情 報 保 護 學 會 誌
第 16 卷 第 4 號, 2006. 8

개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크

송 유 진*, 이 동 혁**

요 약

향후의 유비쿼터스 사회(U-Society)는 정보화에 따른 여러가지 새로운 위험들이 나타나는 사회가 될 것이며, 개인정보 생성, 수집 등을 통해 개인정보 지식베이스 형성을 가능하게 하는 정보위험사회의 도래가 예상되고 있다. 따라서, 사용자의 상황에 맞게 적응적(Adaptive)이고 적시적(Just-In-Time)으로 개인정보보호 서비스 제공이 가능한 새로운 프레임워크 개발이 요구된다. 본 논문에서는 U-Society와 프라이버시 개념의 변화 과정을 검토하고, 개인정보 및 프라이버시 침해의 유형을 비교 분석한다. 아울러, 기존 프라이버시 보호 프레임워크 모델인 WASP 아키텍처와 IBM의 TPM 작동 과정과 주요 기능을 살펴보고 이에 따른 문제점을 지적한다. 또한, 개인정보보호 대책을 수립하기 위해 개인정보의 라이프사이클 관점에서 수집, 저장/관리, 이용/제공, 폐기의 4단계로 분석하고 개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크 모델을 제시한다.

Ⅰ. 서 론

정보통신 기술의 발달과 함께 나타난 다양한 응용기술들은 산업 전반에 많은 변화를 가져왔으며, 개인에게는 삶의 질 향상을, 기업에게는 새로운 이익의 창출과 비즈니스의 혁신이 가능하게 되었다. [1]

또 한편으로는 범세계적 정보통신서비스의 기반 확대에 따라 개인정보가 컴퓨터에 의해 처리·활용되어 개인의 명예훼손이나 지적 재산권 문제, 정크 메일의 홍수 등 디지털화된 개인정보의 오·남용 피해가 증가함에 따라 개인정보보호 문제에 대한 능동적이고 효과적인 기술적 및 제도적 조치가 필요하게 되었다. [3]

현재, 유비쿼터스 컴퓨팅 환경 구축에 필요한 인프라, 요소기술의 표준화, 보안 등에 관련된 연구들이 활발하게 이루어지고 있다. [2] 유비쿼터스로의 진행 과정에서 특히 논란이 되는 문제들로는 개인정보보호, 시스템 혼란 방지, 확장성, 보안 등 다음과 같은 이슈들이 있다. [16]

- o 개인정보보호(privacy) : 센서와 상황 모델의 적용에 따라 개인의 사적 활동에 대한 정보가 노출되며, 자동 지원 시스템이 증가할수록 개인정보의 노출도 심각하게 된다. 따라서 필요한 정보만 활용하고 개인정보는 보호할 수 있는 장치가 요구된다.
- o 보안(security) : 모든 네트워크화된 장치나 시스템이 서로 연결되므로, 인증되지 않은 소프트웨어나 하드웨어의 공격을 막고 제한하는 방법이 강구되어야 한다.
- o 적응성(Adaptive)과 적시성(Just-In-Time) : 사용자의 상황(Context)에 따라 능동적으로 작동할 수 있는 어플리케이션이 요구된다. 한편, 정보의 제공은 사용자에게 실시간으로 가공되어 제공되어야 한다.
- o 시스템 혼란 방지(complexity) : 센서와 상황 모델로부터 생성되는 의미 있는 정보와 무의미한 정보가 구별되지 않는 상태에서 자동지원 시스템에 폭주하게 되면 시스템의 정상적 대응은 무리다. 따라서 무의미한 정보로부터의 혼란을 방지할 수 있는 시스템의 구현이 요구된다.
- o 확장성(extensibility) : 유비쿼터스 컴퓨팅 시스템은 여러 장소에 분산된 하드웨어와 소프트웨어로 구성된다. 따라서 상위의 응용 수준에서부터 하위의 통신 수준까지 함께 동작할 수 있는 시스템 관리가 필요하다.

* 동국대학교 전자상거래학과 교수(song@dongguk.ac.kr)
** 동국대학교 대학원 전자상거래학과(jazzbop@korea.com)

이를 위해 유비쿼터스 환경에서의 개인정보를 보호하기 위한 방법으로 WASP 아키텍쳐와 IBM의 TPM이 개발되었다.[22][29] 그러나 WASP 아키텍쳐에서는 사용자 정보 수집 이력 관리에 필요한 모니터링 기능이 없고, 인증 기능을 별도로 고려하지 않아 정보 유출의 위험이 존재한다. 그리고 IBM의 TPM은 유비쿼터스 환경의 주요한 요소가 되는 사용자의 Context 수집에 관한 부분을 고려하지 않는다. 따라서 사용자의 상황에 맞게 적응적(Adaptive)이고 적시적(Just-In-Time)인 서비스를 제공할 수 없다.

이와 같이, 기존 연구에서 나타난 WASP의 단점인 모니터링 기능과 인증기능, TPM에서 나타난 Context 수집의 문제를 보완한 새로운 프레임워크 개발이 요구된다. 본 논문에서는 유비쿼터스 사회에서 개인정보의 수집, 저장/관리, 이용/제공, 폐기라는 라이프사이클에 따른 프라이버시보호 프레임워크를 구축한다.

Ⅱ. u-Society와 프라이버시 보호

1. u-Society 프라이버시 보호 개념의 변화

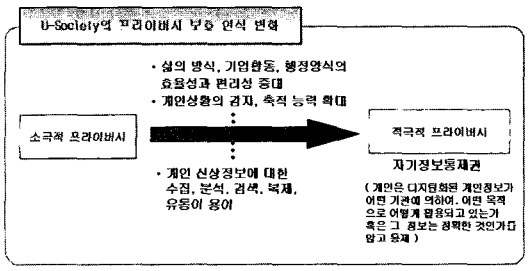
향후의 유비쿼터스 사회(U-Society)는 정보화에 따른 여러가지 새로운 위험들이 나타나는 사회가 될 것이다. 개인정보 생성, 수집 등을 통해 개인정보 지식베이스 형성을 가능하게 하는 정보위험사회의 도래가 예상되고 있다.[23]

나아가 우리의 모든 일상은 개인정보의 소통을 통해 이루어지게 될 것이며 따라서 개인정보의 보호는 이러한 개인정보의 소통을 전제로 이루어져야 한다. 요컨대 영역별(공공, 민간)로 나누어 보호한다거나, 사안별(어플리케이션 등)로 나누어 보호하는 것이 아니라, 개인정보의 보호 자체를 독자적인 항목으로 하는 개인정보 라이프사이클을 기반으로 하는 법제도적, 기술적 대책이 필요하다.

한편, 유비쿼터스 사회에서는 프라이버시 보호에 새로운 인식변화가 요구된다. 프라이버시권은 원래 '혼자 있을 권리' 또는 원하지 아니하는 '공표로부터의 자유(freedom from unwanted publicity)' 라고 인식되었을 정도로 소극적 개념이었으나, 현대 정보화 사회에 와서는 '자기에 관한 정보를 관리, 통제할 수 있는 권리'까지 포괄하는 적극적 개념으로 파악되고 있다.

한 개인이 자기에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시키느냐를 스스로 결정하는 권리로서 프라이버시 개념이 이해되기 시작되었기 때문에 최근 스팸메일 발송, 개인정보를 제3자에게 제공하는 행위, 개인에게 동의를 받지 않고 개인정보를 수집하는 행위 등을 프라이버시 침해라고 문제삼는 것이다.

이러한 측면에서 유비쿼터스 사회에서의 프라이버시 보호의 개념은 유비쿼터스를 지향하는 신정보사회에서의 개인정보통제권을 의미한다고 할 수 있다. [24] 여기서, 개인정보통제권은 단순히 사생활 보호의 측면에서가 아니라 정보활용권을 가지는 정치적, 사회적 권력체, 공공기관, 기업 등에 대한 민주적 통제와 감시권으로서 새로이 인식될 필요가 있다.[그림 1]



[그림 1] U-Soicety 프라이버시 개념의 변화

즉, U-Society에서의 개인정보통제권 (U-Privacy) 관점에서 개인정보 라이프사이클에 따른 U-Privacy에 대한 연구가 필요하다. 본 논문에서는 개인정보통제권을 자신의 정보가 어떻게 수집, 처리, 관리, 이용(개인정보의 라이프사이클) 되는지에 대한 감독권이라는 측면에서 프라이버시 보호 프레임워크를 조명하고자 한다.

2. 개인정보 및 프라이버시 침해 유형

[표 1]은 개인정보의 유형과 종류를 나타내고 있다. [표 2]는 현행과 유비쿼터스 환경의 프라이버시 침해 유형을 비교하고 있다.

Ⅲ. 기존 프레임워크 모델 분석

1. WASP Privacy Architecture [29]

Context Aware 컴퓨팅은 보다 진보된 서비스를

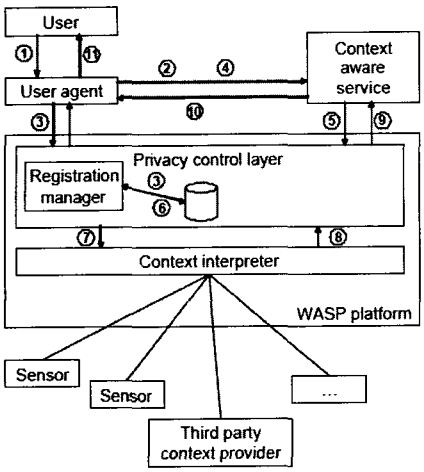
〔표 1〕 개인정보의 유형과 종류 〔9〕

구 분	개인정보 유형
일반 정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족 정보	가족 구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대 유형 주특기, 근무부대
부동산 정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
동산 정보	보유현금, 저축현황, 현금카드, 주식, 채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석
소득 정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타 소득의 원천, 이자소득, 사업소득
기타수익정보	보험(건강, 생명 등), 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격테스트결과, 직무태도
법적 정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화 내용, 로그파일(log file) 쿠키(cookies)
위치정보	GPS 나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

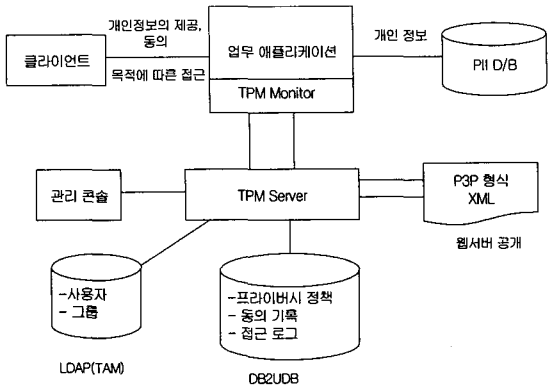
〔표 2〕 현행과 유비쿼터스 환경의 프라이버시 침해 유형 비교 〔9〕

프라이버시 침해유형	현 행	유비쿼터스 환경
부적절한 접근과 수집	정보주체 동의 없는 개인정보의 수집	정보주체의 동의뿐 아니라 정보주체가 인식할 수 없는 상황에서 정보주체가 완전한 자기정보 통제권을 상실할 가능성이 큼
부적절한 분석	부적절하게 수집된 정보의 분석, 동의 없는 사적 정보의 분석	부적절하게 수집된 정보의 분석을 통해 개인 지배 또는 개인에 대한 통제행위가 심화될 가능성 큼
부적절한 모니터링	동의 없는 개인의 인터넷 활동을 모니터링(쿠키)	부적절한 모니터링을 통한 개인의 라이프스타일 등 개인의 생활 전반이 노출될 가능성이 큼
부적절한 이전	개인정보를 제3자에게 양도하는 등 불법적 거래	개인정보를 제3자에게 양도하는 등 다양한 유형의 개인정보가 불법적으로 거래되거나, 분석된 개인정보가 유통될 가능성 큼
원하지 않은 영업행위	동의 없는 상품광고, 광고성 정보전송 행위	개개인의 특성에 정확하게 조응하는 광고성 구체적 상품광고가 동의 없이 무차별적으로 유통될 수 있음
부적절한 저장	정보보안의 미흡으로 이한 외부 유출과 정보수집 목적 달성 후 개인정보가 파기 되지 않는 행위	한번 수집된 정보는 파기되지 않고 수차의 분석을 통해 다양한 용도로 재활용될 가능성 큼

제공하기 위한 새로운 패러다임이며, Context-Awareness는 정보제공을 위한 새로운 근거를 제공한다. 본 장에서는 Context-Awareness 환경에서 WASP를 위한 프라이버시 제어 아키텍처에 대해 검토한다.〔그림 2〕



〔그림 2〕 WASP 프라이버시 아키텍처



〔그림 3〕 TPM 구성

사용자는 사용자 에이전트(User Agent)를 통해 자연스럽게 WASP 플랫폼과 상호 작용이 가능하다. 사용자 에이전트는 사용자의 프라이버시 Preference에 접근한다. 사용자 에이전트는 자동으로 서비스의 프라이버시 정책을 평가한다. 정보의 흐름은 다음과 같다.

① 사용자는 사용자 에이전트에 Context-Aware service를 사용할 것임을 알린다.
② 사용자 에이전트는 Context-Aware 서비스의 프라이버시 정책을 획득한다.
③ 사용자 에이전트는 사용자의 Preference를 검토하여 접근 가능한지를 판단하고 그러한 경우 사용자의 Context-Dependent Preference를 플랫폼에 등록한다.
④ 사용자 에이전트는 Context-Aware 서비스를 불러온다.
⑤ Context-Aware 서비스는 WASP 플랫폼으로부터 Context 정보를 불러온다.
⑥ Privacy Layer는 사용자의 Context 정보가 Context-Dependent Preference에 등록되어 있는지에 대한 여부를 판단한다.
⑦ Privacy Layer는 요청을 Context Interpreter에 전송한다.
⑧ Context Interpreter는 사용자의 정보를 Privacy Layer에 전송한다.
⑨ Privacy Layer는 Context 정보를 Context-Aware 서비스에 전송한다.
⑩ Context-Aware 서비스는 사용자 에이전트에 전송한다.
⑪ 사용자 에이전트는 Context-Aware 서비스의 결과를 사용자에게 보여준다.

2. IBM Tivoli Privacy Manager 〔22〕

IBM의 Tivoli Privacy Manager for e-business는 기존의 누가, 어떤 정보를 취급할까라는 부분만을 관리하는 것이 아니라, 기업의 개인정보에 대한 프라이버시 정책에 근거해서 누가, 무슨 목적으로, 누구의 정보를 취급할까 라는 프라이버시 관리에 필요한 기능을 제공한다.

프라이버시 정책을 IT시스템에 적용하는 것에 의해 복잡한 프라이버시 관리 작업을 자율화시키고 개인정보를 효율적으로 관리해 프라이버시 보호에 적절히 대응하여 비용을 절감할 수 있다.

TPM 시스템 구성은 〔그림 3〕과 같이 크게 두 개의 컴포넌트인 Privacy Manager Server(TPM Server)와 Privacy Manager Monitor(TPM Monitor)로 나눌 수 있다.

Privacy Manager Server는 Privacy Manager Monitor로부터 받은 개인정보에의 접근 제어 정보에 의해 프라이버시 정책에 적합한지를 판단하여 접근 여부를 결정한다.

Privacy Manager Monitor는 개인정보에 접근하는 애플리케이션 프로그램에 내장되어 개인정보 접근이 발생했을 때 Privacy Manager Server에의 접근 여부 판단을 요청해서, 판단 결과를 애플리케이

〔표 3〕 Tivoli 소프트웨어의 주요 기능과 장점

항 목	기 능	장 점
Policy Editor	사용하기 쉬운 고급 P3P 인터페이스를 통해 작성된 개인정보보호 정책에서 기계를 판독할 수 있는 개인정보보호 정책을 작성하는데 적합한 사용하기 쉬운 자연어 인터페이스 제공	개인정보보호 담당자, 변호사, IT 담당자 등이 함께 협력해 정책을 실무 관해에 통합한 개인정보보호 규칙을 작성할 수 있도록 지원, 정책을 작성하기 위해 IT 시스템에 대한 전문 지식을 보유할 필요가 없음
정책배치	조직이 각 애플리케이션에서 개별 시스템에 대한 사용자의 개인정보보호 설정을 모니터일하고 기록할 수 있도록 지원, 정책을 작성한 다음, 감시 대상 시스템이 있는 모든 곳에 배치할 수 있는 모든 곳에 배치할 수 있음.	애플리케이션 전반에 개인 설정을 포함시키기 위해 기존 애플리케이션을 수정하거나, 재작성하는 것보다 비용적인 측면에서 효율적, 추후 손쉽게 정책을 업데이트 할 수 있으며 환경에 미치는 영향을 최소화
Report Generator	배치된 정책 시행 위치, 개인정보보호 정책 등에 따라 개인정보 관리는 상세하게 보여 주는 감사, 추적 정보 등이 포함되어 있는 전사적 보고서를 작성	내부 감사 및 규제 관련 검토는 물론, 데이터 소유자의 요청 등 목적을 위해 개인정보 사용 내역에 즉시 접근 가능
Administration	Tivoli Privacy Manager for e-business의 운영 매개 변수를 관리하고 조정하는 중앙 콘솔	개인 전반에서 정책 스토리지 찾기, 감사 로그 개인 설정, 동의 등을 제어, 콘솔은 역할 기준 접근 제어를 지원하며, 각 사용자는 자신의 업무를 이행하는데 필요한 기능만 볼 수 있음
모니터 SDK (소프트웨어 개발 킷) 및 레퍼런스 모니터	Java 라이브러리를 포함하고 있는 유연한 SDK 및 샘플 코드(RedMon)를 제공해 애플리케이션, 미들웨어 데이터 래퍼치토리 및 개인정보에 민감한 정보를 지속적으로 저장하는 기타 시스템을 위한 Tivoli Privacy Manager for e-business를 개발할 수 있도록 지원	Tivoli Privacy Manager for e-business의 기능을 확장해 각 기업 환경에 맞추어 자체 구현을 정의할 수 있음. 레퍼런스 모니터에는 모니터를 작성하는데 필요한 코드의 거의 90%가 포함되어 있기 때문에 더욱 신속하게 배치 가능
기타 모니터	LDAP 및 Slebel 7 용 모니터가 포함되어, 애플리케이션 모니터링, 규정 시행 및 감사 등을 수행	기존 애플리케이션에 개인정보보호 모니터를 포함시킬 수 있는 유연성 제공

션 프로그램에 응답한다. 이러한 접근 기록에 의해 종래의 DBMS의 기능만으로는 곤란한 읽기를 포함한 데이터베이스에의 문의 결과를 본인 동의의 유무, 접근제어 정책의 검사 결과, 데이터의 이용자 정보와 함께 취득할 수 있다.

Tivoli 소프트웨어의 주요 기능과 장점을 〔표 3〕으로 정리한다.

Ⅳ. 라이프사이클에 따른 프라이버시 보호 프레임워크

1. 개인정보 라이프사이클 관점에서의 프라이버시 보호

IT 기반의 개인정보보호 대책을 수립하기 위해 개인정보의 라이프사이클 관점에서 분석한다.〔27〕 개인정보의 라이프사이클인 「수집」, 「접근/이용」, 「저장/유통」, 「폐기」의 4단계에서 개인정보 침해유형에 대한 대책을 검토한다.

1.1. 개인정보 라이프사이클 관점에서의 프라이버시 침해 문제

현행 정보통신환경에서 개인정보 침해 유형은 정보생명주기에 따라 정보의 수집, 정보의 저장/관리, 정보의 이용/제공, 정보의 폐기로 구분할 수 있다. 본 절에서는 개인정보 라이프사이클 관점에서 발생 가능한 프라이버시 침해 유형에 대하여 알아본다.

1) 수집

- 서비스 제공자가 개인정보의 수집 및 이용목적을 제시하지 않을 경우에 프라이버시 문제가 발생할 수 있다.
- 서비스제공자가 동의 없이 개인정보를 수집하게

될 경우 프라이버시 문제가 발생할 수 있다.
- 쿠기에 대한 설명 없이 이용자들의 쿠키를 수집하게 될 경우 프라이버시 문제가 발생할 수 있다.

2) 저장/관리
- 개인정보의 제휴 및 공유대상을 밝히지 않고 약관을 통해 포괄적 동의를 구하지 않게 되면 프라이버시 문제가 발생할 수 있다.
- 기업을 인수/합병하면서 아무런 고지 없이 개인정보를 넘기게 되면 프라이버시 문제가 발생할 수 있다.
- 동일기업에서 운영하는 사이트들 간에 개인경로를 공유하게 되면 프라이버시 문제가 발생할 수 있다.

3) 이용/제공
- 타인의 개인정보를 무단으로 도용하여 사용하게 될 경우 프라이버시 문제가 발생할 수 있다.
- 동의 없는 개인정보의 무단 제공 및 공유하게 되면 프라이버시 문제가 발생할 수 있다.

4) 폐기
- 개인정보에 관한 동의철회, 즉 탈퇴요구를 무시할 경우에 프라이버시 문제가 발생할 수 있다.
- 탈퇴 후에도 개인정보를 삭제하지 않게 되면 프라이버시 문제가 발생할 수 있다.
- 탈퇴메뉴가 존재하지 않거나 탈퇴의 방법과 절차에 대한 안내가 없게 될 경우 프라이버시 문제가 발생할 수 있다.

1.2. 프라이버시 보호 대책에 따른 요구사항 도출

본 절에서는 위의 1.1에서 언급한 개인정보 라이프사이클에 대한 문제점으로부터 도출한 프라이버시 보호 요구사항과 그 대책에 대하여 알아본다.

1) 수집

요구사항 1 : 이용 목적, 범위의 명시
- ㅇ 수집하는 개인정보의 종류, 이용 목적, 공유 범위, 취급 기준 등을 명시
  - 웹 사이트에서 수집할 경우, 프라이버시 정책을 페이지 상에 기재

요구사항 2 : 정당한 수집
- ㅇ 업무 수행에 필요 최소한의 개인정보 수집
- ㅇ 앙케이트와 같은 임의 정보 제공 시, 정보를 제공하는 본인이 얻을 수 있는 이익, 편리성을 명시
  - 제공된 개인정보에 대해서는「귀하의 개인정보 사용에 동의합니까?」등 확인과정을 통해 개인정보를 제공한 본인의 의지 표시가 가능하도록 함

2) 저장/관리

요구사항 3 : 프라이버시를 고려한 개인정보 이용
- ㅇ 개인을 특정할 수 있는 형태는 개인정보 수집 시 합의한 업무범위에만 사용
- ㅇ 데이터 마이닝 등 본인이 명시한 이외의 목적으로 사용하는 경우, 개인을 특정하지 않는 범위에서 추상화(랜덤화)

요구사항 4 : 상세한 접근제어/관리 수행
- ㅇ 정보 이용자와 본인과의 관련에 의한 접근
- ㅇ 본인 동의의 유무에 따른 개인정보 처리
- ㅇ 개인정보에 관한 접근, 로그의 취득 등 설명 책임을 유지하기 위해 필요한 조치
- ㅇ 프라이버시 정책 적합성 체크

요구사항 5 : 보유 데이터의 공개, 정정의 구조
- ㅇ 보유하고 있는 개인정보의 공개/정정 요구에 대응하는 기능 및 구조의 작성
  - 본인이 사용하기 위한 애플리케이션을 구축해 대응, 혹은 요구가 있던 시점에서 기업 측이 개별적으로 대응
- ㅇ 필요한 사람에게 필요한 개인정보만을 공개
- ㅇ 프라이버시 정책에 근거한 단일관리

요구사항 6 : 부주의한 공개 방지 대책
- ㅇ 작업 파일의 잔존, 정규 이용자의 악의적인 접근 대책을 강구
- ㅇ 개인정보를 취급하는 업무에는 사용자 인증 기능을 마련
- ㅇ 사용자 인증 시에 이용하는 사용자 ID의 타인 사용 금지

3) 이용/제공

요구사항 7 : 보유 상황, 이용 방법의 파악과 적절한 운용
- ㅇ 어떠한 개인정보를 어느 부문에서 보유하고 어떻게 사용하고 있는지를 다음 관점으로부터 파

〔표 4〕 개인정보 취급단계 및 침해유형

취급단계	수 집	저장/관리	이용/제공	폐 기
침해유형	서비스 제공자가 개인정보의 수집 및 이용 목적을 제시하지 않은 경우	개인정보의 제휴 및 공유대상을 밝히지 않고 약관을 통해 포괄적 동의를 구하는 경우	타인의 개인정보를 무단으로 도용하여 사용하는 경우	개인정보에 관한 동의철회, 즉 탈퇴요구를 무시한 경우
	서비스 제공자가 동의 없이 개인정보를 수집한 경우	기업을 인수/합병하면서 아무런 고지 없이 개인정보를 넘긴 경우	동의 없는 개인정보의 무단 제공 및 공유	탈퇴 후에도 개인정보를 삭제하지 않는 경우
	쿠키에 대한 설명 없이 이용자들의 쿠키를 수집하는 경우	동일기업에서 운영하는 사이트들 간에 개인정로를 공유한 경우		탈퇴메뉴가 존재하지 않거나 탈퇴의 방법과 절차에 대한 안내가 없는 경우
요구사항 및 해결방안	Context에 기반한 개인정보 수집 및 암호화 된 D/B구축	인증을 통해 개인정보의 접근권한을 가진 사용자에게만 정보 공개 및 관리	암호화 된 PII D/B를 통해 정보의 이용 시 제공자의 동의를 얻음	D/B는 정보 제공자의 요구에 의해 언제라도 파기 가능

악, 운용. 필요에 따라 부정 접근 방지를 위해서 데이터를 암호화.
- 입수 목적, 입수 경로, 입수방법, 유지 방법
- 취급 경로(정보의 소유자, 이용자 등)
- 보관 장소(일시 보관 포함), 보관 형태, 보관 기간
- 유통경로(복제 이용, 위탁, 제공 등)

요구사항 8 : 보안 이벤트 관리
- ㅇ 로그 데이터로부터 부정 이벤트를 조기 발견
- ㅇ ID를 특정할 수 있는 로그 기록

요구사항 9 : 정확성·안전성의 확보
- ㅇ 부정한 접근을 방지
  - 조작의 제한(복제 금지 등), 암호화, 인증 강화
- ㅇ 보유 데이터의 신규성, 정확성을 유지
  - 기업이 보유한 데이터 상태가 사실과 다르다는 본인으로부터의 지적이 있는 경우, 대응, 수정할 수 있는 구조를 준비
  - 전사적으로 공통 취급하는 데이터베이스를 애플리케이션 마다 복제하여 사용하는 경우, 복제하는 곳에서의 사용 방법(재복제의 유무를 포함)을 파악하고 유지하는 구조 확보

4) 폐기

요구사항 10 : 폐기 방법의 확정과 적절한 운용
- ㅇ 개인정보 마다 보관 기간 후의 폐기 방법을 결정해 운용.
- ㅇ 미디어나 기기를 폐기할 때에 개인정보를 남기지 않음.

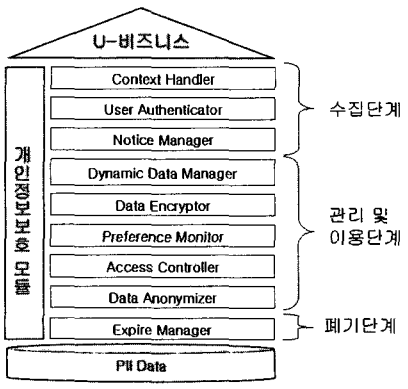
개인정보 라이프사이클에 따른 프라이버시 침해유형과 이에 대한 보호 대책을 정리하면 〔표 4〕와 같다.

2. 프라이버시 보호 프레임워크 구성

개인정보 라이프사이클을 기반으로 개인정보보호에 필요한 요구사항과 그 대책을 바탕으로 프라이버시 보호 프레임워크를 구성한다.

2.1 요구사항에 근거한 프라이버시 보호 모듈 구성

요구사항에 근거하여 프라이버시 보호 모듈을 구성하면 〔그림 4〕와 같다.



〔그림 4〕 요구사항에 근거한 프라이버시 보호 모듈

[그림 4]는 요구사항에 따라 구성한 프라이버시 보호 모듈을 나타내고 있다. Context Handler 및 User Authenticator, Notice Manager는 수집 단계에서 작동한다. Dynamic Data Manager 및 Data Encryptor는 저장 단계에서 작동하며, Preference Monitor 및 Access Controller 및 Data Anonymizer는 정보 이용 단계에서 작동하고, Expire Manager는 정보 폐기 단계에서 작동한다. 각 모듈의 기능을 설명하면 다음과 같다.

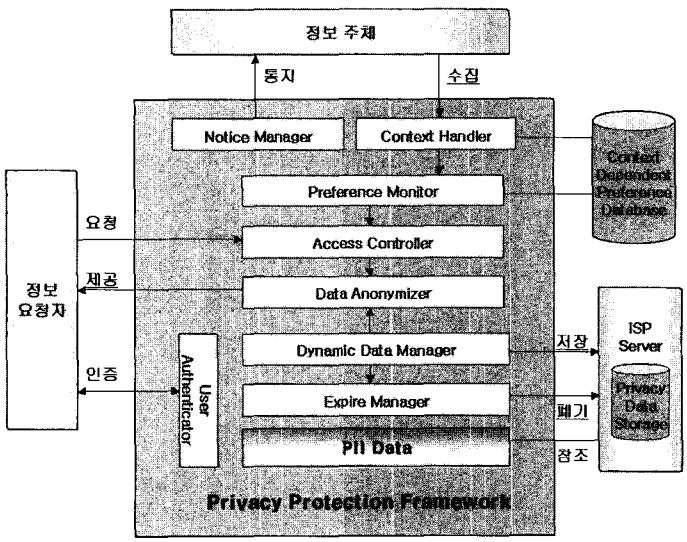
- Context Handler - 사용자의의 Context를 수집 및 가공 처리하고 Dynamic Data Manager에 전달한다.
- User Authenticator - 사용자를 인증하는 기능을 가진다.
- Notice Manager - 정보 수집 및 접근 발생 시, 정보 주체에게 접근이 허가되었음을 실시간으로 알린다.
- Dynamic Data Manager - 시공간에 따라 변하는 정보 주체의 데이터를 관리하고 저장한다.
- Data Encryptor - 사용자의 데이터에 대한 암호화 작업을 수행한다.
- Preference Monitor - 사용자의 Preference를 가져오고 실시간 모니터링한다.
- Access Controller - Context와 Preference에 따라 정보 공개에 대한 접근 권한을 설정한다.
- Data Anonymizer - Access Controller가 결정한 익명화 정도를 바탕으로 개인정보를 일정 수준의 익명화된 데이터로 가공 처리한다.
- Expire Manager - 정보에 대한 이용 기간이 지나면 삭제하는 기능을 담당한다.

2.2 프라이버시 보호 프레임워크 모델 구성

[그림 5]는 프라이버시 보호를 위한 프레임워크 모델을 나타내고 있다. Preference Monitor는 Context Handler를 통하여 사용자의 Context를 수집하고, 이에 따라 Preference를 동적으로 변화시킨다. 즉, 정보 주체의 상황에 따른 제약 조건 변경이 가능하다. 정보 요청자가 정보에 대한 요청을 할 경우, Access Controller는 Preference를 참조하여 정보 공개의 가부를 결정하고, 정보 공개로 판정될 경우 정보 주체의 개인정보가 공개된다. Dynamic Data Manager로부터 불러들여진 데이터는 Data Anonymizer에 의하여 익명화되고 사용자에게 제공되며, 허가된 기간 이상 보관된 개인정보는 Expire Manager에 의하여 폐기된다.

V. 결 론

본 논문에서는 유비쿼터스 환경에서 개인정보의 라이프사이클에 따른 사용자의 프라이버시를 보호할 수 있는 아키텍처를 제안하였다. 제안한 아키텍처의



[그림 5] 프라이버시 보호 프레임워크 모델

특징으로 기존 WASP 프레임워크에서 고려하지 않았던 인증 모듈을 추가하였으며, 시간에 따라서 개인정보를 적절히 폐기할 수 있다. 한편, 사용자의 Preference를 고려하여 시스템의 정책과는 별도로 정보 접근에 대한 정책을 변경 가능하다. 또한, 데이터 관리 모듈에서는 개인정보에 대한 기밀성을 유지할 수 있으며, TPM의 장점인 사용자 개인정보 실시간 모니터링의 기능을 그대로 가지고 있다. 제안한 아키텍처를 통하여 Context-Aware 환경에서 개인정보를 더욱 안전하게 보호할 것으로 기대된다.

참 고 문 헌

[1] Ayres Robert U. and Williams Eric., "The Digital Economy : Where do we stand?", Technological Forecasting Social Change, 2004..

[2] Andrew Fano and Anatole Gershman, "The Future of Business Services in the Age of Ubiquitous Computing", Communications of the acm, vol. 45, no. 12, 2002.

[3] 김연수, 2001. 『개인정보보호 : 고도 지식정보사회의 개인정보보호와 Cyber Law』. 서울 : 사이버출판사, p5, pp.10~11, pp.33~41 참조.

[4] 강홍렬, 윤준수, 황경식. 1997. 고도정보사회의 정보윤리 확립을 위한 정책방안, 「연구보고」, 97-1 정보통신정책연구원. 〈http://www.kisdi.re.kr/publishing/view.html〉

[5] 오재인, "서비스 @ 유비쿼터스 스페이스", 전자신문사, 2004

[6] 전석호, 김원제, 『유비쿼터스 사회와 방송』 커뮤니케이션북스 2005. 3

[7] Jay, Rosemary and Angus Hamilton. 1999 data Protection : Law and Practice. London : Sweet & Maxwell., pp.28~29 참조.

[8] 한국정보보호진흥원, "개인정보 유형 분류", http://www.cyberprivacy.or.kr/kisa

[9] 윤용근, 전병주, "유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형 분석", 한국전산원 2004. 6

[10] 이인호, "정보통신 기술의 발전과 프라이버시", 2001.

[11] 『개인정보보호 백서』 2003

[12] 송유진, 남택용 外 2인, "개인 정보보호 기술동향" 주간기술동향 2005. 10

[13] 송유진, 이동혁, "Context-Aware환경에서의 개인정보보호 연구동향", 정보보호학회지, 2005. 10

[14] 박승창, "유비쿼터스 IT의 2030년 사용자 시나리오(I, II, III, IV, V, VI, VII)," 전자부품연구원 전자정보센터, 2003

[15] Martijn Zuidweg, "A P3P-based privacy architecrure for a context-aware services platform", University of Twente, 2003. 8

[16] Steven A. N. & Shafer, S. A.(2001), "ubiquitous computing and the EasyLiving Project" [online available]

[17] 최남희 『유비쿼터스 컴퓨팅 기술의 응용과 과제 : u-비즈니스를 중심으로』 (2003.4)

[18] 인터넷 침해사고피해 대응지원센터 (http://www.krcert.or.kr)

[19] 한국 전산원 (http://www.nca.or.kr)

[20] 한국 정보보호 진흥원 (http://www.kisa.or.kr)

[21] 정보통신윤리 위원회(http://www.icec.or.kr)

[22] IBM TPM, Tivoli Privacy Manager, http://www-6.ibm.com/jp/software/tivoli/

[23] 홍성태, 21세기 한국 메가트렌드 시리즈 III-정보위험사회의 도래와 대응에 관한 연구, 정보통신정책연구원, 2005.10

[24] 강홍렬, 유비쿼터스 사회의 역기능에 관한 법제도적 기초연구, 정보통신정책연구원, 2004.12

[25] 강달천, "정보통신환경의 변화와 개인정보보호," 개인정보보호 정책 Forum, 2005. 5. 19.

[26] 개인정보보호를 위한 IT 솔루션, IBM Japan http://www-6.ibm.com/

[27] Misa Aoki, IT 시스템에 의한 프라이버시 대책, PROVISION No.42 Summer 2004

[28] Yoshiaki Watanabe, 정보개시 관리솔루션, PROVISION No.42 Summer 2004

[29] Martijn Zuidweg, A P3P-Based Privacy Architecture For A Context-Aware Services Platform, University of Twente, August 2003

〈著 者 紹 介〉

송 유 진 (You Jin Song)

1982년 2월 : 한국항공대학교 전자공학과 졸업
1987년 8월 : 경북대학교 대학원 정보시스템전공 석사
1995년 3월 : 일본 Tokyo Institute of Technology 정보보호전공 박사
1988년 3월~1996년 2월 한국전자통신연구원 선임연구원
2003년 12월~2005년 2월 : 미국 Universty of North Carolina at Charlotte 연구교수
2006년 7월~8월 : 일본 정보보호대학원대학 객원교수
1996년 3월~현재 : 동국대학교 전자상거래학과/대학원 교수
2005년 현재 동국대학교 부설 전자상거래연구소 소장
1998년~현재 한국정보보호학회 이사
1997년~현재 한국정보시스템학회 이사
2001년 ICISC2001 운영위원장
2003년 하계CISC2003 프로그램 위원장
2006년 CISC-S2006 공동프로그램 위원장
관심분야 : 전자상거래응용 보안 (Ubiquitous/Web Service Privacy, Location Privacy, 디지털컨텐츠 보호, XML보안, SCM/CRM 보안 등), Context Aware Application Security/Privacy Protection

이 동 혁 (Dong Hyeok Lee)

학생회원

2004년 8월 : 동국대학교 전자상거래학과 졸업
2005년 3월~현재 : 동국대학교 대학원 전자상거래학과 석사과정
관심분야 : 유비쿼터스/웹서비스 프라이버시 보호, 전자상거래 보안