technology Journal*, Volume 22 Issue 2, Pages:.28-38, April, 2004.

[2] Eila Niemela, and Juhani Latvakoski, "Survey of requirements and solutions for ubiquitous software", *Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia MUM '04*, New York, NY, USA, Pages: 71-78, October, 2004.

[3] Gregory D. Abowd, and Elizabeth D. Mynatt, "Charting past, present, and

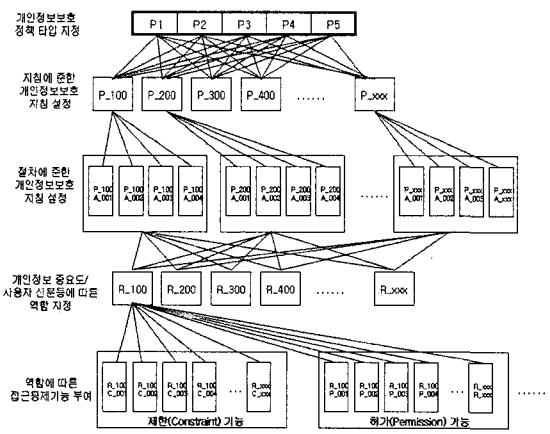

그림 5. 능동적 개인정보 기반의 역할기반 접근통제 흐름도

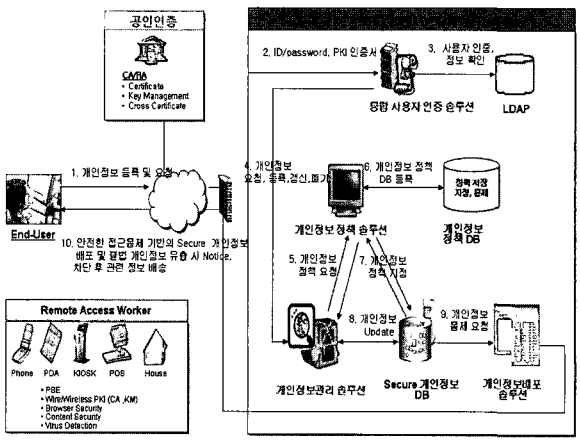

그림 6. 개인정보 시스템 아키텍처

future research in ubiquitous computing", *ACM Transactions on Computer-Human Interaction (TOCHI)*, Volume 7 Issue 1, Pages: 29-58, March, 2000.
[4] Jason I. Hong, and James A. Landay, "Support for location: An architecture for privacy-sensitive ubiquitous computing", *Proceedings of the 2nd international conference on Mobile systems, applications, and services MobiSys'04*, Boston, MA, USA, Pages: 177-189. June, 2004.
[5] Simson Garfinke, and Gene Spafford, "Web Security, Privacy, and Commerce", *O'reilly & Associates, Inc., 2nd Edition*, Pages: 230-256, January, 2002.
[6] Giovanni Iacjello and Gregory D. Abowd, "Privacy and Proportionality: *Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing", CHI ACM*, Pages: 91-100, April 2-7, Portland, Oregon, USA, 2005.
[7] Privacy and data-sharing-The way forward for public services Performance and Innovation Unit in the U.K., Available at*http://www.piu.gov.uk/privacy/index.htm*
[8] Bettina Berendt, Oliver Gunther, and Sarah Spiekermann, "Privacy in e-Commerce: Stated Preference vs. Actual Behavior", *Communications of ACM*, Vol. 48 No. 4, Pages: 101-106, April, 2005.
[9] Jean-Philippe Cotis, "Economic Policy Reforms : Going for Growth 2006", *OECD Publishing2*, 7, 2006.
[10] A list of privacy surveys, Available at http://www.w3.org/P3P/p3pfaq.html.
[11] 조화순, "IT혁명과 개인정보보호", *한국전산원*, 05, 2004.
[12] 개인정보보호백서 2003, *한국정보보호진흥원*, 2003.

〈著者紹介〉

홍 승 필 (Seng-phil Hong) 종신회원
1993년 Indiana State University (학사)
1994년 Ball State University (석사)
1997년 Illinois Institute of Technology (박사수료)
2003년 한국정보통신대학교 (박사)
1997년 ~ 2004년 LG CNS Systems, Inc.
2005년~현재 성신여자대학교 컴퓨터정보학부
〈관심분야〉 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호

이 철 수 (Lee ChulSoo) 정회원
소속: 경원대학교 소프트웨어 대학(software collage of Kyungwon university)
1975-1977 KAIST 전산과 석사
1977-1981 KAIST 전산과 박사
1982-1993 (주) 데이콤
1993-1998 한국전산원
1999-2000 한국 정보보호원
2000-2002 정보통신대학교
2003- 현재 경원대학교
〈관심분야〉 정보보호 정책, 침해사고 대응기술