경영정보학연구
제18권 제1호
2008년 3월

프라이버시 보호 상황인식 시스템 개발을 위한 쌍방향 P3P 방법론*

권 오 병**

A Mutual P3P Methodology for Privacy Preserving Context-Aware Systems Development

Ohbyung Kwon

One of the big concerns in e-society is privacy issue. In special, in developing robust ubiquitous smart space and corresponding services, user profile and preference are collected by the service providers. Privacy issue would be more critical in context-aware services simply because most of the context data themselves are private information: user's current location, current schedule, friends nearby and even her/his health data.

To realize the potential of ubiquitous smart space, the systems embedded in the space should corporate personal privacy preferences. When the users invoke a set of services, they are asked to allow the service providers or smart space to make use of personal information which is related to privacy concerns. For this reason, the users unhappily provide the personal information or even deny to get served. On the other side, service provider needs personal information as rich as possible with minimal personal information to discern royal and trustworthy customers and those who are not. It would be desirable to enlarge the allowable personal information complying with the service provider's request, whereas minimizing service provider's requiring personal information which is not allowed to be submitted and user's submitting information which is of no value to the service provider. In special, if any personal information required by the service provider is not allowed, service will not be provided to the user.

P3P (Platform for Privacy Preferences) has been regarded as one of the promising alternatives to preserve the personal information in the course of electronic transactions. However, P3P mainly focuses on preserving

* 본 연구는 서울시 산학연 협력사업(과제번호: 10802)의 재래시장 활성화를 위한 u-Market 개발 과제로부터 지원을 받아 수행되었다.

** 교신저자, 경희대학교 국제경영학부

the buyers' personal information. From time to time, the service provider's business data should be protected from the unintended usage from the buyers. Moreover, even though the user's privacy preference could depend on the context happened to the user, legacy P3P does not handle the contextual change of privacy preferences.

Hence, the purpose of this paper is to propose a mutual P3P-based negotiation mechanism. To do so, service provider's privacy concern is considered as well as the users'. User's privacy policy on the service provider's information also should be informed to the service providers before the service begins. Second, privacy policy is contextually designed according to the user's current context because the nomadic user's privacy concern structure may be altered contextually. Hence, the methodology includes mutual privacy policy and personalization.

Overall framework of the mechanism and new code of ethics is described in section 2. Pervasive platform for mutual P3P considers user type and context field, which involves current activity, location, social context, objects nearby and physical environments. Our mutual P3P includes the privacy preference not only for the buyers but also the sellers, that is, service providers.

Negotiation methodology for mutual P3P is proposed in section 3. Based on the fact that privacy concern occurs when there are needs for information access and at the same time those for information hiding. Our mechanism was implemented based on an actual shopping mall to increase the feasibility of the idea proposed in this paper. A shopping service is assumed as a context-aware service, and data groups for the service are enumerated. The privacy policy for each data group is represented as APPEL format.

To examine the performance of the example service, in section 4, simulation approach is adopted in this paper. For the simulation, five data elements are considered:

- UserID
- User preference
- Phone number
- Home address
- Product information
- Service profile

For the negotiation, reputation is selected as a strategic value. Then the following cases are compared:

- Legacy P3P is considered
- Mutual P3P is considered without strategic value
- Mutual P3P is considered with strategic value

The simulation results show that mutual P3P outperforms legacy P3P. Moreover, we could conclude that when mutual P3P is considered with strategic value, performance was better than that of mutual P3P is considered without strategic value in terms of service safety.

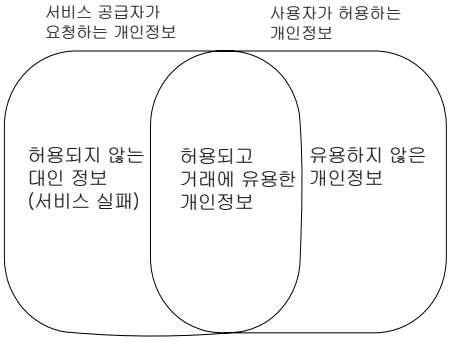
Keywords : P3P, Context-aware Computing, Agent Technology, Privacy-aware System

Ⅰ. 서 론

전자거래의 활성화를 위해 프라이버시에 대한 관심은 현재 매우 큰 사회적인 이슈이다[Culnan, 2003]. 편재적 혹은 유비쿼터스 서비스 및 어플리케이션에서 사용자의 민감한 정보는 다양한 서비스 공급자에 의해 수집되는데, 이는 프라이버시를 위협할 수 있으며 상황인식 컴퓨팅 환경에서 작동하는 전자거래 서비스 내에서는 더욱 강조된다[Adams, 2005].

프라이버시 보호 이슈는 전자거래의 성공을 위해 주목 받는 이슈들 중 하나이며 프라이버시 정책 솔루션의 개발이 중요하다. 예를 들어 수많은 상업적인 웹사이트들은 프라이버시 정책을 제공하는데, 이는 이 사이트들이 사용자에게 이름, 이메일 주소, 특정 선호도, 심지어 주민등록번호까지 요청하고 있기 때문이다. 현재까지 웹사이트의 프라이버시 정책에서는 사용자가 서비스를 등록하기 전에 사용자에게 이에 대해 일일이 열거하여 알려주는 방식이 사용자의 프라이버시에 대한 우려를 감소시킬 수 있는 가장 좋은 방법으로 알려지고 있다.

일반적으로 사용자는 서비스 등록 시 개인적인 정보를 제출해야 하는데, 이는 사용자의 프라이버시 정책과 직결된다. 사용자들은 자신의 프라이버시 정책에 따라 마지못해 혹은 신중하게 그들의 프라이버시를 제공하거나, 아예 서비스 받는 것 자체를 포기하기도 한다. 반면 서비스 공급자는 고객 세분화 등에 활용할 목적으로 가능한 많은 개인적인 정보를 수집하고자 한다. <그림 1>은 서비스 공급자와 서비스 사용자 간의 활용 가능한 정보에 대한 관점의 불일치를 보여준다. 이상적으로는 허용되지 않는 구매자가 노출을 허용하지 않으려는 개인정보 요청을 없애고 사용자는 서비스 공급자에게 프라이버시 보호 우려가 적으면서도 공급자에게 유용한 정보를 최대한 허가해 줌으로써, 결국 허용된 개인적인 정보를 증가시키면서도 동시에 사용자의 프라이버시 침해에 대한 염려를 감소시키는 것이 이상적이다.



<그림 1> 개인 정보의 격차

프라이버시 정책 표준 규격인 P3P는 웹 기반 서비스 사용자가 개인적인 정보를 스스로 제어하고 자동적으로 그 정보가 공유되도록 하기 위해 최근 진행되고 있는 노력들 중 가장 의미 있는 것 중 하나이다. P3P는 P3P 정책에 따라 XML 형태로 표현되며, 프라이버시 정책에 의한 웹사이트에서의 데이터 수집 및 데이터 사용을 위한 방법을 제공한다[Cranor, 2002]. 하지만 P3P를 포함한 현재 기술 수준에서 프라이버시 보호와 서비스 질 간의 균형을 위한 여러 노력들이 실제 거의 효과가 없는 것으로 나타나고 있다[Neustaedter, 2003]. 더욱이 지금까지의 상황인식 서비스에서 프라이버시 관련 연구는 사용자 데이터를 보호하는 관점에서의 정책에 집중되어 왔다. 하지만 연구자들은 그들의 연구에서 사용자 데이터와 서비스 간의 개인적인 정보 교환 과정에서 요구되는 협상 메커니즘은 없음을 가정하고 있다. 그런 까닭에 우리는 동적인 사용자의 개인적인 정보 등록 시 단지 사용자의 자유의 정도를 강화하는 방향으로만 기존의 P3P 기반의 프라이버시 관리를 확장하고 있다. 하지만 공급자의 프라이버시 정책은 사용자 개개인에 맞춰 개인화 되어야 한다. 특별히 평판이라는 측면에서의 사용자 가치는 프라이버시 정책의 개인화를 위한 중요한 고려

요소가 되어야 한다. 그러나 이를 고려한 시스템이 아직 부재하다.

따라서 본 논문의 목적은 기존의 P3P를 확장하여 구매자와 판매자 모두의 프라이버시 관련 선호도 정책을 표현할 수 있고, 상황에 따른 선호도 변화를 감안할 수 있는 쌍방향 P3P를 제안하는 것이다. 이때 협상 방법론은 상호적인 프라이버시 정책, 상황인식적인 정책 디자인, 개인화를 포함하며, 특별히 사용자의 현재 위치, 외부 상황 및 내부 상황과 같은 개인적인 프로파일을 각각 고려한다.

본 논문은 다음과 같이 구성된다. 먼저 제 Ⅱ장에서는 프라이버시 이슈 및 P3P 인지 시스템들을 정리한다. 제 Ⅲ장에서는 쌍방향 P3P 개념과 함께 협상 메커니즘을 기술한다. 제 Ⅳ장에서는 APPEL로 구현한 쌍방향 P3P의 코드를 하나의 실제 사례로 보여주고 실험 결과를 소개한다, 마지막으로 제 Ⅴ장과 제 Ⅵ장에서는 본 연구의 의의에 대한 토의 사항과 결론 및 공헌, 그리고 향후 연구방향 등을 기술하였다.

Ⅱ. 프라이버시 이슈 및 P3P

P3P는 사용자가 웹 기반 서비스를 신뢰를 가지고 사용할 수 있도록 하는 개인 정보에 대한 선호도를 결정할 수 있게 해주는 플랫폼이자 아키텍처이며 또한 프로토콜을 지칭하기도 하다[Cranor, 2002]. W3C는 이미 P3P를 표준으로 받아들여 사용을 권고하고 있으며 성공적인 확산을 위해 노력하고 있다. P3P의 사용자 에이전트 디자인 역시 부분적으로 Code of ethics로부터 비롯되었다. CMA Code of ethics에 기초하여 사용자 에이전트는 <표 1>에 정리된 바와 같은Code of ethics를 따라야 한다[W3C, 2002].

프라이버시 정책을 완성되고 표준화된 방법으로 기술하기 위해 정책 기술 언어인 EPAL과 P3P가 사용되어 왔다. 이 중 P3P에서의 정책 기술은 P3P 기반의 프라이버시 정책에 대한 신텍스와 시멘틱스로 정의되어 있다. 그 기술서는 기계가 읽을 수 있는 형식으로 되어 있어 사용자 에이전트는 P3P 기술서 이해할 수 있다. 또한 이를 통해 사용자를 대신하여 자동적으로 적절한 의사결정을 수행함으로써 사용자는 그들이 방문하는 모든 사이트의 프라이버시 정책을 일일이 읽을 필요가 없어진다. 사용자 에이전트는 사용자의 정책 하에서 사용자를 대신하여 서비스와의 상호작용을 조정하는 프로그램이다. 사용자 에이전트는 e-지갑 혹은 사용자 데이터 관리 도구들로 구축될 수 있다.

P3P 기반의 다양한 프라이버시-인지 유비쿼터스 및 편재적 시스템은 최근 10년간 끊임없이 제안되어 왔다. 전산학 분야에서는 기술적인 메커니즘 제안과 구현 가능성에 초점을 두어 제안되어 왔다[Ackeman, 2004; Jutla, 2006]. 또한 프라이버시 관리 및 거래성사에 대한 기대수익이라는 관점에서의 경제 모델이나 유비쿼터스 컴퓨팅 내 정보 흐름을 분석하기 위해 경제학 기반의 접근법을 사용하는 등 경제학적인 접근법도 제안된 바 있다[Price, 2005].

또한 P3P는 이론으로 그치지 않고 실용화 단계로 진입하고 있다. 예를 들어 마이크로소프트사는 이미 Internet Explorer 6.0에 P3P를 채택하였다. 또한 AT&T(http://privacybird.com)나 JRC (http://p3p.jrc.it)에서도 P3P기반의 사용자 에이전트를 운영토록 허용하고 있다.

그러나 P3P가 완전한 표준으로 자리잡기 위해서 해결해야 하는 문제가 아직도 남아 있다. 첫째로, APPEL기반의 P3P는 사용자가 직접 자신의 선호도를 입력해야만 작동되는 메커니즘이며 이것이 사용자의 사용용이성을 떨어뜨린다. 그래서 이를 위해 P3P를 더욱 개선한 새로운 언어가 제안되기도 한다. 예를 들어 Xpref는 P3P의 APPEL이 더욱 쉽게 사용자 선호도를 기술할 수 있게 해주는 언어이다[Agrawal, 2005]. 또한 McBride 등은 RDFS 기반의 P3P언어를 개발하여 사용자 선호도에 대해 보다 풍부하게 표현할 수 있도록

<표 1> Code of ethics

Category	Code of ethics
게시 및 커뮤니케이션	사용자에게 서비스의 정보 활용을 보여주는 메커니즘을 제공한다.
	사용자가 개인적인 정보를 사용자 에이전트 facility로 변화하는 것에 대해 쉽게 검토하고, 이를 동의하거나 거절할 수 있는 옵션을 제공한다.
	사용자의 동의없이 서비스 공급자가 프라이버시를 디폴트로 설정하지 않도록 한다.
	사용자 에이전트에 의해 제공되는 프라이버시관련 옵션에 대해 사용자에게 알린다.
선택 및 제어	사용자에게 그들의 선호도에 따라 커스터마이징 할 수 있게 하는 환경설정 도구를 포함한다.
	사용자로 신뢰된 상대로부터 P3P 선호도를 가져와 커스터마이즈 할 수 있게 한다.
	사용자에게 자연스럽게 혹은 프라이버시에 맞춰진 방법으로 환경설정 옵션을 보여준다.
	설치 혹은 환경설정의 한 과정으로 사용자에 요청하지 않고 사용자의 개인적인 정보를 저장하는 것을 가능하게 한다.
공평성 및 완전성	사용자에 의해 기입된 정책에 따라서만 사용자를 대신하여 행동할 수 있다.
	서비스 공급자의 행동은 정확하게 표현되어야 한다.
보안	에이전트에 의해 유지되는 모든 데이터 리파지토리에 저장된 프라이버시의 보호를 위한 메커니즘을 제공한다.
	데이터 전송 안전성을 위해 적절히 신뢰된 프로토콜을 사용한다.
	불안정한 전송 메커니즘이 사용될 때는 사용자에게 경고한다.

고안하였다[McBride, 2002]. 이를 더욱 발전시킨 것이 Rei기반의 이를 신뢰 기반의 추천 시스템에 응용한 바 있다[Kolari, 2004]. 두 번째로, APPEL의 사용이 계산 상의 부하를 낳게 하고 반응 속도가 느려짐으로 말미암아 결과적으로 웹 사용상의 불편을 초래하게 된다. 이를 위해서도 언어를 보완하려는 노력이 진행되고 있다. 세 번째로 표현 상의 한계점이 있다는 것이다. 특히 규칙을 표현하기에는 XML 기반의 APPEL이 한계가 많은 것으로 알려지고 있다[Hogben, 2002].

그러나 무엇보다도 지금까지의 P3P관련 연구는 편재적 컴퓨팅 환경에서 사용자의 상황이 그 사용자의 선호도에 미치는 영향을 전혀 고려하고 있지 않다. 즉, 미치는 영향 서비스 공급자와 사용자 간의 프라이버시에 대한 정책의 차이를 해결하는 방법에 대해서는 좀처럼 언급하고 있지 않다. 실제로 현재 P3P는 보다 좋고 완벽한 상세화 및 사용을 위해 계속 논의되고 있는 중이다. 그러므로 상황인식 컴퓨팅 환경에서 동적인 사용자를 위한 프라이버시-인지 전자거래 서비스는 확장된 P3P 기술서가 요구된다.

Ⅲ. 쌍방향 P3P 메커니즘

3.1 전체 프레임워크

편재형 컴퓨팅 기술을 적용한 서비스에서의 쌍방향 P3P 메커니즘을 위해 <그림 2>와 같은 전체적인 협상 프레임워크를 제안한다. 최적의 서비스 사용량을 확보하기 위해 본 프레임워크는 다음과 두 가지 요구 조건을 만족시키는 것을 목표로 한다.

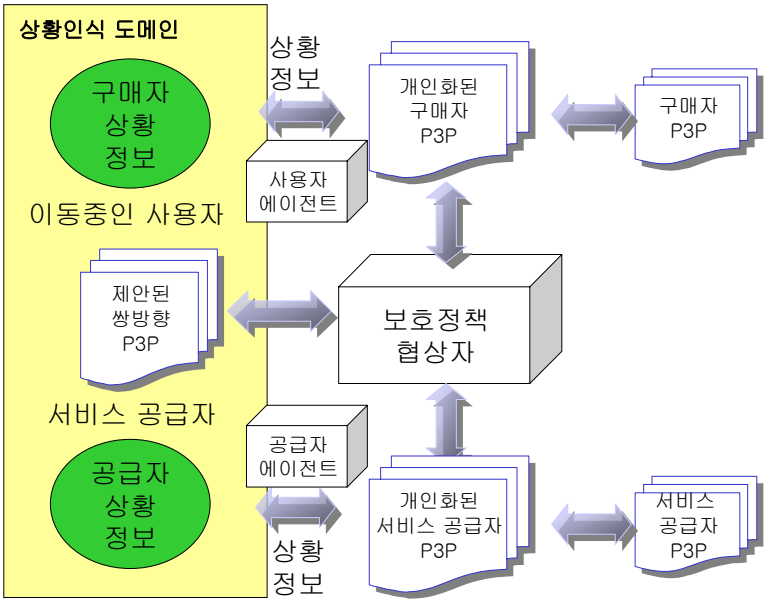
<표 2> 쌍방향 P3P 에서의 확장된 Code of ethics

Category	Code of ethics
게시 및 커뮤니케이션	사용자에게 서비스의 정보 활용을 보여줌과 동시에 서비스 공급자에게도 사용자가 획득한 서비스 관련 정보를 보여주는 메커니즘을 제공한다.
	사용자가 상황 정보를 포함한 개인적인 정보 및 서비스 공급자가 서비스 공급자 관련 정보를 사용자 에이전트 facility로 변화하는 것에 대해 쉽게 검토하고, 이를 동의하거나 거절할 수 있는 옵션을 제공한다.
	사용자의 동의 없이 서비스 공급자가 프라이버시를 디폴트로 설정하지 않도록 하며, 서비스 공급자의 동의 없이 사용자 에이전트가 공급자의 정보를 디폴트로 설정하지 않도록 한다.
	사용자 에이전트에 의해 제공되는 프라이버시 관련 옵션에 대해 사용자에게 알린다.
선택 및 제어	사용자 및 서비스 공급자에게 그들의 선호도에 따라 커스터마이징 할 수 있게 하는 환경설정 도구를 포함한다.
	사용자 및 서비스 공급자로 신뢰 받은 상대로부터 P3P 선호도를 가져와 커스터마이즈 할 수 있게 한다.
	사용자 및 서비스 공급자에게 자연스럽게 혹은 프라이버시에 맞춰진 방법으로 환경설정 옵션을 보여준다.
	설치 혹은 환경설정의 한 과정으로 사용자에 요청하지 않고 사용자의 개인적인 정보를 저장하는 것을 가능하게 한다.
공평성 및 완전성	사용자 및 서비스제공자에 의해 기입된 정책에 따라서만 각각 사용자 및 서비스 공급자를 대신하여 행동할 수 있다.
	사용자 에이전트 및 서비스 공급자의 행동은 정확하게 표현되어야 한다.
보안	에이전트에 의해 유지되는 모든 데이터 리파지토리에 저장된 프라이버시의 보호를 위한 메커니즘을 제공한다.
	데이터 전송 안전성을 위해 적절히 신뢰 받은 프로토콜을 사용한다.
	불안정한 전송 메커니즘이 사용될 때는 해당되는 사용자 또는 서비스 공급자에게 경고한다.

- 사용자의 상황 변동에 따른 동적인 P3P 정책 변화가 가능해야 한다.
- 프라이버시 정책에 대한 사용자 및 서비스 공급자 모두의 상호 동의가 있어야 한다.

한편 이에 따른 확장된 Code of Ethics는 다음 <표 2>와 같이 될 것이다. <표 2>에서 밑줄로 표시된 부분이 서비스 공급자에 관련된 사항으로 새롭게 추가된 부분이며 기존의 Code of Ethics와 차별화되는 부분이 된다.

<그림 2>에서 쇼핑센터와 같이 상황인식이 가능한 물리적 영역이 있다고 가정하자. 그러면 그 영역 내에 존재하는 구매자와 서비스 공급자에 대한 상황 정보가 상황인식 시스템에 의하여 획득되면 구매자 에이전트와 공급자 에이전트는 각각 기존에 존재하는 구매자 P3P기술 및 서비스공급자 P3P기술과 함께 그 상황에 맞는 개인화 된 구매자 P3P 및 개인화 된 서비스 공급자 P3P를 동적으로 작성하게 된다. 이때 사용자 및 서비스 공급자는 각각 그들의 에이전트를 통하여 자동적으로 참여할 수 있다. 보호정책 협상자는 일련의 협상 과정을 통해 결국 쌍방간에 합의가 된 제안된 쌍방향 P3P기술을 작성하여 구매자와 서비스 공급자 사이에 상호작용을 시작하도록 한다. 이러한 서비스가 작동되는 플랫폼은



<그림 2> 쌍방향 P3P 기반 서비스 제공 프레임워크

웹 서비스를 기반으로 하는 것이 좋으며 상황인식을 위해서는 센서 네트워크와 관련 미들웨어가 기본 모듈로 필요하다. 그리고 보호정책 협상자를 포함한 에이전트들은 미들웨어 상위에 존재하며 쌍방향 P3P 어플리케이션을 형성한다. 그리고 최종적으로 사용자 인터페이스는 웹 브라우저 혹은 웹 기반의 일반 인터페이스를 사용하게 될 것이다.

본 연구에서는 P3P문서에 대해 P3P 1.0 기술서를 채택하였는데, P3P 1.0 기술서의 정책 레퍼런스는 P3P 정책이 잘 알려진 곳에 위치하는 것을 허용하므로 우리는 서비스 에이전트 및 사용자 에이전트가 서비스 실행을 위한 협상 시 쉽게 액세스할 수 있도록 프라이버시 정책 정보는 온톨로지 파일로 저장되는 것으로 가정한다.

편재적 컴퓨팅 서비스 환경에서 동적 사용자를 위한 사용자 인터페이스는 웹 브라우저만으로 국한되지 않으며, 멀티모드, 상호작용, 증강현실, 행동인지와 같은 진보적 기술의 반영이 가능한 인터페이스로 확장될 것이다. 이러한 이유로 본 프레임워크에서는 쌍방향 P3P 협상 상호작용이 포함된 서비스를 위한 편재적 컴퓨팅 서비스 존을 그 인터페이스로 설정했다. 이 존 내에서는 여러 센서들을 통해 사용자의 현재 상황 데이터가 탐지되며, 그 정보는 미리 서비스되고 있던 센서 네트워크를 통해 사용자 에이전트로 전달된다.

서비스 존으로 들어설 때 사용자 에이전트는 사용자의 입장에서 서비스를 선택하기 위해 서비스 리스트를 액세스 한다. 편재적 컴퓨팅 서비스는 해당 규칙에 맞추기 위해 현재 규제 제도에 대한 인지 과정을 반드시 포함한다[Price, 2005].

3.2 서비스 공급자의 프라이버시 정책

서비스 공급자의 프라이버시 정책은 서비스 에이전트로 하여금 사용자 에이전트와 어떤 정보를 제공할 것인가의 합의에 도달하기 위한 협상을 진행할 수 있게 하므로 사용자의 프라이버

<표 3> 서비스 공급자의 프라이버시 선호 관련 목적 및 카테고리

Purpose	<s_current/>	One-time getting informed activity
	<s_develop/>	Individual R&D (e.g. research paper)
	<s_pseudo-analysis/>	Pseudonymous analysis
	<s_pseudo-decision/>	Pseudonymous decision
	<s_individual-analysis/>	Analysis for R&D purpose and reporting
	<s_individual-decision/>	Decision for directly affecting the service provider
	<share_small/>	Share with my small group (e.g. family, study group)
	<share_all/>	Share with many and specifiedpersons (e.g. personal homepage, BBS, etc.)
	<academic/>	Academic activity (e.g. lecture)
	<commerce/>	Commercial use
	<other-purpose> string <other-purpose/>	Misc.
Category	<s_physical/>	Physical contact information (e.g. internal phone number, company profile, CEO)
	<s_online/>	Online contact information (e.g. e-mail)
	<s_uniqueid/>	Non-financial identifiers (e.g. web site ID)
	<s_financial/>	Financial information (e.g. ROI, Income statement)
	<s_computer/>	Computer information (e.g. IP, OS)
	<s_content/>	Content (e.g. e-mail text, chat text)
	<s_preference/>	Preference data on likes or dislikes (e.g. color, music)
	<product/>	Product information (e.g. image, logo, brand)
	<code/>	Source code (e.g. web page code)
	<other-category> string </other-category>	Miscellaneous

시 정책만큼이나 필수적이다. 사용자와 비교해 볼 때 서비스 공급자는 평판이 높은 더 가치 있는 사용자를 선호한다. 예를 들어 서비스를 액세스하고 서비스와 관계된 정보를 또 다른 사이트에 전달하거나 허가없이 재판매를 위해 서비스를 재사용하는 사용자에 대해서는 서비스 공급자에게 통보되어야 한다. 이는 공급자가 그들이 서비스를 받기 전이든 아니든 그들의 행동에 대해 사전적인 통제를 가할 수 있게 한다. 또한 서비스 공급자는 서비스 공급자의 경쟁자에게 정보를 전달하는 것과 같이 사용자가 계획하지 않은 목적의 서비스에서 이전에 획득된 정보를 재사용하는 잠재적인 상황에 대한 정책을 가지고 있어야 한다.

즉 서비스 공급자는 회사 프로파일, 상품 정보, 서비스 프로파일, 직원 개인 데이터 등과 같은 서비스에 내장된 정보를 보호하기 위한 고유한 프라이버시 정책을 명확히 해야 한다. 이러한 정보들은 P3P에서 이미 논의되었듯이 고객들의 프라이버시 정책과 서비스 공급자의 프라이버시 정책간의 약간의 차이를 가져온다. 결과적으로 서비스 공급자의 프라이버시 정책 목적 및 카테고리는 <표 3>과 같이 나타낼 수 있다.

예를 들어 서비스 공급자의 웹 페이지 소스 코드는 상품 이미지 파일을 포함하며 쌍방향 P3P에서는 <표 3>을 적용하여 다음과 같이 기술된다.

```
<ENTITY>
  <DATA-GROUP>
   <DATA
ref="#serviceprovider.name">AAAService
</DATA>
   <DATA ref="#
serviceprovider.webpage.code">servi-
ceA.html</DATA>
```

```
<DATA-STRUCT
name="serviceprovider.webpage.code"
    short-description="Web Page Source
Code">
    structref="#html">
    <CATEGORIES><code/><prod-
uct/></CATEGORIES>
</DATA-STRUCT>
```

3.4 협상 방법론

프라이버시에 대한 우려는 액세스를 통해 정보를 얻고자 하는 측과 개인적인 정보를 숨기고 싶어하는 측 간의 긴장이 있을 때 발생한다[Redell, 1992]. 본 논문에서는 사용자 프라이버시에 대한 경제 기반 모델을 협상 방법론에 채택했다. 경제 기반 모형이란 특정의 사용자 프라이버시 방법에 대해 프라이버시를 보호하는 데서 얻어지는 안전성과 관련된 효익과, 그 반대로 불편함에서 비롯되는 비용을 비교하여 사용자의 효용을 극대화하는 의사결정을 탐색하는 것이다. 효용은 기본적으로 누군가의 개인적 정보를 다른 편으로 전달하는 과정에서 발생하는 서비스 결핍 비용과 감시 비용 사이의 트레이드 오프에 의해 계산된다. 이것은 프라이버시 정책과 실제 행동 주체가 트레이드 오프 관계를 가지며 이는 사용자를 복잡하게 하는 전자상거래 상황에서 종종 관찰된다[Berendt, 2005].

우선 프라이버시에 영향을 주는 결정요인이 i, c_j가 i번째 결정요인에 대한 감시 수준 정도라고 할 때, 각 결정요인 별로 서비스 결핍에 따른 비용과 감시에 따른 비용은 감시 수준의 정도에 각각 반비례 및 비례 관계가 성립될 것이다. 또한 감시 수준의 정도에 포만효과가 있다고 가정할 때 그 함수의 모습은 지수함수의 모습을 가지게 될 것이다. 따라서 본 연구에서는 서비스 결핍에 따른 비용은 $y=\alpha_{1i}e^{-\beta_{1i}c_i}$ 이고 감시에 수반되는 비용은 $y=\alpha_{2,i}e^{\beta_{2,i}c_i}$ 라고 보았다. 이때 제안하는 협상 방법론은 다음과 같이 표현될 수 있다.

STEP 1 : 구매자 에이전트 및 공급자 에이전트는 각각 자신의 사용자의 상황기반 P3P 정책을 가져온다. 이때 상황기반 P3P 정책은 식 (1), 식 (2)와 같이 구매자용인 와 공급자용인 로 표현한다.

$$P_B=\{(c_{1B},p_{1B},o_{1B},r_{1B}),\ldots,(c_{iB},p_{iB},o_{iB},r_{iB}),\ldots,(c_{NB},p_{NB},o_{NB},r_{NB})\} \quad (1)$$

$$P_S=\{(c_{1S},p_{1S},o_{1S},r_{1S}),\ldots,(c_{iS},p_{iS},o_{iS},r_{iS}), \quad (2)$$

P3P 정책에 포함된 데이터 요소의 개수가 N개일 때, C, P, O는 $c_{i.}\in C$, $p_{i.}\in P, o_{i.}\in O=\{always, opt-in, opt-out\}, r_{i.}\in R$를, R은 카테고리, 목적, 옵션, 각각의 집합을 나타낸다.

STEP 2 : 구매자 에이전트 및 판매자 에이전트 전체비용을 최소화하는 최적의 솔루션을 제공한다. 구매자 및 판매자의 전체비용은 각각 다음 식 (3) 및 식 (4)와 같이 표현될 수 있다.

$$TC_{VB}=Min(f_{1B}(c^*_{1B}|p_{1B},o_{1B},r_{1B}),f_{2B}(c^*_{2B}|p_{2B},o_{2B},r_{2B}),\ldots,f_{NB}(c^*_{NB}|p_{NB},o_{NB},r_{NB})) \quad (3)$$

$TC_{US}=Max\{f_{1S}(c^*_{1S}|p_{1S},o_{1S},r_{1S}),f_{2S}(c^*_{2B}|p_{2S},o_{2S},r_{2S}),..f_{NS}(c^*_{NB}|p_{NS},o_{NS},r_{NS})\}$

(4)

$c_{i.}$ 는 i번째 카테고리에 대한 감시 수준을 의미하며, 서비스 결핍 비용이 $y=\alpha_{1i}e^{-\beta_{1,}c_i}$ 이고, 감시 비용이 $y=\alpha_{2,i}e^{\beta_{2,}c_i}$ 의 형태일 때 $f_i(c_i^*\mid p_i,o_i,r_i)=\alpha_{1i}e^{-\beta_{1,}c_i}+\alpha_{2i}e^{\beta_{2,}c_i}$ 이다. 여기에서 i번째 데이터 요소의 최적의 감시 수준을 몬테칼로 시뮬레이션 방법으로 구한다.

STEP 3 : $TC_{U.}=f_{M.}(c^*_{M.}\mid p_{M.},o_{M.},r_{M.}),1\le M\le N$ 를 가정했을 때 각 사용자 정책의 최적 집합인 $\{c^*_{1B},c^*_{2B},..c^*_{iB},..c^*_{NB}\mid p_{1B},..p_{NB},o_{1B},..o_{NB}r_{1B},..r_{NB}\}$ 및 $\{c^*_{1S},c^*_{2S},..c^*_{iS},..c^*_{NS}\mid p_{1S},..p_{NS},o_{1S},..o_{NS}r_{1S},..r_{NS}\}$ 은 협상자에게 전달되고, 협상자는 구매자와 서비스 공급자가 각각 제안한 프라이버시 정책을 비교한다.

STEP 4 : i 번째 카테고리의 서비스 에이전트 집합은 $c_i=c_i^*$ 이다. 이 때 구매자 및 서비스 공급자의 전체 비용은 각각 식 (5), 식 (6)과 같이 표현될 수 있다.

$TC_B=Max\{g_{1B}(p^*_{1B},o^*_{1B},r^*_{1B}\mid c_{1B}),..g_{jB}(p^*_{jB},o^*_{jB},r^*_{jB}\mid c_{jB}),..g_{NB}(p^*_{NB},o^*_{NB},r^*_{NB}\mid c_{NB})\}$

(5)

$TC_S=Max\{g_{1S}(p^*_{1S},o^*_{1S},r^*_{1S}\mid c_{1S}),..g_{jS}(p^*_{jS},o^*_{jS},r^*_{jS}\mid c_{jS}),..g_{NS}(p^*_{NS},o^*_{NS},r^*_{NS}\mid c_{NS})\}$

(6)

STEP 5 : 구매자와 서비스 공급자의 정책을 고려한 협상자 입장에서의 최적의 프라이버시 정책 집합은 식 (7)과 같이 표현될 수 있다. 만약 이 정책 집합이 공집합이면 완화 과정인 STEP 6으로 진행한다.

$$r_1^*,...,r_j^*,...,r_N^*\mid c_1,...,c_i,...,c_N\} \quad (7)$$

STEP 6 : 구매자 및 공급자 에이전트에게 각각 상대방의 전략적 가치(V)에 대한 평가를 하도록 한다. 전략적 가치에 대한 평가 함수는 다음 식 (8)과 같다.

$$V=h(I,E) \quad (8)$$

이때 I는 상대방과 자신과의 내적 관계에서의 전략적 가치이며, E는 상대방의 일반적인 전략적 가치를 의미한다. 예를 들어 구매자가 그 서비스 공급자의 서비스를 그 동안 얼마나 많이 사용해 왔는지에 대한 거래 실적 등이 I에 속하게 되며, 그 구매자의 일반적인 신용등급, 사회적 명성, 직업, 소득 수준 등은 E에 속하게 될 것이다. 각 에이전트는 각기 나름대로의 전략적 가치 관련 함수를 가질 수 있다. 협상 가능성 평가를 위해 STEP 7로 이동한다.

STEP 7 : 식 (8)의 식으로 얻어진 전략적 가치 (V) 값이 임계치($\theta_{t.}$)보다 충분히 큰 경우 이전 프로세스의 현재 선택된 최대값을 유발한 요소를 고려 대상에서 제외하고 다시 STEP 3로 돌아간다. 단 여기서 임계치의 t는 협상 반복 수이며 임계치는 t에 비례하여 증가하게 된다. 증가 함수는 각 에이전트의 고유 권한이다. 한편 전략적 가치 값이 충분히 크지 못한 경우에는 멈추게 되며, 협상은 결렬된다.

<표 4> 쇼핑 시나리오에서의 데이터 그룹

	Data group	Category	Purpose	Option	Retention
Service user	UserID User preference Phone number Home address	<government/> <preference/> <physical/> <physical/>	<tailoring/> <pseudo-decision/> <pseudo-decision/> <pseudo-decision/>	Opt_in Opt_in Opt_in Opt_in	<no-retention/> <stated-purpose/> <stated-purpose/> <stated-purpose/>
Service provider	Product information Service profile	<product/> <s_physical/>	<share_small/> <s_develop/>	Opt_in Opt_in	<indefinitely/> <stated-purpose/>

Ⅳ. 실 험

쌍방향 P3P가 어떻게 작동되는지를 쇼핑 상황에서 시뮬레이션 방법으로 실험했다. 이때 쇼핑 서비스 시나리오에서 참조하는 카테고리, 목적, 보존의 내용을 포함한 데이터 그룹은 다음 <표 4>와 같다고 하자.

첫째, 실험 대상 서비스의 정적 프라이버시 정책은 APPEL로 다음과 같이 표현될 수 있다.

```
<appel:RULESET xmlns:ap-
pel="http://www.w3.org/2002/04/APPELv1"
xmlns:p3p="http://www.w3.org/2000/12/P
3Pv1"
crtdby="W3C"
crtdon="2000-03-15T16:41:21+01:00">
<appel:RULE behavior="limited"
prompt="yes"
description="Service collects personal
ID and preference.">
promptmsg="Warning! Service collects
personal ID, phone number, home address
and preference. Do you want to continue
(using limited access)?">
   <p3p:POLICY>
     <p3p:STATEMENT>
       <p3p:DATA-GROUP>
         <p3p:DATA ref="#
          serviceuser.id.Activity.public">
           <p3p:CATEGORIES>
             <p3p:government/>
            </p3p:CATEGORIES>
         </p3p:DATA>
       </p3p:DATA-GROUP>
    <p3p:DATA ref="#
serviceuser.phone.number">
          <p3p:CATEGORIES>
            <p3p:physical/>
           </p3p:CATEGORIES>
        </p3p:DATA>
       </p3p:DATA-GROUP>
    <p3p:DATA ref="#
serviceuser.home.address">
          <p3p:CATEGORIES>
            <p3p:physical/>
           </p3p:CATEGORIES>
        </p3p:DATA>
       </p3p:DATA-GROUP>
         <p3p:DATA ref="#
          serviceuser.current.preferen
          ce.Activity.public">
          <p3p:CATEGORIES>
               <p3p:preference/>
          </p3p:CATEGORIES>
        </p3p:DATA>
       </p3p:DATA-GROUP>
     </p3p:STATEMENT>
   </p3p:POLICY>
  </appel:RULE>

 <appel:RULE behavior="request"
prompt="yes"
description="Service collects data for
tailoring or
pseudo-decision purposes.">
promptmsg="FYI: This service collects
data for tailoring or anonymous decision
purposes. Continue?">
```

```
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:PURPOSE appel:con-
         nective="or">
          <p3p:tailoring/>
          <p3p:pseudo-decision/>
    </p3p:PURPOSE>
      </p3p:STATEMENT>
    </p3p:POLICY>
 </appel:RULE>
</appel:RULESET>
```

한편 서비스 사용자의 정적 프라이버시 정책은 다음과 같이 표현될 수 있다.

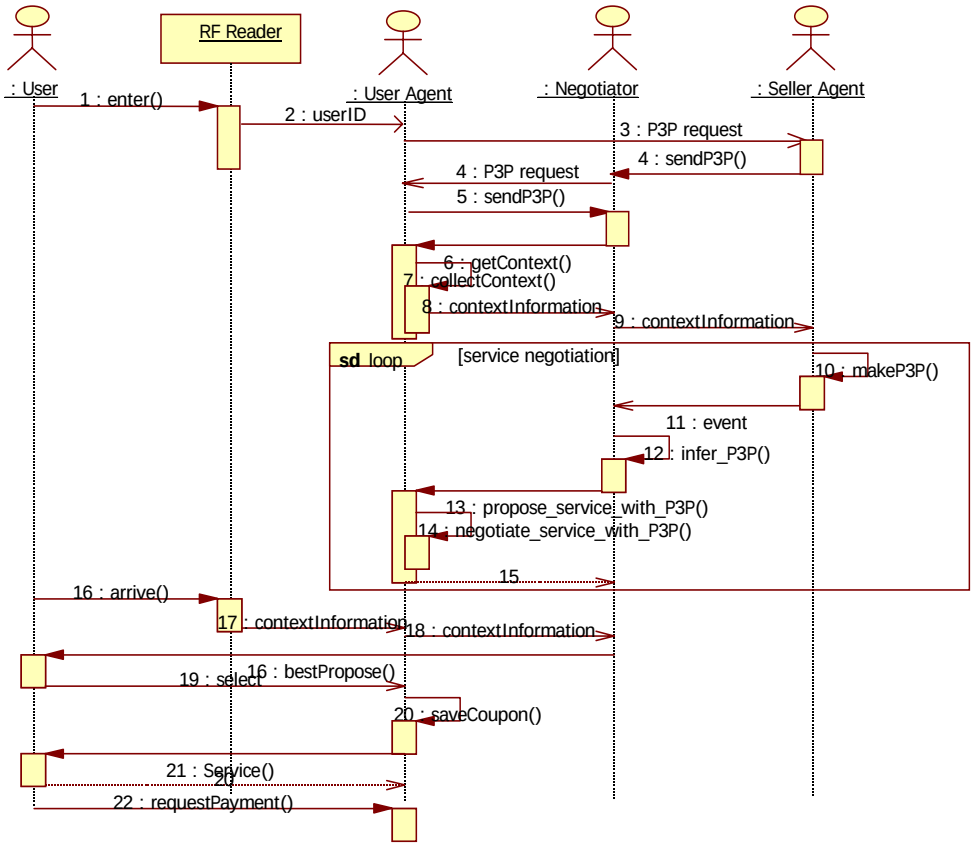
```
<appel:RULESET xmlns:ap-
pel="http://www.w3.org/2002/04/APPELv1
"
xmlns:p3p="http://www.w3.org/2000/12/P
3Pv1"
crtdby="W3C"
crtdon="2000-03-15T16:41:21+01:00">
<appel:RULE behavior="limited"
prompt="yes"
description="The user collects product
and service profile.">
promptmsg="Warning! The user collects
product and service profile. Do you want
to continue (using limited access)?">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:DATA-GROUP>
          <p3p:DATA
           ref="#company.product.information">
            <p3p:CATEGORIES>
              <p3p:product/>
             </p3p:CATEGORIES>
          </p3p:DATA>
        </p3p:DATA-GROUP>
           <p3p:DATA ref="#service-
            .profile">
            <p3p:CATEGORIES>
                 <p3p:s_physical/>
            </p3p:CATEGORIES>
          </p3p:DATA>
`       </p3p:DATA-GROUP>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>

 <appel:RULE behavior="request"
prompt="yes"
description="The user collects product
and service data for sharing with small
group or individual research purpose.">
promptmsg="FYI: The user collects prod-
uct and service data for sharing with
small group or individual research
purpose. Continue?">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:PURPOSE appel:con-
         nective="or">
          <p3p:share_small/>
          <p3p:s_develop/>
    </p3p:PURPOSE>
      </p3p:STATEMENT>
    </p3p:POLICY>
 </appel:RULE>
</appel:RULESET>
```

한편 사용자와 서비스 공급자 양쪽에서 P3P 파일을 사용하여 쌍방향 P3P 서비스를 수행하는 과정을 설계하기 위하여 시퀀스 다이어그램으로 표현한 것은 <그림 3>과 같다.

프라이버스관련 주요 이슈 중 하나는 사용자들의 프라이버시에 대한 염려에도 불구하고 서비스 이용률을 증가시키는 것이다. 그것은 주로 사용자들이 서비스를 받기 위해 선택적으로 데이터 항목을 제출하는 것이 불가능한 현재 웹기반 시스템의 한계에서 기인한다. P3P 기반 프라이버시-인지 시스템의 경우 조차도 오직 서비스 공급자만 P3P의 컨텐츠를 결정할 수 있다. 따라서 우리는 우리의 협상 메커니즘이 서비스 이용률을 증가시키는데 유의한 정도로 유용한지에 대해 확인해 보았다. 이를 위한 실험에서는 시뮬레이션 접근법을 사용했다.

본 실험에서는 위의 데이터 요소를 가지고 카



<그림 3> 실험 대상 서비스에 대한 시퀀스 다이어그램

테고리를 결정하였으며 다음과 같은 순서로 시뮬레이션을 진행하였다. 단, 시뮬레이션의 단순화를 위하여 공급자의 비용함수는 정해져 있다고 가정하였다.

단계 1 : 각 카테고리별 비용함수를 나타내는 $f_i(c_i^* \mid p_i, o_i, r_i) = \alpha_{1,i} e^{-\beta_{1,i} c_i} + \alpha_{2,i} e^{\beta_{2,i} c_i}$ 에 대해서 감시수준을 나타내는 c_i 외의 모수들은 각 개인별 선호도 값을 입력 받는다.

단계 2 : 각 카테고리별 값 c_i 을 변화시켜가며 노출에 따른 비용과 결핍에 따른 비용을 각각 구하고, 이를 합하여 총비용을 유도한다.

단계 3 : 총비용 중에서 최저 값에 해당하는 c_i 및 다른 모수 값을 결정한다.

단계 4 : 각 카테고리의 최저 값 중에서 최대 비용 값을 도출하고 그 때의 카테고리가 무엇인지 인식한다.

단계 5 : 그 최대 비용 값을 서비스 공급자에 의하여 결정된 허용 값과 비교한다. 이때 허용 값보다 최대 비용 값이 허용 값보다 작으면 거래를 허용하고 멈춘다. 만약 그렇지 않으면 해당 사용자에 대한 전략적 가치 값을 계산하여 협상의 여지가 있는지를 점검한다. 본 시뮬레이션에서는 전략적 가치로서 명성

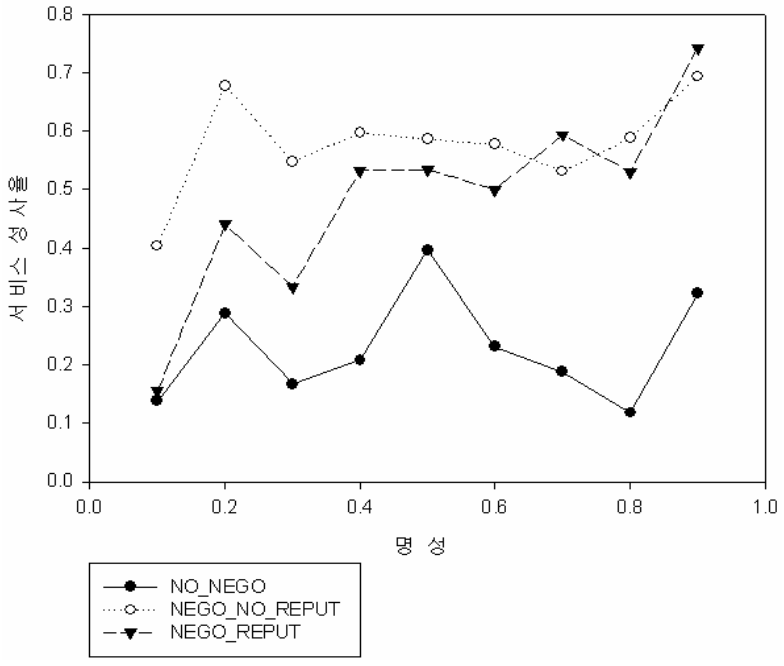
(reputation)을 선정하였다.

단계 6 : 전략적 가치 값이 서비스 공급자가 설정한 값보다 크면 각 카테고리의 최저 값 중에서 두 번째로 큰 비용 값을 도출하여 허용 값과 비교한다. 이때 허용 값보다 최대 비용 값이 허용 값보다 작으면 거래를 허용하고 멈춘다. 만약 그렇지 않으면 해당 사용자에 대한 전략적 가치 값이 추가적으로 협상의 여지가 있는지를 점검한다. 이 상태를 반복 수행한다. 여기서 두 번째 큰 비용 값을 가지는 요소를 고려하는 이유는 명성으로 대변되는 전략적 가치가 크므로 첫번째로 큰 비용 값이 수반되는 사생활 침해 요소에 대해서는 제외하기 때문이다. 따라서 이 경우 두 번째로 큰 비용 값을 가지는 요소가 자연스럽게 사생활 침해 여부 판단의 가장 중요한 요소가 되기 때문이다.

프라이버시 관련 선호도는 카테고리 별 비용을 산정하는데 활용되며, 모든 사용되어야 하는 카테고리의 비용의 최대값이 전체 비용 값이 되고, 최대값에 해당하는 카테고리부터 협상 대상이 된다. 결국 협상 대상 선정과 협상 여부를 결정하는데 사용되었다. 카테고리는 P3P에 일반적으로 활용되는 프라이버시 보호 대상 중에서 시뮬레이션 용도로 선별한 것이다. 단, 본 연구에서는 공급자 측면의 프라이버시 선호도 협상을 논외로 하였기 때문에 사용자 식별번호, 사용자 선호도, 전화번호 및 집주소만을 카테고리로 포함하여 수행하였다.

본 연구의 메커니즘의 우수성을 검증하기 위하여 다음과 같은 세 가지의 방법을 비교하였다.

- 쌍방향 P3P 협상을 고려하지 않고 P3P만 고려한 경우 (NO_NEGO)



<그림 4> 전략적 가치의 수준 변화에 따른 서비스 성사율 변화

- 쌍방향 P3P 협상을 고려하되 전략적 가치를 고려하지 않은 (NEGO_NO_REPUT)
- 쌍방향 P3P협상을 고려하되 전략적 가치로 명성을 활용한 경우 (NEGO_REPUT)

그 결과 <그림 4>와 같이 첫째, 전략적 가치를 고려한 협상이 일반적인 P3P만을 고려한 경우보다는 성공적인 협상을 위해 뛰어나다는 결론을 내릴 수 있다. 두 번째로, 쌍방향 P3P를 고려하되 전략적 가치를 고려한 경우와 고려하지 않은 경우에 대해서는 일견 쌍방간 서비스 성사율에 있어서 커다란 차이가 나지 않는 것으로 보일 수 있다. 그러나 명성이 높은 사람들은 그렇지 못한 사람보다 협상에 있어서 더 호혜적인 것이 상식적이라고 볼 때 <그림 4>는 NEGO_REPUT방법이 더욱 명성이라고 하는 전략적 가치에 기민하게 반응하고 있는 것을 볼 수 있다. 본 예에서 보더라도 구체적으로는 서비스 공급자는 매우 높은 평판을 가진 사용자의 거래 성사율을 82%까지 올릴 수 있었으며, 매우 낮은 평판을 가진 사용자의 거래 성사율은 30% 이하로 낮출 수 있었다. 따라서 어느 때나 서비스 성사율을 높이는 NEGO_NO_REPUT보다는 더욱 현실적이고 지능적이라고 볼 수 있다. 결국 본 연구에서 제안한 쌍방향 P3P에 의한 협상 메커니즘은 서비스 위험을 감소시키기 위해 더 낮은 평판을 가진 사용자를 피하는 등의 선택적인 사용자 유인을 가능하게 할 수 있었다.

V. 토 의

본 연구에서 제안한 쌍방향 P3P는 다음과 같은 부분에서 기존의 P3P 및 P3P 기반 시스템과 차별화 된다. 첫째, 사용자의 동적인 상황에 따라서 광고 혹은 결재에 요구되는 사용자 정보가 변경될 수 있도록 하였다. 이를 위해 상황 정보에 대한 데이터 요소가 추가되었으며, APPEL 형식으로 표현되었다.

둘째, 사용자 정보에 대한 선호도를 기반으로 하되, 협상 과정을 통하여 다양한 대안으로 정보를 요청할 수 있도록 하였다. 기존의 P3P 기반에서는 사용자가 자신이 원하는 사용자 정보 관련 선호도를 일방적으로 결정하고 나면 판매자는 그 결정 사항에 따라서 그 사용자와의 인터페이스가 가능 혹은 불가능이라고 하는 두 가지 대안만을 가질 수 있었다. 그러나 쌍방향 P3P 내에서의 협상 메커니즘은 스스로 사용자 혹은 사용자 에이전트와의 반복적인 대화를 통해 더욱 세밀한 대안을 생성하여 궁극적으로 웹 기반 서비스의 사용 비율을 증가시킬 수 있었다. 이를 보이기 위해 본 논문에서는 사용자가 어떤 상점에 있는지에 대한 위치 정보와 그 상점에서 보는 사용자에 대한 전략적 가치 정보를 주요 상황 정보로 하여 보였으며 완전한 상황 정보를 활용하는 것은 추후 연구로 남겨 두었다.

셋째, APPEL 형식의 정의에 사용자의 선호도뿐 아니라 공급자인 웹 기반 서비스 운영자의 자신에 대한 정보의 노출 선호도도 정의할 수 있도록 하였다. 이것은 웹 상에서 노출되는 정보에 대해 악의의 사용자가 다른 용도로 활용하는 것을 막기 위한 것이며, 이것을 통해서 웹 상에서의 거래의 상호 신뢰를 높일 수 있게 되었다. 이는 P3P의 확장 연구로 알려져 있는 Kolari등의 RDFS를 활용한 Rei기반의 보호 시스템이 온톨로지를 활용하여 표현력을 강화한 것에 비하여 사용자 측면의 프라이버시만을 고려한 것에 비하여 더욱 확장적인 것이다 (Kolari, 2004) 그러나 본 논문에서는 이 부분에 대해서는 APPEL 정의만 보이고, 실제 사용 예는 추후 연구 이슈로 남겨 두었다.

VI. 결 론

쌍방향 P3P 기반의 협상 메커니즘은 서비스 공급자가 요구하는 정보와 사용자가 공유를 승인한 개인적인 정보 사이의 격차를 감소시켜 서비스 매치의 가능성을 증가시키고자 하는 목표

를 가지고 개발되고 평가되었다. 기본적으로 쌍방향 P3P는 동적인 사용자와 특정 공간 내 서비스 공급자의 존재를 가정하고 있으며 서비스가 동적으로 변하는 사용자의 데이터를 따라갈 수 있도록 기술서 내에서 상황 정보 요소들을 고려했다. 이러한 동적인 프라이버시 정책 변화에 기초하여, 상대에게 어떤 정보를 전달하고 어느 범위까지 오픈 할 것인지에 대한 협상을 진행하는 것이 본 논문에서 제시하고 있는 아이디어의 핵심 메커니즘이었다.

향후 연구는 다음과 같은 측면이 포함될 것이다. 첫째로 쌍방향 P3P 기반 프라이버시 상황인식 서비스의 완성도를 높이기 위하여 추가적인 쌍방향 P3P 카테고리나 목적 등을 고려할 것이며, 둘째로 현재는 쌍방간 전략적 가치 정보를 위주로 협상을 하도록 했는데 더욱 다양한 상황정보를 가지고 협상을 하도록 할 것이다. 또한 현재 협상 메커니즘에 대한 최적화 점검을 하지 못했으므로 최적의 성과에 도달하기 위한 협상 메커니즘의 평가를 수행해야 한다. 이는 특정의 집중된 전자거래 공간 내에서 대규모의 개인화 된 P3P 협상을 위해 반드시 점검할 부분이다. 마지막으로 본 연구에서 제안한 쌍방향 P3P에서의 확장된 Code of ethics가 완전히 구현된 것은 아니며, 이는 추후 연구로 수행할 것이다. 또한 시뮬레이션을 통해 보인 것은 공급자의 비용함수를 불변의 것으로 하였고, 전략적 가치는 명성이라는 변수만을 사용했는데, 추후에 이 두 가지를 모두 현실적으로 완화시켜 실험할 것이다.

<참 고 문 헌>

[1] Ackeman, M.S., "Privacy in pervasive environments: next generation labeling protocols," *Personal and Ubiquitous Computing,* Vol. 8 No. 6, 2004, pp. 430-439.

[2] Adams, C. and Katos, V., "Privacy challenges for location aware technologies," *IFIP International Federation for Information Processing*, Vol. 191, 2005, pp. 303-310.

[3] Agrawal, R., Kiernan, J., Srikant, R. and Xu, Y., "XPref: A preference language for P3P," *Computer Networks*, Vol. 48 No. 5, 2005, pp. 809-827.

[4] Berendt, B., Ganther, O. and Spiekermann, S., "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, Vol. 48, No. 4, 2005, pp. 101-106.

[5] Cranor, L., Langheinrich, M., Marchiori, M. and Reagle, J., "The platform for privacy preferences 1.0 (P3P1.0) specification," *W3C Recommendation*, HTML Version at www.w3.org/TR/P3P/, April 2002.

[6] Culnan, M.J. and Bies, R.J., "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues,* Vol. 59, No. 2, 2003, pp. 323-342.

[7] Duckham, M. and Kulik, L., "A formal model of obfuscation and negotiation for location privacy," *Pervasive 2005*, Munich, Germany, 2005, pp. 152-170.

[8] Jutla, D.N., Bodorik, P. and Zhang, Y.J., "PeCAN: An architecture for users' privacy-aware electronic commerce contexts on the semantic web," *Information Systems*, Vol. 31, No. 4-5, 2006, pp. 295-320.

[9] Hogben, G., Jackson, T. and Wilikens, M., "A fully compliant research implementation of the P3P standard for privacy protection: Experiences and recommenda-

tions," *Lecture Notes in Computer Science*, Vol. 2502, 2002, pp. 104-125.

[10] Kolari, P., Ding, L., Kagal, L., Ganjugunte, S., Joshi, A. and Finin, T., *Enhancing P3P framework through policies and trust,* UMBC Technical Report, TR-CS-04-13. September Vol. 9, 2004.

[11] McBride, B., Wenning, R. and Cranor, L., "An rdf Schema for P3P," *W3C Note*, 25 January 2002.

[12] Neustaedter, C. and Greenberg, S., "The design of a context-aware home media space for balancing privacy and awareness," *Lecture Notes in Computer Science,* Vol. 28, Vol. 64, 2003, pp. 297-314.

[13] Price, B., Adam, K. and Nuseibeh, B., "Keeping ubiquitous computing to yourself: A practical model for user control of privacy," *International Journal of Human- Computer Studies,* Vol. 63, No. 1-2, 2005, pp. 228-253.

[14] Redell, D., *Information technology and the privacy of the individual*, Daft ACM Whitepaper on Computer and Privacy, September 1992.

[15] W3C, *http://www.w3.org/TandS/QL/QL98/pp/APPEL-QLW.html,* 1998.

[16] W3C, *http://www.w3.org/TR/2002/WD-P3P-preferences-20020415/,* 2002.

◆ 저자소개 ◆

권오병 (Ohbyung Kwon)
서울대학교 경영대학 학사, 1990년과 1995년에 한국과학기술원 경영과학과에서 경영정보시스템 전공으로 각각 공학석사와 박사학위를 취득하였다. 1996년부터 2003년까지 한동대학교 경영경제학부에 재직하였고 2004년부터 현재까지 경희대학교 국제경영학부에서 교수로 재직 중이다. 2002년에는 미국 Carnegie Mellon University 전산학부의 ISRI에서 유비쿼터스 컴퓨팅 관련 프로젝트를 수행하였다. 관심분야는 상황인식 컴퓨팅, 다중에이전트 기술, 유비쿼터스 서비스 요구분석 및 평가, 의사결정지원시스템 등이며, Decision Support System, ECRA, Behavior and Information Technology, Simulation, 경영정보학연구 등에 관련 학술논문을 다수 게재하였다.

◈ 이 논문은 2007년 12월 27일 접수하여 1차 수정을 거쳐 2008년 01월 21일 게재확정되었습니다.