情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

유비쿼터스 환경에서 프라이버시보호의 기술적 요구사항과 프레임워크

송 유 진*, 이 동 혁**, 남 택 용***, 장 종 수****

요 약

개인정보의 수집에 대해 프라이버시를 최대한 보장하면서, 다양한 서비스마다 각기 다른(Service-specific) 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용 범위를 제공하는 지능형 개인정보보호 에이전트 및 접근제어 기술 개발이 요구된다. 본 논문에서는 IT 환경변화에 따른 기술발전 과정에서 필요하게 될 개인정보보호 요구사항을 검토한다. 또한, 개인정보보호에 대한 요구사항에 대응할 수 있는 프라이버시 보호 프레임워크를 검토한다.

Ⅰ. 서 론

정보기술의 발전으로 사용자는 편리하게 정보서비스를 제공받을 수 있게 되었다. 최근 대두되는 유비쿼터스 컴퓨팅 환경은 기존의 컴퓨팅 환경에서 발전한 새로운 패러다임으로 변화되고 있다. 유비쿼터스 환경은 모바일 기술과 더불어 5-Any 즉 언제나(Anytime), 어디서나(Anywhere), 어느 장소(Anyplace), 어느 장치(Anydevice), 어느 네트워크(Anynetwork)에서 사용자에게 맞는 편리한 서비스를 제공받을 수 있는 네트워크 환경이다.

유비쿼터스 환경에서의 주요 키워드는 상황 인식(Context-Aware)으로 사용자의 직무, 역할 및 위치에 대하여 사용자가 직접 입력하지 않고 상황에 맞게 자동적으로 처리해 주는 것을 뜻한다. 이러한 기술을 통하여 사용자는 인비저블(invisible) 형태의 편리한 서비스를 제공받을 수 있을 것이다.

한편, 유비쿼터스 환경에서는 모든 사람들이 자신의 의지와는 상관없이 항상 네트워크 공간에 놓이게 된다. 유선과 무선을 통합한 유비쿼터스 컴퓨팅 시대에서는 사용자의 모든 모습들을 계속 감시하고 분석하며 실시간으로 개인정보를 계속 전송할 수 있다. 이러한 유선과 무선사용 환경에서 개인 정보활동이 증가함에 따라 개인정보 노출이 심해지고 불법 취득도 많아질 것이 예상된다. 이와 같이, 개인정보의 부적절한 노출로 인한 개인정보 침해 문제는 유비쿼터스 컴퓨팅의 순기능적 효과를 반감시키는 요인이 될 수 있으며 지금까지의 네트워크에서 생각하는 개인정보보호의 상식을 크게 바꿀 수 있다.

유비쿼터스 컴퓨팅 기술을 응용한 u-시티, u-워크 등의 분야가 확산될수록 사생활과 개인정보의 안전에 대한 위협도 커질 수밖에 없다. 아울러 내부 사용자에 의한 개인정보 유출 행위도 더욱 더 활발해질 것이다.

다양한 IT기술의 발달에 따라 개인정보침해기술도 발전되어 갈 것이다. IT기술의 부작용과 역기능 현상으로 타인의 개인정보를 획득할 방법이 더욱 많아지게 되었고 심각한 사회문제로 대두되고 있는 개인정보 유출 문제의 시발점은 서비스 제공자의 무분별하고 과도한 개인정보 수집에 기인한다.

새로운 IT기술이 출현하고 사용자들이 이에 대한 새로운 서비스를 제공받기 위해서는 반드시 사용자들의 일정 정보는 기업과 해당 마케팅 업자에게 알려지게 된다. 즉, 핸드폰 사용, 온라인 신문 보기 등과 같은 기술에서 각각의 접근 지점에 대한 사용자들의 개인정보가 축적된다.

온라인을 통한 서비스 제공자들의 양적 증가와 개인정보에 대한 기업들의 관심 증가로 기업들과 서비

* 동국대학교 전자상거래학과 교수
** 동국대학교 대학원 전자상거래학과
*** ETRI 개인정보보호연구팀 팀장
**** ETRI 네트워크보안그룹 그룹장

스 주체들은 상업적 목적이나 분류의 편의성에 따라 경쟁적으로 필요 범위 이상의 개인정보를 이용자에게 요구하게 되었고, 이에 따라 예전에는 특정 공공기관과 특수한 기업만이 독점하던 개인정보를 이제는 기업들도 직접 수집, 보관, 유통하게 되었다. 셀 수 없이 많은 서비스 기관과 기업, 단체들이 인터넷을 통해 직접 개인정보를 취급함에 따라 개인정보는 본인의 자기결정권 범위를 벗어나 유출되거나 오용될 심각한 위기에 처해 있다.[16]

이와 같이, 네트워크 및 컴퓨팅 패러다임의 환경 변화를 통해 IT기술의 발전으로 개인정보 침해기술에 대한 대응기술이 필요하게 되었다. 특히, 정보기술의 발달은 강력한 검색엔진이나 메일주소 수집기와 같은 자동화된 에이전트에 의한 개인 정보의 수집과 확산이 정보 주체가 모르는 사이에 증가되고 있다.

즉, 검색엔진이나 P2P 서비스와 같은 정보기술의 활용이 늘어나면서 이전에는 감추어져 있던 개인정보가 인터넷 포탈 사이트와 전문 검색 사이트를 통해 쉽게 노출될 수 있기 때문에 지능적인 기계나 에이전트 등에 의한 자동화된 개인정보의 수집을 막거나 개인 식별정보의 노출을 근본적으로 막는 기술 개발이 요구된다.

II. 개인정보보호 요구사항

유비쿼터스 환경의 프라이버시를 고려한 정보보호 시스템[5]에서 필요로 하는 개인정보보호 요구사항을 분석한다.

개인정보의 수집에 대해 프라이버시를 최대한 보장하면서, 다양한 서비스마다 각기 다른(Service-specific) 개인 프라이버시 정보의 접근에 대해 적응적이고 동적으로 정보 이용 범위를 제공하는 지능형 개인정보보호 에이전트 및 접근제어 기술 개발이 요구된다. [그림 1]

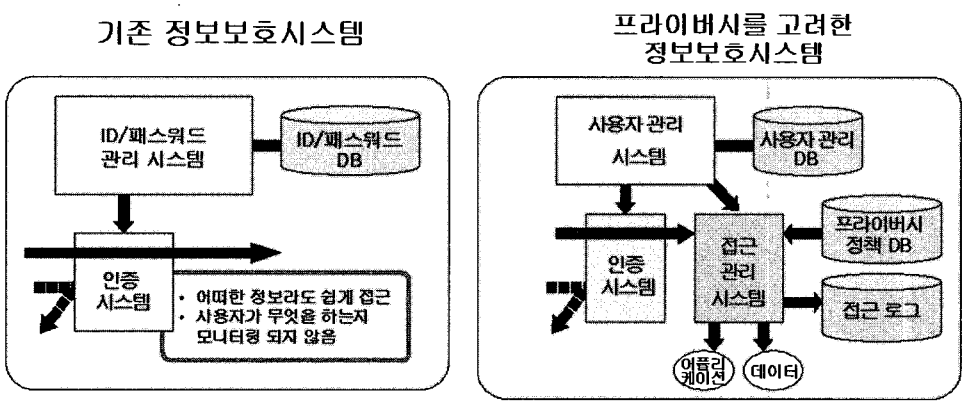
이를 위해 다음과 같은 사항이 고려되어야 한다.

- 개인정보의 접근/사용시 상황정보를 토대로 User Preference의 동적인 적용에 따라 프라이버시 정책(Privacy Policy) 제공을 통한 개인정보 특성에 따른 정보공개의 판정 메커니즘 제공
- 클라이언트-서버 통합 지능형 에이전트 기반 프라이버시 보호 기술 개발
- 프라이버시·정책에 의한 접근 판단 및 동적 상황에 근거한(Context Aware) 접근제어를 통한 개인정보에 대한 수집 에이전트로부터 불법 접근 제한, 동적 개인정보 이용
- 개인 신상정보와 분리된 상황인식 데이터 관리를 통한 적응적 개인정보 이용

프라이버시를 고려한 정보보호시스템을 개발하기 위해 요구되는 사항을 살펴본다.

2.1 요구사항(1) : 프라이버시 보호기능의 인프라화

프라이버시 보호기능을 비즈니스 프로세스로부터 분리하여 프라이버시 보호계층(PPI, Privacy Protection



• 시스템 불법 접근이 허용되면 어떠한 대책을 취해야 할지를 모름
• 로그인 기록만으로 자원에 대한 접근 기록이 곤란

•프라이버시 정책에 근거한 접근관리
•사용자의 종류, 등급 등에 의한 어플리케이션 그룹이나 개인정보에의 접근 관리와 기록
•시간이나 상황에 따른 동적인 관리

[그림 1] 프라이버시를 고려한 정보보호시스템

Infrastructure)으로서 기능을 분리하는 것이 요구된다.

예를 들어, 종래의 접근 보호를 위해서 여러 가지의 조건을 붙여 복수의 SQL문을 생성하는 업무도 업무의 필요성에 따라 단일의 SQL문을 만드는 것만으로 끝나게 된다. 이 SQL문에 대해서 그 업무가 실행된 상황, 조작자, 입수 정보와의 관련에 의한 필터링을 프라이버시 보호계층이 수행해서 적절한 정보만을 업무처리에 전달하도록 하는 것이다.

프라이버시 보호계층을 업무처리 기능으로부터 분리함으로써 업무처리 기능은 본래의 업무 처리에만 전념할 수 있으므로 결과적으로 프로그램 작성의 생산성도 향상될 수 있다.[11]

이와 같이 인프라 기능 내에 개인정보보호를 위한 개인 식별정보의 통합관리, 접근제어, 이용자의 식별과 인증 등 새로운 IT기능을 개발하고 인프라화할 필요가 있다.

2.2 요구사항(2) : 개인정보 특성에 따른 처리 (개인화에 따른 상황인식 데이터[1] 관리)

최근 기업의 어플리케이션 서비스는 On Demand 형태로 일반화되고 있다. 기업이 보유한 중요한 개인정보의 유효한 활용이 요청되고 있는 것이다. 즉, 보유한 개인정보를 유효하게 활용하면서 동시에 개인정보의 부정사용을 방지하고 정보 노출을 막아야 하는 모순된 2가지 요건을 만족시켜야 한다.[29]

이를 위해 개인에 대한 적정 수준의 프라이버시를 유지할 수 있도록 개인정보 특성에 따라 처리함으로써 서비스 중에 개인이 프라이버시의 수준을 선택할 수 있도록 개인화되어야 한다.

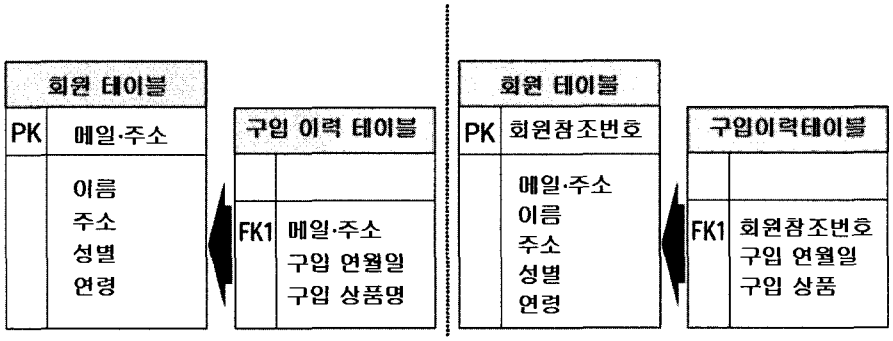
예를 들면, [그림 2]의 왼쪽에 나타낸 것처럼, 회원 정보와 그 구입 이력을 보관 유지하기 위해서 개인 신상 정보 (PII, Personally Identifiable Information : 개인을 특정할 수 있는 정보) 라고 나타내지는 메일·주소를 키(FK1-PK)에 관련지을 경우, 구입 이력 테이블도 개인정보로서 신중한 취급이 필요할 것이다. 한편, [그림 2]의 오른쪽 2개의 테이블을 관련짓는 키를 개인과는 직접 관계없는 것(회원 참조 번호)으로 했을 경우, 회원 참조 번호 자체는 PII는 아니기 때문에 구입 이력 테이블은 개인정보로서 취급되지 않게 된다.

개인 프라이버시 보호의 관점에서 개인정보를 포함한 데이터는 가능한 한 다른 데이터와 분리하여 PII만을 포함한 데이타베이스나 테이블을 구축하는 것이 필요하다. PII[2]가 필요한 경우만 데이터베이스나 테이블에 접근함으로써 이용범위 및 이용자의 제한, 어플리케이션으로부터의 개인정보 이용 제어가 용이하게 된다.

2.3 요구사항(3) : 프라이버시를 보호하는 접근제어 (동적인 접근제어)

개인정보는 소유자의 동의 유무에 의해 개인정보의 사용 범위가 변화되는 특징이 있고 또 다른 특징은 「누가, 무슨 목적으로, 누구의 정보를 취급할까」에 의해 접근 가부가 결정된다는 것이다. 즉, 개인정보의 접근 판단은 누가, 누구의 정보를, 무슨 목적으로 접근하고 있는가 하는 동적인 상황에 의해 변화한다.

예를 들면[27], 어느 쇼핑 사이트의 고객인 A는 자신의 개인정보를 쇼핑에 필요한 배송 등의 업무 이외에는 이용되지 않기를 바라고 있다. 한편, B씨는 자



[그림 2] 데이타베이스 설계의 예[27]

1) 개인을 묘사하는 모든 것으로서 데이터 기록, 개인의 특성, 구매 내역, 의료 기록, 현 거주지, 쇼핑 습관 등
2) 개인의 신분을 확인하기 위해 이용할 수 있는 정보

신 앞으로의 개인화된 세일 정보 등을 E메일로 시기 적절하게 받기를 희망하고 있다. 이 쇼핑 사이트상의 데이타베이스를 이용해서 마케팅 매니저가 구입 동향을 분석하기 위해 구입 이력, 연령, 성별 등을 이용하는 경우, 어떻게 처리하면 좋을까? 또한, 개인화된 마케팅 활동을 하는 경우는 어떨까? 이때, 데이타베이스상의 데이터 항목마다 개인정보 사용자(배송이나 마케팅 부문의 담당자) 각각에 대해 이용목적에 따른 접근제어가 요구된다.

이와 같이 개인정보를 사용할 경우, 식별정보, 처리시간, 환경, 목적 등의 동적인(Dynamic) 요소, 즉 개인정보 접근을 위한 문맥(Context) 요소도 고려할 필요가 있다.

개인정보의 사용범위는 기업 등이 사용자에게 제시한 프라이버시 정책에 의해 명시된 범위로서 허가된 업무인가에 따라 결정된다. 즉, 프라이버시 정책[3]에 적합한 개인정보 요구자만이 개인정보 사용이 허가된다.〔그림 3〕

2.4 요구사항(4) : 개인정보의 안전한 분산 관리 및 추출

인터넷상의 온라인 상거래가 늘어나면서 민간 사업자에 의한 개인정보의 수집이 늘어나고 있으나, 개인정보 보호 의식이 저조하여 저장된 개인의 정보가 악의적인 해킹에 노출되는 경우가 많고, 공공기관의 경우도 개인 정보보호를 위한 보안 관리가 허술하고 과도한 개인정보 열람 등으로 프라이버시를 침해하고 있다.

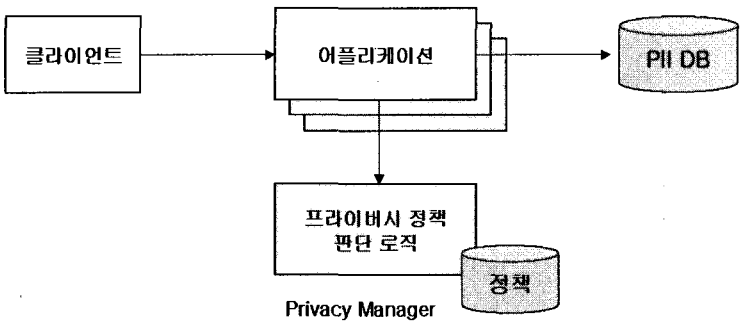
이에 대한 대책으로서 개인정보의 안전한 분산 저장관리 및 추출 기능이 요구되고 있다.

2.4.1. 개인정보의 안전한 분산 저장 관리

개인정보의 안전한 저장 관리를 위한 기술적 대책으로서 비밀정보 분산(Secret Sharing) 기술에 의해 기밀성을 유지함으로써 개인 정보의 안전한 저장이 가능하고, 시간이 흐르면 해독될 우려가 있는 암호화·전자서명의 약점을 극복하고 안전하게 장기간의 저장을 낮은 비용으로 처리하기 위한 분산, 저장 기능이 요구된다.

최근의 개인정보 노출의 가장 큰 원인은 정당한 개인정보 관리자에 의한 부정 이용 이다. 관리자는 사용자의 기밀 문서를 몰래 복사하거나 고쳐 쓰는 것도 가능하다. 사용자 키가 로그인 패스워드라면 그 사용자를 위장하는 것도 가능하게 된다. 이와 같이 접근 권한을 한곳에 집중시키면 관리는 쉽지만 이에 따르는 리스크가 커지게 된다. 이것을 해결하는 수단으로서 리스크 분산을 들 수 있다.[33]

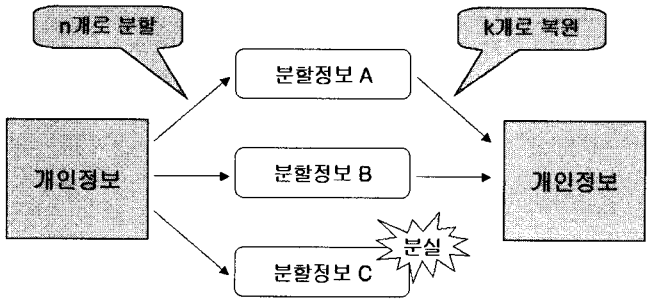
리스크 분산을 개인정보 관리에 적용했을 경우, 예를 들면, 중요한 개인정보를 3개의 분할 정보로 나누어 3사람의 관리자에게 각각 맡기는 시스템을 가정한다. 개인정보를 복원하고 싶을 때, 관리자 3인이 자신의 가지고 있는 분할 정보를 모으면 키를 복원할 수 있다. 이러한 처리는 실제 비밀분산 방식이라고 하는 k-out-of-n 분산 방식으로서 「분할시키는 수 : n」, 「복원에 필요한 수(임계치): k」인 방식이다.



통상의 접근제어 => 사용자(그룹)은 자원에 대해 조작을 행한다.
프라이버시를 고려한 접근제어 구현 => 사용자는 소유자의 데이터에 대해 소유자가 동의한 경우에만 조작을 행한다.

〔그림 3〕 프라이버시를 고려한 접근제어 개념

3) 개인정보보호 방침을 의미하는 것으로서, 개인정보 취득이나 보호에 관해 기업이 준수해야 할 체제나 프로세스



〔그림 4〕 비밀분산방식 2-out-of-3

예를 들면, 2-out-of-3의 경우(파라미터는 $k \leq n$ 을 만족하도록 설정), 중요한 개인정보를 3개로 나누어 그 중 임의의 2개가 모이면 복원할 수 있게 된다. 〔그림 4〕

비밀분산 방식은 향후 유비쿼터스 사회에서의 개인정보보호를 위해 개인정보의 분산 저장관리를 가능하게 하는 기술로서 사용될 것이다.

2.4.2 개인정보의 안전한 추출

정보기술의 발달로 기술적이고 교묘한 방법으로 개인정보를 추출하거나, 개인 정보를 자동적으로 추론하는 등의 기법으로 개인의 디지털 정체성을 새롭게 생성해냄으로써 개인 프라이버시를 침해하고 있다.

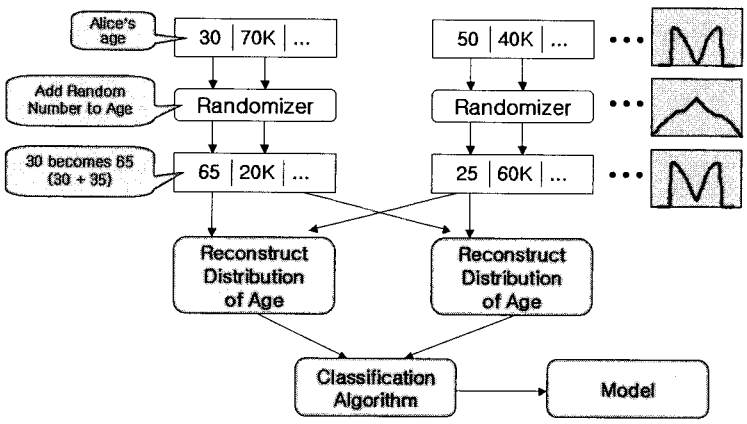
최근 활용되고 있는 데이터 마이닝의 목적은 구매정보 등의 개인정보를 대량으로 모아 관련 상품 구매분석 등 일반적으로 성립되는 규칙을 찾아내는 것이다. 일반화된 규칙 자체를 공개하는 것은 프라이버시상 문제는 없지만 데이터 마이닝의 과정에서 개인정보가 마이닝 엔진에 보내짐으로써 프라이버시 침해 우려가 발생될 수 있다.

이를 방지하기 위해 구매이력 등 관련 개인정보를 열람하고자 하는 목적, 대상 및 서비스의 목적에 따라 차등적으로 개인정보의 범위를 선택적으로 추출해 주는 기술인 프라이버시 보호 데이터마이닝 (PIDM, Privacy Incorporated Data Mining) 기술이 필요하다.

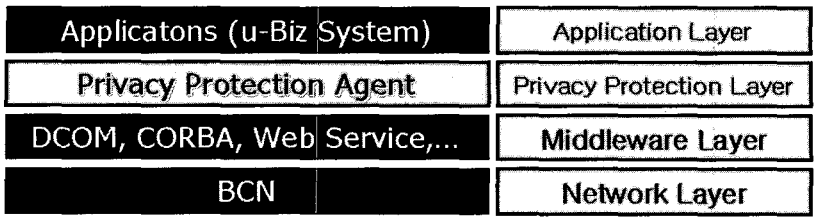
PIDM은 급여나 연령 등의 통계적 분포로부터 개인의 급여나 연령을 직접 모으지 않고 이러한 숫자에 난수를 부가해 랜덤화하며 수집한 것으로부터 원래의 급여나 연령 분포를 복원함으로써 개인의 프라이버시를 보호하고 있다.

예를 들면, 브라우저상의 앙케이트를 생각하면, 브라우저의 Java 스크립트 등에 의해 입력치가 랜덤화되어 서버에 보내지게 된다. 또한, 랜덤화할 수 있는 대상은 수치 속성뿐만이 아니라 직업 등의 분산치에도 적용 가능하다.

즉, 웹 사용자가 나이나 연봉과 같은 개인정보를 입력하면, 입력된 숫자에 개별적인 랜덤한 숫자를 더하거나 빼는 등의 방법으로 개인정보를 보호하고 있



〔그림 5〕 랜덤화를 통한 개인정보의 보호 예



〔그림 6〕 PPI계층구조

다.〔그림 5〕 위에서 열거한 요구사항 외에 운용관리 측면에서 개인정보 노출 등에 대한 기록, 감시 기능이 필요하게 된다.

일반적으로 대량의 개인정보 누설은 내부로부터 발생하고 있는 것이 대부분이다. 즉, PC나CD-ROM, DVD 등의 형태로 개인정보가 노출되는 경우가 많다. 이를 방지하기 위해 개인정보 데이터의 사용, 가공, 복사, 삭제, 매체 전달 등의 행위가 있는 시간과 개인을 추적할 수 있는 로그 등의 기록, 감시 기능이 필요하게 된다.

정보시스템의 로그 기록 기능을 사용해서 중요한 개인정보 접근에 관한 상세 기록을 구현함과 동시에 정기적으로 분석하고, 부정사용이나 누설의 유무를 감시한다. 많은 종류의 대량의 로그를 정규화하고 효과적으로 감시할 수 있도록, 그리고 누설 사건이 발생했을 경우에 신속하게 그 범위나 시간, 경로에 의해 개인을 추적할 수 있도록 한다.

Ⅲ. 프라이버시 보호 인프라(Privacy Protection Infrastructure)

2장에서는 개인정보 보호에 필요한 요구사항과 그 대책에 대하여 살펴보았다. 본 절에서는 요구사항에 따라 향후 개발 필요성이 있는 PPI를 설계한다.

3.1 PPI 계층구조

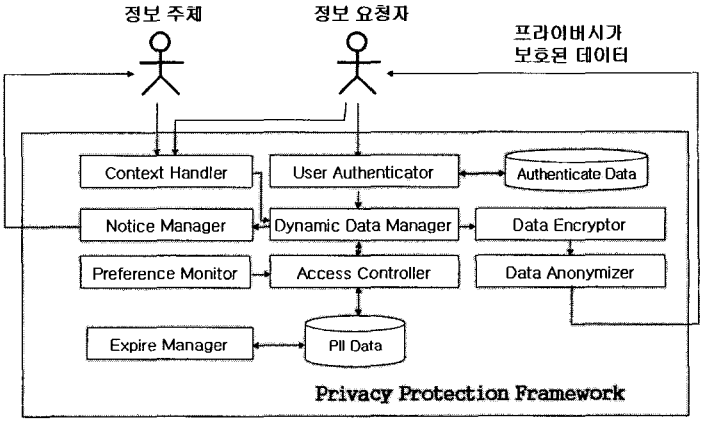
PPI는 각종 개인정보보호 어플리케이션 (u-Biz 시스템)의 하단에서 중간 매개 역할을 하며 사용자의 개인 정보를 상황에 따라 관리한다. Network 계층은 BcN, USN, WiBro 네트워크와 같은 통합/융합망을 의미한다. 그리고 Middleware계층은 Ubiquitous Web Service 기반 Middleware Platform으로 이루어진다. Application 계층은 개인정보보호 서비스 어플리케이션을 포함하며 Privacy Protection 계층에서는 익명성 제공기술 및 PPA 에이전트기술, 네트워크 기반기술, Data Mining 등을 포함한다. PPI 계층구조는 〔그림 6〕에 나타나 있다.

3.2 요구사항에 근거한 프라이버시 보호 모듈 구성

〔표 1〕〔그림 7〕 은 요구사항에 따라 설계한 프라이버시 보호 모듈을 나타내고 있다. Context Handler 및 User Authenticator, Notice Manager는 수집단계에서 작동한다. Dynamic Data Manager 및 Data Encryptor는 저장 단계에서 작동하며, Preference Monitor 및 Access Controller 및

〔표 1〕 요구사항에 근거한 모듈 구성

구성 모듈	요 구 사 항
User Authenticator	정당한 수집
Preference Monitor	이용 목적, 범위의 명시
Notice Manager	상세한 접근제어/관리 수행, 보안 이벤트 관리
Dyamic Data Manager	보유 데이터의 공개, 정정의 구조
Access Controller	부주의한 공개 방지 대책 및 적절한 운용
Data Encryptor	정확성 및 안전성의 확보
Expire Manager	폐기 방법의 확정과 적절한 운용
Data Anonymizer	프라이버시를 고려한 개인정보 이용
Context Handler	유비쿼터스 환경을 위한 Context 처리



〔그림 7〕 프라이버시 보호 프레임워크(PPF) 구성

Data Anonymizer는 정보 이용 단계에서 작동하고, Expire Manager는 정보 폐기 단계에서 작동한다.

3.3 프라이버시 보호 프레임워크(Privacy Protection Framework)

Privacy Protection Framework(PPF)의 각 모듈 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.

Ⅳ. 결 론

본 논문에서는 IT 환경변화에 따른 프라이버시보호의 필요성에 대해 살펴보았고 IT 기술발전 과정에서 필요하게 될 개인정보보호 요구사항을 검토하였다.

또한, 요구사항에 대한 대응책으로 프라이버시 보호 프레임워크를 제안하였다. PPF를 통하여 주요 개인정보를 상황에 따라 권한 있는 자만이 접근할 수 있도록 하며, 개인정보의 활용범위를 통제할 수 있다.

향후에는 개인정보보호 기술개발을 위한 요구사항을 체계적으로 구체화해서 유비쿼터스 IT 환경에 적합한 개인정보보호기술 개발에 착수해야 할 것이다. 또한, 개인정보가 갖는 특성을 고려해서 기존의 정보보호시스템이 갖는 한계점을 분석한 후 이를 해결할 수 있는 새로운 프라이버시 보호 인프라 및 프라이버시를 고려한 개인정보보호체계 분석도 병행되어야 한다.

참 고 문 헌

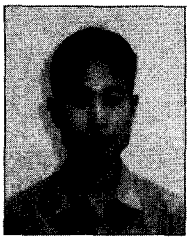
〔1〕 한국전산원, 개인정보보호를 위한 기술개발 및 기술정책에 관한 보고서, 2004.9
〔2〕 서동일, 개인정보보호기술의 개발과 산업육성, ETRI, 2005
〔3〕 PORTIA Project, http://crypto.stanford.edu/portia
〔4〕 MIPA Project, http://www.cs.jhu.edu/~ateniese/mipa.html
〔5〕 IBM, http://www-6.ibm.com/jp/services/secur

ity/features/
[6] **PISA** Project, http://pet-pisa.openspace.nl/pisa org/pisa/index.html
[7] P3P, The Platform for Privacy 「Preferences 1.0(P3P 1.0) Specification」, http://www.w3.org/p3p
[8] JJ.Borking, "M. van Eck, P.Siepel, Intelligent Software Agents and Privacy"
[9] www.pet-pisa.nl, "Privacy Incorporated Software Agent System Architecture (PSA)"
[10] Handbook of Privacy and PET (Privacy Enhancing Technology), PISA Project
[11] IBM TPM, Tivoli Privacy Manager, http://www-6.ibm.com/jp/software/tivoli/products/privacy.html
[12] NTT, Secure USB 메모리, http://www.ntt.co.jp/
[13] NEC, http://www.nec.co.jp
[14] 윤재석, 국외 프라이버시보호기술의 개발 동향과 발전 전망, 한국정보보호진흥원, 2001.3
[15] 조동기, 김성우, 인터넷의 일상화와 개인정보보호, KISDI 이슈리포트, 2003.8.25
[16] 지승훈, 개인정보보호 동향 및 서비스 제공자의 책임, 전자신문, 2005.8.2
[17] 홍준형, 도청·해킹 기술 갈수록 정교-개인정보보호법 제정 시급, 한국일보, 2005.8.17
[18] KT, 인터넷 개인정보노출 막는다, 디지털타임스, 2005.8.19
[19] 윤재석, P3P의 논의 현황과 문제점 및 국내정책 방향, 전자신문, 2005.3.28
[20] 이성몽, 유비쿼터스 컴퓨팅 환경에서 개인정보보호방법, 국민은행 전산정보그룹, 정보통신연구진흥원 (www.iita.re.kr), 주간기술동향, 2005.5.4
[21] 윤용근, 정병주, "유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형분석," 한국전산원 정보화정책 이슈, 2004.
[22] 박승창, "유비쿼터스 IT의 2030년 사용자 시나리오(I, II, III, IV, V, VI, VII)," 전자부품연구원 전자정보센터(www.eic.re.kr)
[23] 개인정보 보호백서, 2002.
[24] 강달천, "유비쿼터스 컴퓨팅 환경에서의 개인정보보호," 한국인터넷 법학회, Mobile · Ubiguitous와 법제, 12, 2004, pp.19-45
[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] IBM, http://www-6.ibm.com, 프라이버시: 개인존중을 바탕으로 한 서비스: Steven Adler와의 인터뷰
[30] 정보통신부, 중장기정보보호로드맵, 2005.5
[31] 한국정보보호산업협회, 2004.11
[32] 정보통신부, 개인정보보호를 위한 종합대책(안), 2005.9
[33] Takuya Iwamoto, 정보관리 방식 「임계치 비밀 분산법」, 2004/11/27

〈著 者 紹 介〉

송 유 진 (You Jin Song)
회원

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

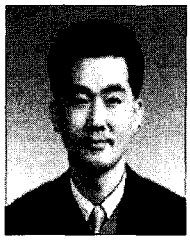


이 동 혁 (Dong Hyeok Lee)
학생회원

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

남 택 용 (Nam Taek Yong)
회원

1987년 충남대학교 계산통계학과 이학사
1990년 충남대학교 계산통계학과 이학석사
2005년 한국외국어대학교 전자정보공학과 공학박사
1987년 ~ 현재 한국전자통신연구원 정보보호연구단 개인정보보호연구팀 팀장(책임연구원)
관심분야 : 정보보호, 인터넷, 이미지마이닝 등



장 종 수 (Jang Jong Soo)
회원

1984년 경북대학교 전자공학과 공학사
1986년 경북대학교 전자공학과 공학석사
2000년 충북대학교 컴퓨터공학과 공학박사
1989년 - 현재 한국전자통신연구원 네트워크보안그룹 그룹장(책임연구원)
한국정보보호학회 이사
학회지 편집위원장
한국정보처리학회 논문지 편집위원
한국정보과학회 논문지 편집위원
한국통신학회 회원