(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0080645
(43) 공개일자 2009년07월27일

(51) Int. Cl.
H04L 12/12 (2006.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2008-0006522
(22) 출원일자 2008년01월22일
심사청구일자 2008년01월22일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 국제캠퍼스내
(72) 발명자
권오병
경기 용인시 기흥구 신갈동 도현마을 현대아파트 207동 801호
(74) 대리인
김재섭

전체 청구항 수 : 총 13 항

(54) 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피기반의 프라이버시 정책 협상방법

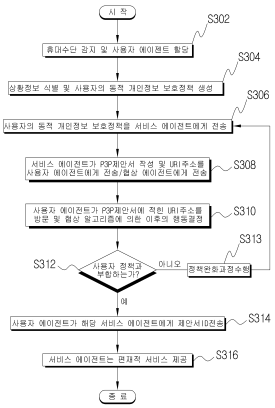
(57) 요 약

본 발명은 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법에 관한 것이다.

유비쿼터스 환경에서 사용자의 휴대수단을 감지하는 적어도 하나 이상의 상황정보감지수단, 상황정보인식수단, 서비스수단 및 적어도 하나 이상의 사용자 에이전트, 서비스 에이전트 또는 협상 에이전트(또는 협상자)를 포함하여 상황인식 서비스를 제공하는 상황서버를 포함하는 프라이버시 정책 방법에 있어서,

(a) 상기 상황정보감지수단으로부터 사용자의 상황정보를 수신받아 사용자 에이전트를 할당하는 단계; (b) 상기 사용자 에이전트가 사용자의 상황정보를 식별하여 사용자의 동적 프라이버시 정책파일을 생성하고, 사용자의 동적 프라이버시 정책파일을 서비스 에이전트에게 전송하는 단계; (c) 상기 서비스 에이전트가 수신된 사용자의 프라이버시 정책을 고려하여 서비스 공급자의 P3P(Platform for Privacy Preferences)제안서를 작성하고 사용자 에이전트에게 URI주소를 전송하는 단계; 및 (d) 상기 사용자 에이전트가 수신된 URI주소를 방문하여 소정의 협상 알고리즘에 의한 서비스 공급자의 P3P제안서를 평가하고 이후의 행동을 결정하는 단계; 를 포함하여 이루어지는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법에 관한 것이다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	10802
부처명	서울특별시
연구사업명	2006년도 서울시 산학연 협력사업 기술기반구축(일반)사업
연구과제명	재래시장 활성화를 위한 u-Market 개발
주관기관	경희대 산학협력단
연구기간	2007년 08월 01일 ~ 2008년 07월 31일

특허청구의 범위

청구항 1

유비쿼터스 환경에서 사용자의 휴대수단을 감지하는 적어도 하나 이상의 상황정보감지수단, 상황정보인식수단, 서비스수단 및 적어도 하나 이상의 사용자 에이전트, 서비스 에이전트 또는 협상 에이전트(또는 협상자)를 포함하여 상황인식 서비스를 제공하는 상황서버를 포함하는 시스템의 프라이버시 정책 방법에 있어서,

(a) 상기 상황정보감지수단으로부터 사용자의 상황정보를 수신받아 사용자 에이전트를 할당하는 단계;

(b) 상기 사용자 에이전트가 사용자의 상황정보를 식별하여 사용자의 동적 프라이버시 정책파일을 생성하고, 사용자의 동적 프라이버시 정책파일을 서비스 에이전트에게 전송하는 단계;

(c) 상기 서비스 에이전트가 수신된 사용자의 프라이버시 정책을 고려하여 서비스 공급자의 P3P(Platform for Privacy Preferences)제안서를 작성하고 사용자 에이전트에게 URI주소를 전송하는 단계; 및

(d) 상기 사용자 에이전트가 수신된 URI주소를 방문하여 소정의 협상알고리즘에 의한 서비스 공급자의 P3P제안서를 평가하고 이후의 행동을 결정하는 단계; 를 포함하여 이루어지는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 2

제1항에 있어서,

(e) 상기 (d)단계에서 서비스 공급자의 P3P제안서가 사용자의 프라이버시 정책에 부합한다면 사용자 에이전트는 서비스 에이전트에 동의한 후 해당 서비스에 대한 사용자의 제안서ID를 서비스 에이전트로 전송하는 단계; 를 더 포함하여 이루어지는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 3

제1항에 있어서, 상기 (d)단계의 협상알고리즘은

개인정보를 다른 편으로 전달하는 과정에서 발생하는 서비스 결핍비용과 감시비용 사이의 트레이드 오프에 의해 계산되어진 효용을 이용한 경제기반모델인 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 4

제1항에 있어서, 상기 (d)단계의 협상알고리즘은

(d-1) 사용자 에이전트가 서비스 공급자의 P3P제안서를 가져오는 단계;

(d-2) 상기 사용자 에이전트가 서비스 공급자의 P3P제안서와 사용자의 프라이버시 정책 룰에 근거하여 전체비용을 최소화하는 사용자 정책의 최적집합을 도출하고 최적의 감시비용을 계산 후 협상 에이전트(또는 협상자)에게 제공하고, 상기 서비스 에이전트가 서비스 공급자의 프라이버시 정책 룰에 근거하여 전체비용을 최소화하는 서비스 공급자 정책의 최적집합을 도출하고 최적의 감시비용을 계산 후 협상 에이전트(또는 협상자)에게 제공하는 단계; 및

(d-3) 상기 사용자 정책의 최적집합을 이용하여 협상 에이전트(또는 협상자)가 사용자의 프라이버시 정책과 서비스 공급자의 프라이버시 정책을 비교하여 사용자 에이전트에게 서비스 공급자의 최적정책을 수락할 것인지를 묻는 단계; 를 더 포함하여 이루어지는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 5

제4항에 있어서, 상기 (d-3)단계는

(d-4) 상기 (d-3)단계에서 사용자 에이전트가 수락하면 상기 서비스 에이전트는 사용자에게 편재적인 서비스를 제공하고, 거절하면 정책완화의 과정을 수행한 후 다시 협상하는 단계; 를 더 포함하여 이루어지는 것을 특징으

로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 6

제5항에 있어서, 상기 (d-4)단계에서 사용자 에이전트의 정책완화는

(d-41) 사용자 에이전트는 사용자의 신용을 증명하기 위한 프라이버시 정책 외의 프로파일을 보내고, 서비스 에이전트는 사용자를 위한 더 높은 조건의 카테고리 값을 요청하는 단계;

(d-42) 상기 수신된 정보를 이용하여 사용자의 프라이버시 정책 룰에 근거하여 사용자의 프라이버시 정책을 최적화하는 단계; 및

(d-43) 상기 사용자 에이전트가 상기 (d-42)단계에서 수행하는 작업을 사용자의 휴대수단으로 전송하여 사용자에게 알리는 단계; 를 더 포함하여 이루어지는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 7

제5항에 있어서, 상기 (d-4)단계에서 서비스 에이전트의 정책완화는

(d-411) 서비스 에이전트는 서비스 공급자의 신용을 증명하기 위한 프라이버시 정책 외의 프로파일을 보내고, 사용자 에이전트는 서비스 공급자를 위한 더 높은 조건의 카테고리 값을 요청하는 단계;

(d-422) 상기 수신된 정보를 이용하여 서비스 공급자의 프라이버시 정책 룰에 근거하여 서비스 공급자의 프라이버시 정책을 최적화하는 단계; 및

(d-433) 서비스 에이전트는 상기 (d-422)단계의 결과를 서비스 공급자의 서비스 수단으로 전송하여 서비스 공급자에게 알리는 단계; 를 더 포함하여 이루어지는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 8

제6항 또는 제7항에 있어서, 상기 프로파일은 사용자의 현재 위치, 외부 상황 또는 내부 상황 중 어느 하나 이상을 포함하여 이루어지는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 9

제4항에 있어서, 상기 사용자의 프라이버시 정책 룰에 근거하여 전체 비용을 최소화하는 사용자 정책의 최적집합은

$\{c_1^*, c_2^*, \ldots c_i^*, \ldots c_N^* \mid p_1, \ldots, p_N, o_1, \ldots, o_N, r_1, \ldots, r_N\}$ 로 표시되고,

전체비용은 $TC_U = Max\{f_1(c_1^* \mid p_1, o_1, r_1), f_2(c_2^* \mid p_2, o_2, r_2), \ldots, f_N(c_N^* \mid p_N, o_N, r_N)\}$

으로 표시되는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 10

제4항에 있어서, 상기 서비스 공급자의 프라이버시 정책 룰에 근거하여 전체 비용을 최소화하는 서비스 공급자 정책의 최적집합은

$\{p_1^*, \ldots, p_j^*, \ldots, p_N^*, o_1^*, \ldots, o_j^*, \ldots, o_N^*, r_1^*, \ldots, r_j^*, \ldots, r_N^* \mid c_1, \ldots, c_i, \ldots, c_N\}$ 로 표시되고,

전체비용은 $TC_S = Max\{g_1(p_1^*, o_1^*, r_1^* \mid c_1), \ldots, g_j(p_j^*, o_j^*, r_j^* \mid c_j), \ldots, g_N(p_N^*, o_N^*, r_N^* \mid c_N)\}$

으로 표시되는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 11

제4항에 있어서, 상기 사용자의 프라이버시 정책 룰 또는 서비스 공급자의 프라이버시 정책 룰에 근거한 최적집합을 이용하여 아래 식에 의한

$$c_i^* = \frac{log\frac{\alpha_2\beta_2}{\alpha_1\beta_1}}{\beta_1-\beta_2}, \text{ if } \beta_1 \neq \beta_2$$

최적의 감시비용을 계산하는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 12

제1항에 있어서, 상기 서비스 공급자의 P3P제안서는

$$P = \{(c_1, p_1, o_1, r_1), \ldots, (c_i, p_i, o_i, r_i), \ldots, (c_N, p_N, o_N, r_N)\}$$

으로 작성되는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

청구항 13

제1항에 있어서, 상기 P3P제안서는

프라이버시 정책 수집을 원하는 웹사이트를 위한 데이터 표준 스키마, 사용성, 수용성, 데이터 카테고리, 또 다른 프라이버시 기술서들의 표준 집합, 프라이버시 정책 표현을 위한 XML형식, 웹페이지, 사이트, 쿠키들의 프라이버시 정책 조합을 위한 수단 또는 P3P(Platform for Privacy Preferences)정책을 http프로토콜로 전송하기 위한 메커니즘 중 어느 하나 이상을 포함하여 구성되는 것을 특징으로 하는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법에 관한 것이다.

<2> 더욱 상세하게는 유비쿼터스 환경하에서 동적이고 유연한 방법으로 개인화된 프라이버시-인지 서비스를 위해 동적으로 적응하는 피쓰리피(P3P)기반의 정책(P4P), 프라이버시를 관리하기 위한 피쓰리피(P3P)기반의 협상메커니즘 및 다중 에이전트를 이용한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법에 관한 것이다.

배 경 기 술

<3> 최근 프라이버시 보호는 하드웨어, 네트워크 프로토콜, 상호작용, 애플리케이션, 연산방법과 함께 유비쿼터스 혹은 편재적 컴퓨팅의 주요 이슈 중 하나이다. 2002년 미국의 인터넷 프라이버시 관련 연구에서는 사용자의 59%가 프라이버시 정책을 읽고 있으며, 동시에 91%가 post 프라이버시 정책을 중요하게 생각한다고 응답한 것으로 나타났다. 전자사회에서의 프라이버시에 대한 관심은 현재 매우 큰 사회적인 이슈이다. 편재적 혹은 유비쿼터스 서비스 및 애플리케이션에서 사용자의 민감한 정보는 다양한 서비스 공급자에 의해 수집되는데, 이는 프라이버시를 위협할 수 있다. Lahloh 외 여러 연구자들은 서비스 사용자에 의해서 작성된 프라이버시 양식에 대한 우려를 표현하고 있으며, 편재적 컴퓨팅 환경에서 보이지 않는 컴퓨터에 의해 구성된 강화된 프라이버시 지도의 중

요성을 강조하고 있으며, 프라이버시 이슈들은 편재적 컴퓨팅 환경에서 작동하는 상황인지 서비스 내에서 더욱 강조된다.

<4> 유비쿼터스 모바일 컴퓨팅의 잠재성을 충분히 입증하기 위해 애플리케이션 디자이너는 사용자의 개인적인 프라이버시 정책을 반드시 수립해야 하며, 유비쿼터스 혹은 편재적 컴퓨팅 환경에서 사용자의 프라이버시를 보호하기 위한 방법으로 타 문헌에서는 Privacy Profile Negotiation Protocol(PPNP)이 제안되었는데, 일본 Keio 대학의 Tohda Lab에서 개발한 PPNP는 사용자의 프라이버시 프로파일이 신뢰된 서비스를 제외하고는 전달되는 것을 금지하고 있다. 이와 유사하게 ETH Zurich는 P3P(Platform for Privacy Preferences)를 적용한 프라이버시-인지 시스템(pawS)을 개발 중이다.

<5> 일반적으로 사용자는 서비스 등록시 개인적인 정보를 제출해야 하는데, 이는 사용자의 프라이버시 정책과 직결된다. 사용자들은 자신의 프라이버시 정책에 따라 마지못해 혹은 신중하게 그들의 프라이버시를 제공하거나, 아예 서비스받는 것 자체를 포기하기도 한다. 반면 서비스 공급자는 고객 세분화 등에 활용할 목적으로 가능한 많은 개인적인 정보를 수집하고자 한다.

<6> 도 4는 본 발명의 일 실시예에 의한 종래 프라이버시 정책의 불일치를 나타내는 참조도면이다. 도 4에 도시된 바와 같이 서비스 공급자와 사용자 간의 활용 가능한 정보에 대한 생각 불일치를 보여준다. 이상적으로는 서비스 공급자의 지나친 개인적인 정보 요청을 최소화하고 사용자의 서비스 공급자에게는 가치가 없는 또 다른 개인적인 정보 제출을 허가함으로써, 허용된 개인적인 정보를 증가시키는 동시에 사용자의 불안감을 감소시키는 것이 가능하다.

<7> 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 있으며, 프라이버시 정책을 완성되고 표준화된 방법으로 기술하기 위해 정책 기술 언어인 EPAL과 P3P(Platform for Privacy Preferences)가 사용되어 왔다.

<8> 이 중 상기 프라이버시 정책 표준규격인 P3P(Platform for Privacy Preferences)는 P3P정책에 따라 XML 형태로 표현되며, 프라이버시 정책에 의한 웹사이트에서의 데이터 수집 및 데이터 사용을 위한 방법을 제공하며, 상기 P3P에서의 정책 기술은 P3P기반의 프라이버시 정책에 대한 신텍스(Syntax)와 시멘틱스(Semantics)로 정의되어 있다. 그 기술서는 기계가 읽을 수 있는 형식으로 되어 있어 사용자 에이전트는 P3P기술서 이해할 수 있다. 또한 이를 통해 사용자를 대신하여 자동적으로 적절한 의사결정을 수행함으로써 사용자는 그들이 방문하는 모든 사이트의 프라이버시 정책을 일일이 읽을 필요가 없어진다.

<9> 이러한 P3P기술서의 도움으로 웹 사용자는 그들이 웹 사이트를 방문했을 때 어떤 데이터가 전송될 것인지에 대해 보다 쉽게 이해할 수 있다. 이를 위해 P3P기술서는 다음을 포함한다.

<10> - "P3P기반 데이터 스키마" 알려진 프라이버시 수집을 원하는 웹사이트를 위한 데이터 표준 스키마

<11> - 사용성, 수용성, 데이터 카테고리, 또 다른 프라이버시 기술서들의 표준 집합

<12> - 프라이버시 정책 표현을 위한 XML 형식

<13> - 웹 페이지, 사이트, 쿠키들의 프라이버시 정책 조합을 위한 수단

<14> - P3P(Platform for Privacy Preferences) 정책을 http로 전송하기 위한 메커니즘 등

<15> 하지만, P3P를 포함한 현재 기술 수준에서 프라이버시 보호와 서비스 질 간의 균형을 위한 여러 노력들이 실제 거의 효과가 없는 것으로 나타나고 있다.

<16> 또한, 최근 수년간 많은 연구팀들은 P3P기반 프라이버시-인지 유비쿼터스 컴퓨팅 시스템 및 서비스에 집중하고 있으며, Ackeman는 데이터 요청 및 그 결과라는 관점에서 사용자에게 정보를 전달하는 기술적 메커니즘을 제안했으며, 프라이버시 관리 모듈은 프라이버시-인지 시스템에 미들웨어로 내장될 수 있다. PeCAN(The Personal Context Agent Networking) 지식 아키텍처는 고객 및 웹 사이트 양 측면에서의 아키텍처적 데이터 구성요소 및 서비스로 이루어져 있으며, 이는 사용자에게 전자상거래 내에서의 온라인 프라이버시 및 신뢰에 관해 알려주는 역할을 한다. Langheinrich는 P3P확장 프레임워크를 사용하여 프라이버시-인지 시스템에서의 데이터 수집 위치 기반 보급 활동에 대한 메커니즘을 구현했다.

<17> 하지만, P3P기반의 프라이버시-인지 편재적 서비스를 확장하기 위해서는 상당한 수의 센서, 데이터 변환, 다양한 프라이버시 정책을 가진 사용자들을 고려할 경우에만 P3P적용이 가능해질 것으로 보여지며, 편재적 서비스

(Pervasive service)에서 프라이버시 정책은 사용자의 주변 상황과 크게 관련되어 있다. 그러므로 상황에 대한 고려가 없는 획일적인 프라이버시 정책은 편재적 서비스 모델에서 제대로 작동되기 어려운 문제점이 있었으며,

<18> 상기 P3P(Platform for Privacy Preferences)의 유용성에도 불구하고 여전히 시스템의 차이에 따라 프라이버시 정책을 협상하거나, 어떻게 그들의 목적을 달성할 수 있는지를 사용자에게 조언하는 메커니즘은 거의 없었다. Cranor과 Resnick의 웹 사이트와 사용자 에이전트 사이에서 협상 전략에 의한 협상을 적용한 연구에 의하면 P3P에서 상황인지는 반드시 추가적으로 고려되어야만 한다. 사용자는 그들의 프라이버시 정책이 각각 다름에도 불구하고, 언제나 동일한 전체 프라이버시 정책에 의해 처리된다. 이 같은 방식은 충성된 사용자들을 실망시키거나 그들의 충성도를 약화시키는 계기가 될 수 있다.

<19> 한편, 편재적 컴퓨팅 서비스에서 개인 정보 흐름은 경제 모델로 설명되어 왔다. Acquisti는 프라이버시 관리 및 거래성사에 대한 기대수익이라는 관점에서의 경제 모델을 설명했다. Jiang외 여러 연구자들은 유비쿼터스 컴퓨팅 내 정보 흐름을 분석하기 위해 경제 기반의 접근을 사용했다. Price와 Adam은 유비쿼터스 컴퓨팅 환경에서 공개된 개인적인 데이터에 대한 사용자의 유동적 관리를 가능하게 하는 프레임워크를 기술했다.

<20> 하지만 지금까지의 연구는 편재적 컴퓨팅 환경에서 서비스 공급자와 사용자 간의 프라이버시에 대한 정책의 차이를 해결하는 방법에 대해서는 좀처럼 언급하고 있지 않았다. 실제로 현재 P3P는 보다 좋고 완벽한 상세화 및 사용을 위해 계속 논의되고 있는 중이다. 그러므로 편재적 컴퓨팅 환경에서 동적인 사용자를 위한 프라이버시-인지 서비스는 보다 정교하게 손질된 P3P 기술서가 요구되고 있는 실정이다.

발명의 내용

해결 하고자하는 과제

<21> 본 발명은 상술한 바와 같은 문제점을 해결하기 위하여 안출된 것으로, 사용자의 개인적인 특성 및 서비스 시점의 사용자 주변 상황을 자동적이고 동적이며 유연한 방법으로 반영하는 개인화된 프라이버시 정책을 제공하여 신중하고 안정된 편재적 컴퓨팅(Pervasive computing)의 서비스 실현을 구현할 수 있도록 하는 데 그 목적이 있고,

<22> 다른 목적으로는, 사용자 데이터와 서비스간의 개인적인 정보 교환 과정에서 요구되는 협상 메커니즘을 제공하여 사용자 및 서비스 공급자의 프라이버시 정책을 고려하고, 상황에 따라 변화하는 동적인 사용자의 프라이버시 정책을 서비스 공급자의 프라이버시 정책에 동적으로 디자인할 수 있도록 하며, 서비스 공급자의 프라이버시 정책을 사용자 개개인에 맞춰 개인화될 수 있도록 하는 데 그 목적이 있고,

<23> 또 다른 목적으로는, 유비쿼터스 환경하에서 동적이고 유연한 방법으로 개인정보를 관리하기 위한 피쓰리피(P3P)기반의 프라이버시(P4P)와 다중 에이전트를 이용한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법을 제공하는 데 그 목적이 있다.

과제 해결수단

<24> 상술한 바와 같은 목적은, 유비쿼터스 환경에서 사용자의 휴대수단을 감지하는 적어도 하나 이상의 상황정보감지수단, 상황정보인식수단, 서비스수단 및 적어도 하나 이상의 사용자 에이전트, 서비스 에이전트 또는 협상 에이전트(또는 협상자)를 포함하여 상황인식 서비스를 제공하는 상황서버를 포함하는 프라이버시 정책 방법에 있어서, (a) 상기 상황정보감지수단으로부터 사용자의 상황정보를 수신받아 사용자 에이전트를 할당하는 단계; (b) 상기 사용자 에이전트가 사용자의 상황정보를 식별하여 사용자의 동적 프라이버시 정책파일을 생성하고, 사용자의 동적 프라이버시 정책파일을 서비스 에이전트에게 전송하는 단계; (c) 상기 서비스 에이전트가 수신된 사용자의 프라이버시 정책을 고려하여 서비스 공급자의 P3P(Platform for Privacy Preferences)제안서를 작성하고 사용자 에이전트에게 URI주소를 전송하는 단계; 및 (d) 상기 사용자 에이전트가 수신된 URI주소를 방문하여 소정의 협상알고리즘에 의한 서비스 공급자의 P3P제안서를 평가하고 이후의 행동을 결정하는 단계; 를 포함하여 이루어지는 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반(P4P)의 프라이버시 정책 협상방법을 제공함으로써 달성된다.

효 과

<25> 상술한 바와 같이 본 발명인 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반(P4P)의 프라이버시 정책 협상방법은, 에이전트를 이용하여 사용자의 프라이버시 정책과 서비스 공급자의 프라이버시 정책을 협상알

고리즘을 이용하여 서로 상호조정함으로써, 사용자들이 별다른 염려없이 다양한 서비스를 이용할 수 있는 효과가 있고,

<26> 다른 효과로는, 경제기반모델의 협상알고리즘을 사용함으로써, 서비스 공급자가 요구하는 정보와 사용자가 공유를 승인한 개인정보 사이의 격차를 감소시켜 서비스 매치의 가능성을 증가시킬 수 있고, 특정 공간 내에서 동적인 편재적 서비스를 운영할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<27> 이하, 도면을 참조하여 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법을 더욱 구체적으로 설명한다.

<28> 먼저, 본 발명의 피포피(P4P)는 편재적인 P3P(Platform for Privacy Preferences)기술로 사용자뿐만 아니라 서비스 공급자 측면의 프라이버시 정책과, 사용자의 프라이버시 정책이 상황에 따라 변화하므로 서비스 공급자의 프라이버시 정책도 동적으로 디자인되는 것과, 서비스 공급자의 프라이버시 정책이 사용자에게 맞춰지는 것을 특징으로 한다.

<29> 도 1은 본 발명의 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상시스템의 전체적인 구성을 나타내는 도면이다. 도 1을 참조하여 더욱 구체적으로 설명하면,

<30> 본 발명의 시스템은 휴대수단(100), 상황정보감지수단(200), 무선망(300), 상황정보인식수단(400), 상황서버(500) 및 서비스 수단(600) 등을 포함하여 구성된다.

<31> 상기 휴대수단(100)은 PCS, 셀룰라폰, PDA 등의 휴대통신 단말기를 포함하며, 또는 사용자가 휴대하기 쉽도록 만년필 형태 등으로 제작된 무선통신과 메모리가 포함된 통신단말기로써, 상기 상황정보감지수단(200), 상황서버(500) 또는 서비스 수단(600)과의 무선통신을 수행하며, 사용자로부터 사용자의 프라이버시 정책, 프로파일 등을 저장하고 관리하며 상기 상황서버(600)로 사용자의 프라이버시 정책, 프로파일 등을 전송하는 기능을 수행한다.

<32> 상기 상황정보감지수단(200)은 GPS, RFID, EKAW, UWB, CELL 등의 유비쿼터스 센서로 구성되어 상기 휴대수단의 고유식별번호와 주변 상황정보를 감지하여 상황정보인식수단(400)으로 전송하는 기능을 수행한다.

<33> 상기 무선망(300)는 GPS, RFID, EKAW, UWB, CELL 등의 유비쿼터스 센서들로 구성되어 무선통신 기능을 제공하는 무선통신망으로써, 근거리 및 장거리 무선통신망의 기반체계를 사용하며 본 발명의 목적에 부합되지 않는 구체적인 기술적 구성의 설명은 생략한다.

<34> 상기 상황정보인식수단(400)은 특정지역에 위치하는 서버 또는 단말기로써, 특정지역의 서비스수단을 관리하는 서비스 에이전트의 정보, 사용자 에이전트의 정보 또는 서비스 에이전트와 사용자 에이전트의 프라이버시 정책 협상을 유도하는 특정지역 협상 에이전트(또는 협상자)의 정보를 저장하고 관리하며, 상기 상황정보감지수단(200)으로부터 수집된 휴대수단의 고유식별번호와 상황정보를 상황서버(500)로 전송할 뿐만 아니라 특정지역에 해당하는 사용자 에이전트의 정보, 서비스 에이전트의 정보 또는 협상 에이전트(또는 협상자)의 정보를 상황서버(500)로 전송하는 기능을 수행한다.

<35> 상기 상황서버(500)는 다수의 상황정보감지수단(200), 상황정보인식수단(400), 서비스 수단(600)의 고유식별번호와 위치정보를 등록하여 데이타베이스에 저장하며, 또한, 상기 휴대수단별로 할당되는 사용자 에이전트, 서비스 수단별로 할당되는 서비스 에이전트 또는 사용자 에이전트와 서비스 에이전트와의 프라이버시 정책 협상을 유도하는 특정지역의 협상 에이전트(또는 협상자)를 데이터베이스에 저장하고 관리한다.

<36> 특히, 상기 상황정보인식수단(400)으로부터 수신된 휴대수단의 고유식별번호와 상황정보 및, 사용자 에이전트의 정보, 서비스 에이전트의 정보 또는 협상 에이전트(또는 협상자)의 정보를 이용하여 특정지역의 서비스 에이전트, 사용자 에이전트 또는 협상 에이전트(또는 협상자)를 할당하고 관리하며, 상기 휴대수단에 할당된 사용자 에이전트로부터 수신받은 사용자의 프라이버시 정책과 상기 서비스 수단의 서비스 에이전트로부터 수신받은 서비스 공급자의 프라이버시 정책을 협상 에이전트(또는 협상자)에게 제공하고, 협상 에이전트(또는 협상자)가 소정의 협상알고리즘을 이용하여 비교한 후, 서비스 공급자의 프라이버시 정책 중 부합된 사용자의 프라이버시 정책에 대해서 사용자 에이전트에게 제공하게 되고, 사용자가 해당 서비스 수단(600)에 접근하게 되면 상기 부합된 서비스 수단(600)으로부터 최적의 편재적 서비스를 제공하도록 유도하는 기능을 수행한다.

<37> 상기 상황서버(500)는 경제기반모델에 해당하는 상기 소정의 협상알고리즘으로 $\{c_1^*, c_2^*, \ldots c_i^*, \ldots c_N^* \mid p_1, \ldots, p_N, o_1, \ldots, o_N, r_1, \ldots, r_N\}$ 식(1)로 표시되는 사용자 정책의 최적집합과,

<38> $TC_U = Max\{f_1(c_1^* \mid p_1, o_1, r_1), f_2(c_2^* \mid p_2, o_2, r_2), \ldots, f_N(c_N^* \mid p_N, o_N, r_N)\}$ (식2)으로 표시되는 사용자 정책의 전체비용, 및

<39> $\{p_1^*, \ldots, p_j^*, \ldots, p_N^*, o_1^*, \ldots, o_j^*, \ldots, o_N^*, r_1^*, \ldots, r_j^*, \ldots, r_N^* \mid c_1, \ldots, c_i, \ldots, c_N\}$ (식3)로 표시되는 서비스 공급자의 최적 집합과,

<40> $TC_S = Max\{g_1(p_1^*, o_1^*, r_1^* \mid c_1), \ldots, g_j(p_j^*, o_j^*, r_j^* \mid c_j), \ldots, g_N(p_N^*, o_N^*, r_N^* \mid c_N)\}$ (식4)으로 표시되는 서비스 공급자의 전체비용을 이용하는 것을 특징으로 하고 있으며,

<41> $$c_i^* = \frac{\log \frac{\alpha_2 \beta_2}{\alpha_1 \beta_1}}{\beta_1 - \beta_2}, \text{ if } \beta_1 \neq \beta_2$$ (식5)로 계산되어지는 최적의 감시수준(또는 감시비용)을 이용하는 것을 특징으로 하고 있다.

<42> 상기 협상알고리즘은 상호적인 프라이버시 정책, 상황인지적 정책 디자인, 개인화를 더 포함하는 것을 특징으로 한다.

<43> 상기 사용자 에이전트, 서비스 에이전트 또는 협상 에이전트(또는 협상자)는 사용자의 정책 하에서 사용자, 서비스 공급자를 대신하여 사용자와 서비스와의 상호작용을 조정하는 프로그램으로 특히 사용자 에이전트는 e-지갑 혹은 사용자 데이터 관리 도구들로 구축될 수 있다.

<44> 상기 서비스 수단(600)은 유무선 인터넷을 통해 접속 가능한 웹서버, 웹사이트뿐만 아니라 유비쿼터스 환경하에 접속 가능한 TV, 오디오, 비디오, 세탁기, 게임, 조명장치, 디스플레이장치, 음향장치, 에어컨, 보일러 등을 포함하는 장치로써 다양한 형태의 서비스를 제공하며, 상기 상황서버(500)로부터 협상 유도된 서비스에 따라 해당 사용자가 접근하게 되면 서비스 에이전트가 사용자 에이전트와의 상호작용을 통하여 다양한 편재적 서비스를 제공하는 기능을 수행한다.

<45> 이하, 도면을 참조하여 상술한 바와 같은 시스템을 이용하여 본 발명인 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법을 더욱 구체적으로 설명한다.

<46> 도 2는 본 발명의 바람직한 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법을 나타내는 순서도이다. 도 3은 본 발명의 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상알고리즘을 나타내는 순서도이다. 도 5는 본 발명의 일 실시예에 의한 사용자 에이전트, 서비스 에이전트, 협상 에이전트(또는 협상자)간의 유기적인 결합관계를 나타내는 참조도면이다. 도 6은 본 발명의 일 실시예에 따른 서비스 공급자에게 상황정보를 제공하기 위한 상황정보의 카테고리와 속성을 나타내는 도면이다. 도 7은 본 발명의 일 실시예에 따른 서비스 공급자의 프라이버시 정책 목적 및 카테고리를 나타내는 도면이다. 도 8은 본 발명의 일 실시예에 따른 도 7을 적용한 웹페이지 소스코드를 나타내는 도면이다. 도 9는 본 발명의 일 실시예에 따른 경제기반모델을 협상알고리즘으로 채택하여 서비스 결핍비용과 감시비용 사이의 트레이드 오프에 의해 계산된 참조도면이다. 도 10은 본 발명의 일 실시예에 따른 사용자의 동적 프라이버시 정책파일을 생성하는 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다. 도 2 내지 도 10을 참조하여 더욱 구체적으로 설명하면,

<47> 먼저, P4P-인지 편재적 컴퓨팅 서비스를 위해서는 도 5에 도시된 바와 같은 전체적인 협상 프레임워크가 필요하며, 최적의 서비스 사용량을 확보하기 위해서는 다음과 같은 요구 조건을 만족시켜야 한다.

<48> 즉, 사용자의 특성에 따른 동적인 P3P(Platform for Privacy Preferences) 정책 변화가 가능해야 하며, 프라이버시 정책에 대한 사용자 및 서비스 공급자 모두의 상호 동의가 있어야 하고, 사용자의 현재 상황에 따른 동적인 P3P정책 변화가 가능해야 한다는 것이다.

<49> 특히, P3P(Platform for Privacy Preferences)기술서의 정책 레퍼런스는 P3P정책이 잘 알려진 곳에 위치하는 것을 허용하므로 본 발명에서는 서비스 에이전트 및 사용자 에이전트가 서비스 실행을 위한 협상시 쉽게 액세스할 수 있도록 프라이버시 정책 정보는 온톨로지 파일로 저장되는 것이 바람직하다.

<50> 또한, 편재적 컴퓨팅 서비스 환경에서 동적 사용자를 위한 사용자 인터페이스는 웹 브라우저만으로 국한되지 않으며, 멀티모드, 상호작용, 증강현실, 행동인지와 같은 진보적 기술의 반영이 가능한 인터페이스도 포함되는 것이 바람직하며, 이러한 이유로 본 발명의 일 실시예에서는 P4P 협상 상호작용이 포함된 서비스를 위한 편재적 컴퓨팅 서비스 존을 그 인터페이스로 설정했으며, 이 존 내에서는 여러 유비쿼터스 센서들을 통해 사용자의 현재 상황정보가 탐지되며, 그 상황정보는 미리 서비스되고 있던 유비쿼터스 센서 네트워크를 통해 사용자 에이전트로 전달되게 된다.

<51> 유비쿼터스 환경하에서 사용자가 휴대수단을 휴대한 상태에서 서비스 존에 들어서게 되면 상황정보감지수단(200)은 휴대수단과의 무선통신을 통하여 휴대수단의 고유식별번호, 위치정보 또는 주변 상황정보 등을 감지하여 상기 상황정보인식수단(400)으로 전송하게 된다. 상기 상황정보인식수단(400)은 기 저장된 특정지역의 사용자 에이전트, 서비스 에이전트 또는 협상 에이전트(또는 협상자)의 정보와 함께 상기 휴대수단의 고유식별번호, 위치정보 또는 주변 상황정보 등을 상황서버(500)로 전송하게 된다.

<52> 상기 상황서버(500)는 수신된 사용자 에이전트의 정보, 서비스 에이전트의 정보 또는 협상 에이전트(또는 협상자)의 정보, 휴대수단의 고유식별번호, 위치정보 또는 주변 상황정보 등을 이용하여 휴대수단의 사용자 에이전트를 할당하게 되고, 또한 휴대수단 주변의 서비스 수단(600)의 위치를 확인하여 서비스 에이전트를 할당하게 되고, 또한 휴대수단의 주변 특정지역을 담당하는 협상 에이전트(또는 협상자)를 할당하게 된다(S302).

<53> 상기 사용자 에이전트는 사용자가 서비스 존으로 들어설 때 사용자의 입장에서 서비스를 선택하기 위해 서비스 리스트를 액세스하고, 휴대수단의 주변 상황정보를 식별한 후 사용자의 동적 프라이버시 정책파일을 생성하게 되는데(S304),

<54> 본 발명에서 사용되는 P4P(Pervasive Platform for Privacy Preferences)는 전통적인 P3P(Platform for Privacy Preferences)의 확장으로 상황 관련 프라이버시 관리를 위해 그 기술서를 추가적으로 고려한 것으로, P3P기술서의 대표적인 데이터 요소는 트리 구조로 적용되며, 예를 들어, 자동차 모델이라는 데이터 요소는 자동차라는 데이터 요소의 자식 노드가 된다.

<55> 종래 P3P기술서는 상황적 데이터를 고려하지 않고 있으나, 본 발명에서는 같은 방법으로 표기되어 있는 시스템의 데이터 요소를 동적으로 변화시키기 위해 P3P기술서를 확장할 수 있으며, 이러한 데이터 요소의 동적을 변화를 표현하기 위해 다음과 같은 편재적 플랫폼이 제공된다.

<56> P3P *data schema*.**CONTEXT**.*context field*.

<57> 예를 들어, 공적·사적인 활동에서 GPS 위치 데이터의 식별이 필요한 경우 P4P의 데이터 요소에서는 이를 다음과 같은 편재적 플랫폼으로 표현된다.

<58> user.current.GPS_position. **Activity**.public and

<59> user.current.GPS_position. **Activity**.private.

<60> 상술한 바와 같은 편재적 플랫폼을 통해 상기 사용자 에이전트는 동적 프라이버시 정책파일을 생성한 후 서비스 에이전트에게 전송하게 되는데(S306), 이때 사용자의 상황 데이터 요소도 함께 전송하게 되며, 서비스 공급자의 서비스 에이전트에게 상황 데이터 요소를 전달하기 위해서는 개인 상황 온톨로지나 사용자 에이전트로부터 획득된 상황정보가 필요하며, P4P에 적용된 상황정보 모델의 카테고리 및 속성은 도 6에 도시된 바와 같다.

<61> 상기 서비스 에이전트는 사용자 에이전트로부터 수신한 사용자의 동적 프라이버시 정책파일을 이용하여 서비스 공급자의 P3P(Platform for Privacy Preferences)제안서를 작성하고 사용자 에이전트에게 URI주소를 전송하게 된다(S308). 또한, 협상 에이전트(또는 협상자)에게도 전송하게 된다.

<62> 이때, 상기 서비스 공급자의 프라이버시 정책은 서비스 에이전트로 하여금 사용자 에이전트와 어떤 정보를 제공할 것인가의 합의에 도달하기 위한 협상을 진행할 수 있게 하므로 사용자의 프라이버시 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 아니

든 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.

<63> 즉 서비스 공급자는 회사 프로파일, 상품 정보, 서비스 프로파일, 직원 개인 데이터 등과 같은 서비스에 내장된 정보를 보호하기 위한 고유한 프라이버시 정책을 명확히 해야한다. 이러한 정보들은 고객들의 프라이버시 정책과 서비스 공급자의 프라이버시 정책간의 약간의 차이를 가져온다. 결과적으로 서비스 공급자의 프라이버시 정책 목적 및 카테고리는 도 7에 도시된 바와 같이 나타내게 된다.

<64> 예를 들어, 서비스 공급자의 웹페이지 소스코드는 상품 이미지 파일을 포함하며 P4P에서는 도 8에 도시된 바와 같이 기술되게 되는 것이다.

<65> 상기 사용자 에이전트는 수신된 URI주소를 방문하여 서비스 에이전트가 작성한 P3P제안서를 가져온 후, 소정의 협상알고리즘에 의해 비교판단한 후 거절, 수락, 즉각적 응대, 맞제안 등 이후의 행동을 결정하게 되는 데(S310),

<66> 도 3을 참조하여 협상알고리즘을 구체적으로 설명하면,

<67> 프라이버시에 대한 우려는 액세스를 통해 정보를 얻고자 하는 측과 개인적인 정보를 숨기고 싶어하는 측 간의 긴장이 있을 때 발생하게 되는데, 본 발명에서는 사용자 프라이버시에 대한 경제 기반 모델을 협상 알고리즘으로 채택하였다.

<68> 효용은 기본적으로 누군가의 개인적 정보를 다른 편으로 전달하는 과정에서 발생하는 서비스 결핍 비용과 감시 비용 사이의 트레이드 오프에 의해 계산되며, 도 9에 도시된 바와 같이 표현할 수 있다. 이것은 프라이버시 정책과 실제 행동 주체가 트레이드 오프 관계를 가지며 이는 사용자를 복잡하게 하는 전자상거래 상황에서 종종 관찰된다.

<69> 도 9에 도시된 바와 같이 데이터 요소는 i, 감시 비용은 $y=\alpha_{2,i}e^{\beta_{2,i}c_i}$, 서비스 결핍은 $y=\alpha_{1,i}e^{-\beta_{1,i}c_i}$, 감시 수준 정도는 c_i이다.

<70> 먼저, 사용자 에이전트가 URI주소를 방문하여 서비스 공급자의 P3P(Platform for Privacy Preferences)정책을 가져오게 되면(S402), 상기 P3P정책은 아래와 같이 P로 표현되게 된다.

<71> $$P=\{(c_1,p_1,o_1,r_1),\ldots,(c_i,p_i,o_i,r_i),\ldots,(c_N,p_N,o_N,r_N)\}$$

<72> 서비스 공급자의 P3P정책에 포함된 데이터 요소의 개수가 N개 일 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.

<73> 상기 사용자 에이전트 사용자의 프라이버시 정책 룰에 의해 전체비용을 최소화하게 되는데 사용자의 전체비용은 다음과 같이 표현된다.

<74> $$TC_U=Max\{f_1(c_1^*\mid p_1,o_1,r_1),f_2(c_2^*\mid p_2,o_2,r_2),\ldots,f_N(c_N^*\mid p_N,o_N,r_N)\}$$

<75> c_i는 i번째 카테고리를 의미하며, 서비스 결핍 비용이 $y=\alpha_{1,i}e^{-\beta_{1,i}c_i}$ 이고, 감시 비용이 $y=\alpha_{2,i}e^{\beta_{2,i}c_i}$ 일 때 $f_i(c_i^*\mid p_i,o_i,r_i)=\alpha_{1,i}e^{-\beta_{1,i}c_i}+\alpha_{2,i}e^{\beta_{2,i}c_i}$ 으로 표현되며, 여기에서 i번째 데이터 요소의 최적의 감시 수준은 아래 계산식1에 의해 계산된다.

$$c_i^* = \frac{\log \frac{\alpha_2 \beta_2}{\alpha_1 \beta_1}}{\beta_1 - \beta_2}, \text{ if } \beta_1 \neq \beta_2$$

<76> (계산식1)

<77> 즉, $TC_U = f_M(c_M^* \mid p_M, o_M, r_M), 1 \le M \le N$ 임을 가정했을 때 계산결과, 사용자 정책의 최적집합은 $\{c_1^*, c_2^*, ...c_i^*, ...c_N^* \mid p_1, ..., p_N, o_1, ..., o_N, r_1, ..., r_N\}$ 으로 계산되고, 계산된 결과는 협상 에이전트(또는 협상자)에게 전달되게 된다(S404).

<78> 한편, i 카테고리의 서비스 에이전트 집합은 $c_i = c_i^*$ 이다. 이 때 서비스 공급자의 전체 비용은 아래와 같이 표현된다.

$$TC_S = Max\{g_1(p_1^*, o_1^*, r_1^* \mid c_1), ..., g_j(p_j^*, o_j^*, r_j^* \mid c_j), ..., g_N(p_N^*, o_N^*, r_N^* \mid c_N)\}$$

<79>

<80> 따라서, 서비스 공급자의 최적의 프라이버시 정책집합은 계산식1에 의해 아래 같이 표현되게 되며,

$$\{p_1^*, ..., p_j^*, ..., p_N^*, o_1^*, ..., o_j^*, ..., o_N^*, r_1^*, ..., r_j^*, ..., r_N^* \mid c_1, ..., c_i, ..., c_N\}$$

<81>

<82> 서비스 공급자의 최적의 프라이버시 정책집합은 상기 협상 에이전트(또는 협상자)에게 전달되게 된다.

<83> 상기 협상 에이전트(또는 협상자)는 사용자 에이전트로부터 전달받은 사용자의 최적집합과 서비스 에이전트로부터 서비스 공급자의 정책집합을 서로 비교하게 되고(S406),

<84> 상기 서비스 공급자의 정책집합은 협상 에이전트(또는 협상자)가 사용자 에이전트에게 전달하여 서비스 공급자의 최적정책을 수락할 것인지를 묻게 된다(S408).

<85> 상기 사용자 에이전트가 서비스 공급자의 최적정책이 사용자의 프라이버시 정책에 부합되면, 서비스 에이전트의 최적정책에 동의한 후 해당 서비스에 대한 사용자의 제안서ID를 서비스 에이전트로 전송하게 되고(S314), 사용자가 서비스 수단(600)에 접근하게 되면 해당 서비스 에이전트는 사용자에게 편재적 서비스를 제공하게 된다(S316).

<86> 만약, 사용자 에이전트가 서비스 공급자의 최적정책이 사용자의 프라이버시 정책에 부합되지 않는다고 판단하게 되면(S312), 상기 정책완화과정을 수행하게 되는데(S313),

<87> 먼저, 사용자 에이전트의 정책완화과정을 설명하면,

<88> 사용자 에이전트는 사용자의 신용을 증명하기 위한 프라이버시 외의 사용자의 위치정보, 외적상황 또는 내적상황 등의 프로파일을 보내게 되고, 서비스 에이전트는 사용자를 위한 더 높은 조건의 카테고리 값을 요청한 후 프라이버시 정책을 업데이트하여 최적화하게 된다(S412, S414).

<89> 즉, 상기 S404단계에서 TC_U 값을 고정시키고, c_i의 수준을 변화시킨다. 이 때 c_M은 TC_U의 결정자이므로 제외하게 되며, 사용자 에이전트가 TC_U를 증가시키는 c_i와 관련된 어떤 작업을 수행해야 하는 경우, 사용자 에이전트는 사용자의 휴대수단(100)으로 그 사실을 알리게 된다.

<90> 다음으로, 서비스 에이전트의 정책완화과정을 설명하면,

<91> 서비스 에이전트는 서비스 공급자의 신용을 증명하기 위한 프라이버시 외의 서비스 공급자의 위치정보, 외적상황 또는 내적상황 등의 프로파일을 보내고, 사용자 에이전트는 서비스 공급자에게 더 좋은 조건의 카테고리 값을 요청한 후 프라이버시 정책을 업데이트하여 최적화하게 된다(S412, S414)

<92> 즉, 상기 S406단계에서 TC_s값을 고정시키고, (p_j, o_j, r_j)의 수준을 변화시킨다. 이 때 $(p_{opt}, o_{opt}, r_{opt})$은 TC_s의 결정자이므로 제외되며, 서비스 에이전트가 TC_s를 증가시키는 (p_j, o_j, r_j)와 관련된 어떤 작업을 수행해야 하는 경우, 서비스 에이전트는 서비스 공급자의 서비스 수단으로 그 사실을 알리게 된다.

<93> 상술한 바와 같이 정책완화과정을 수행함으로써 사용자 에이전트의 프라이버시 정책과 서비스 공급자의 프라이버시 정책을 상호조정하여 협상할 수 있도록 하게 되는 것이다.

<94> 상술한 바와 같이 P3P정책을 표현하는 프로그래밍 언어로는 APPEL언어를 사용하는 것을 특징으로 하는 데, 상기 APPEL은 룰 형식의 사용자 프라이버시 정책을 인코딩 하거나 변환할 수 있다. APPEL을 사용한 이유는 APPEL이 P3P에 비해 오히려 더 풍부한 룰의 표현을 가능하게 하기 때문이다. 그러나 APPEL 룰은 P3P기반 스키마로 표현될 수 있는 정책뿐만 아니라 P3P 의사결정과 관련된 또 다른 XML 메타데이터 역시 허용한다. 또한 모든 P3P기술서는 APPEL 기반 프라이버시 정책을 내장시킬 수 있다.

<95> 또한, APPEL을 사용할 경우 사용자와 서비스 공급자는 룰 셋이라 불리는 정책 룰의 집합 안에서 그들만의 프라이버시 정책을 표현할 수 있다. 이 때 룰 셋은 P3P(Platform for Privacy Preferences)가 탑재된 웹사이트로부터 기계가 읽을 수 있는 프라이버시 정책의 수락 여부에 관해 자동 혹은 반자동으로 의사를 결정하기 위한 목적으로 사용자 에이전트 및 서비스 에이전트에 의해 사용될 수 있다.

<96> 편재적 P3P인 P4P의 주요한 특징 중 하나는 동적인 프라이버시 정책이 사용된다는 것이다. 예를 들어 P4P-인지 서비스가 도 10에 도시된 바와 같이 APPEL 언어로 프로그래밍 된 데이터 그룹 기술서를 포함한다고 가정하면,

<97> 도 10의 APPEL 코드에서 <P3P:DATA ref="#user.id.Activity.public">과, <P3P:DATA ref="#user.pseudonym.Activity.public">은 각각 사용자, 사용자의 필명에 대응되는 사용자의 현재 활동 타입이 'Public'과 'Private'임을 의미하게 되는 것이다.

<98> 이하, 본 발명의 일 실시예에 따른 실험사례를 설명하도록 한다.

<99> 도 11은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)를 나타내는 참도면이다. 도 12는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 각 과정을 수행하는 참조도면이다. 도 13은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스 시나리오에 참조하는 카테고리, 목적, 보존의 내용을 포함한 참조도면이다. 도 14는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스의 정적 프라이버시 정책을 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다. 도 15는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 사용자의 정적 프라이버시 정책을 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다. 도 16은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스를 수행하는 과정을 나타내는 도면이다.

<100> 도 11 내지 도 16을 참조하여 적용사례를 구체적으로 설명하면,

<101> P4P의 실험사례는 도 11에 도시된 바와 같이 실제로 한국의 가장 큰 쇼핑몰이면서 아시아에서 가장 큰 복합쇼핑센터인 코엑스(COEX) 안에서 P4P가 어떻게 작동되는지를 실험했다. 1979년에 개관한 코엑스 몰은 2004년에 ISO 9001 인증을 획득했으며 21세기 한국을 체감하는 대표적인 공간이 되는 비전을 가지고 있다. 코엑스는 젊은이들을 위한 건전한 놀이 및 문화공간과 전시 및 컨벤션을 찾은 외국인은 물론 내국인을 위한 부대시설을 제공한다. 이는 아시아 최대의 지하 쇼핑공간으로 200개가 넘는 매장을 가지고 있으며, 한국 올림픽 주 경기장의 약 14.5배에 해당하는 규모인 118,000 m^2의 총 시설면적을 가진다. 또한 MULTIPLEX라 불리는 매장은 단일 매장으로 코엑스 몰 최대 규모인 동시에 한국에서 가장 큰 규모이다.

<102> 코엑스 몰은 쇼핑의 편의성을 높이기 위해 663m의 공용통로를 구성하고 있으며, 그 통로의 폭은 18m로 한국 최대이다. 코엑스 몰 이용자 수는 주중에는 15만명, 주말에는 25만명 정도로 추산된다. 더욱이 부근에 백화점, 호텔, 지하철, 도심공항터미널, 타워와 같은 다양한 건물 및 공간들이 있어 코엑스 몰과 함께 시너지 효과를 내고 있다. 특별히 코엑스 몰은 충성된 고객들과의 관계를 강화하기 위해 멤버쉽 카드를 사용하며 여기서 충성된 고객이란 코엑스 몰 내에서 모임, 데이트, 오락 등의 개인적인 활동으로 많은 시간을 보내는 고객들로, 그들은 코엑스 몰 내에서 제공되는 특별한 서비스에 큰 흥미를 가지고 있으며 그러한 특별한 기회를 놓치고 싶지 않아 하는 특징을 가진다.

<103> 본 발명에서 사용한 APPEL언어로 구현된 P4P 서비스가 어떻게 작동하는지 설명하기 위해 사전적 편재적 컴퓨팅

서비스를 MyEntrance라 지칭하기로 한 이 서비스 내용은 도 12에 도시된 바와 같이 쇼핑몰 안에서 테스트 했다.

<104> Joseph은 그의 ID에 대한 데이터가 저장되어 있는 RF-태그를 가지고 있으며, 그는 회전문을 통해 쇼핑몰의 서비스 존으로 입장한다.

<105> 그가 회전문을 통과하는 동안 회전문에 설치된 RF-리더기는 Joseph의 휴대수단에 부착된 RF-태그를 읽게 되며, MyEntrance 서비스는 사용자에게 쇼핑몰 내의 개인화된 이벤트 및 광고를 보여주게 된다.

<106> 이때, MyEntranc 서비스는 사용자의 ID를 요청하고 선택적으로 그의 전화 번호와 집 주소를 요청하며, 요청된 사용자 ID는 맞춤 서비스 제공 및 사용자의 프라이버시 정책 확인에 사용되며, 전화번호와 집 주소는 정보의 허위 여부를 파악하기 위한 입력 정보로 활용된다. 사용자 ID는 계속해서 관리되고 다른 데이터는 특정 기간 동안만 저장된다.

<107> 이상의 프라이버시 정책들은 사전에 서비스 공급자의 P4P 파일에 정의되어 있으며, 사용자 에이전트는 Joseph을 대신하여 P4P 파일을 액세스하고, Joseph이 그의 전화번호와 집주소는 공유하기 원하지 않는다는 사실을 파악한다.

<108> 여기서 발생하는 갈등을 해결하기 위해 이 서비스 존(zone)의 협상 에이전트(또는 협상자)는 해당 시간에만 적용할 Joseph 맞춤형 P4P 파일을 동적으로 생성하기 위해 사용자 및 서비스 에이전트와 통신한다.

<109> 결과적으로 사용자 및 서비스 에이전트는 전화 번호 및 집주소를 받지 않는 것으로 합의하고 Joseph은 서비스를 받게 되며, Joseph이 이벤트 및 광고가 소개되는 키오스크에 도착하자, 서비스 에이전트는 Joseph에게 제공하기 위한 특정 상품에 대한 상세한 정보를 준비한다.

<110> 그러나, 그 서비스 에이전트는 Joseph이 계획하지 않은 서비스에서 이전에 획득한 컨텐츠를 재사용하는 것에 대한 허용하는지에 대해 알지 못해, 사용자의 프라이버시 정책에 이를 문의하게 된다."

<111> MyEntrance 서비스 시나리오에서 참조하는 카테고리, 목적, 보존의 내용을 포함한 데이터 그룹은 도 13에 도시된 바와 같이 나열되어 있으며, 이때 MyEntrance서비스의 정적 프라이버시 정책은 APPEL언어로 표현하면 도 14에 도시된 바와 같이 표현되며, 서비스 사용자의 정적 프라이버시 정책은 도 15에 도시된 바와 같이 표현되게 된다.

<112> 도 16은 사용자 에이전트와 서비스 에이전트를 이용하여 사용자와 서비스 공급자 양쪽에서 P3P파일을 사용하여 P4P-인지 편재적 서비스인 MyEntrance서비스를 수행하는 과정은 개략적으로 나타낸 것이다.

<113> 이상에서 본 발명의 바람직한 일 실시예를 설명하였으나, 본 발명은 다양한 변화와 변경 및 균등물을 사용할 수 있고, 상기 실시예를 적절히 변형하여 동일하게 응용할 수 있음이 명확하다. 따라서 상기 기재 내용은 하기 특허청구범위의 한계에 의해 정해지는 본 발명의 범위를 한정하는 것이 아니다.

도면의 간단한 설명

<114> 도 1은 본 발명의 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상시스템의 전체적인 구성을 나타내는 도면이다.

<115> 도 2는 본 발명의 바람직한 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상방법을 나타내는 순서도이다.

<116> 도 3은는 본 발명의 일 실시예에 의한 유비쿼터스 환경하의 프라이버시-인지 편재적 시스템을 위한 편재적 피쓰리피 기반의 프라이버시 정책 협상알고리즘을 나타내는 순서도이다.

<117> 도 4는 본 발명의 일 실시예에 의한 종래 프라이버시 정책의 불일치를 나타내는 참조도면이다.

<118> 도 5는 본 발명의 일 실시예에 의한 사용자 에이전트, 서비스 에이전트, 협상 에이전트(또는 협상자)간의 유기적인 결합관계를 나타내는 참조도면이다.

<119> 도 6은 본 발명의 일 실시예에 따른 서비스 공급자에게 상황정보를 제공하기 위한 상황정보의 카테고리와 속성을 나타내는 도면이다.

<120> 도 7은 본 발명의 일 실시예에 따른 서비스 공급자의 프라이버시 정책 목적 및 카테고리를 나타내는 도면이다.

<121> 도 8은 본 발명의 일 실시예에 따른 도 8을 적용한 웹페이지 소스코드를 나타내는 도면이다.

<122> 도 9는 본 발명의 일 실시예에 따른 경제기반모델을 협상알고리즘으로 채택하여 서비스 결핍비용과 감시비용 사이의 트레이드 오프에 의해 계산된 참조도면이다.

<123> 도 10은 본 발명의 일 실시예에 따른 사용자의 동적 프라이버시 정책파일을 생성하는 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다.

<124> 도 11은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)를 나타내는 참도면이다.

<125> 도 12는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 각 과정을 수행하는 참조도면이다.

<126> 도 13은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스 시나리오에 참조하는 카테고리, 목적, 보존의 내용을 포함한 참조도면이다.

<127> 도 14는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스의 정적 프라이버시 정책을 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다.

<128> 도 15는 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 사용자의 정적 프라이버시 정책을 APPEL언어로 프로그래밍된 소스코드를 나타내는 도면이다.

<129> 도 16은 본 발명의 일 실시예에 따른 실험장소인 코엑스(COEX)에서 편재적 서비스를 수행하는 과정을 나타내는 도면이다.

<130> *** 도면의 주요부분에 대한 부호의 설명 ***

<131> 100 : 휴대수단 110 : 제어부

<132> 120 : 통신부 130 : 입력부

<133> 140 : 사용자정책저장부 150 : 출력부

<134> 200 : 상황정보감지수단 300 : 무선망

<135> 400 : 상황정보인식수단 500 : 상황서버

<136> 510 : 제어부 520 : 통신부

<137> 530 : 에이전트관리부 535 : 에이전트D/B

<138> 540 : 협상에이전트부 550 : 정책D/B관리부

<139> 553 : 사용자정책D/B 557 : 서비스공급자정책D/B

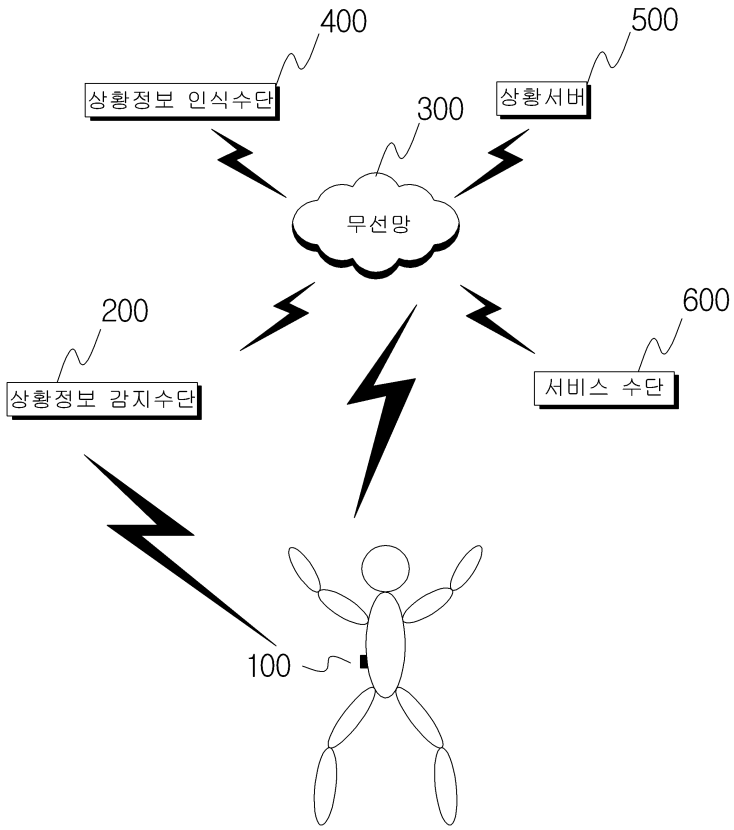
<140> 600 : 서비스 수단 610 : 제어부

<141> 620 : 통신부 630 : 서비스관리부

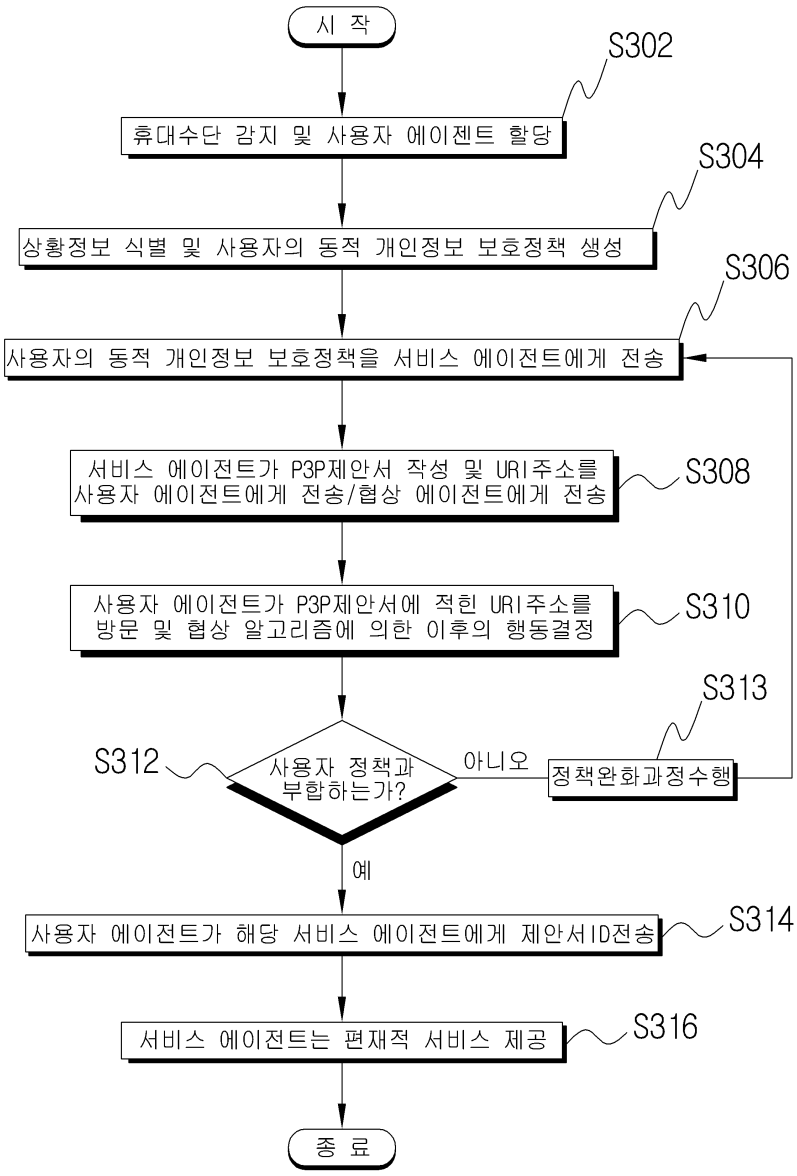
<142> 640 : 서비스공급자정책D/B

도면

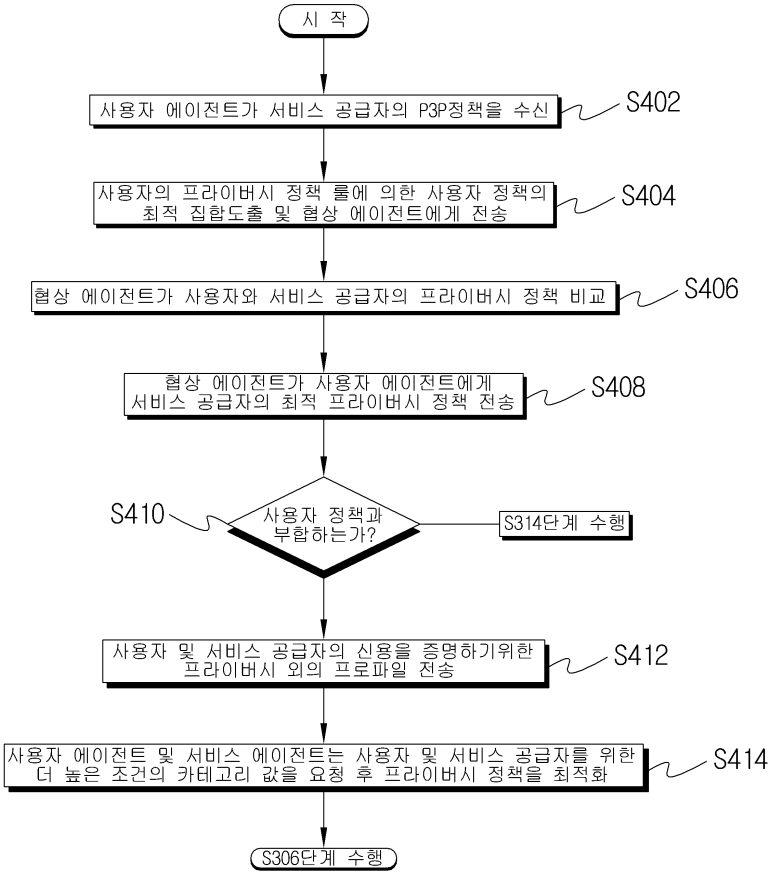
도면1



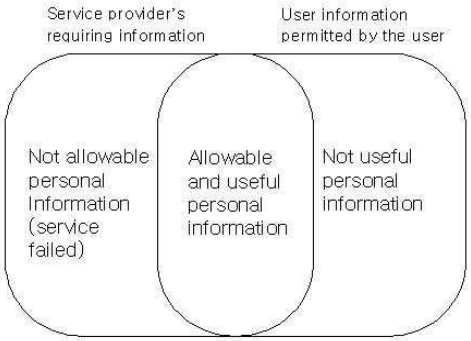
도면2


시 작
S302
휴대수단 감지 및 사용자 에이젠트 할당
S304
상황정보 식별 및 사용자의 동적 개인정보 보호정책 생성
S306
사용자의 동적 개인정보 보호정책을 서비스 에이전트에게 전송
서비스 에이전트가 P3P제안서 작성 및 URI주소를 사용자 에이전트에게 전송/협상 에이전트에게 전송
S308
사용자 에이전트가 P3P제안서에 적힌 URI주소를 방문 및 협상 알고리즘에 의한 이후의 행동결정
S310
S313
S312
사용자 정책과 부합하는가?
아니오
정책완화과정수행
예
사용자 에이전트가 해당 서비스 에이전트에게 제안서ID전송
S314
서비스 에이전트는 편재적 서비스 제공
S316
종 료

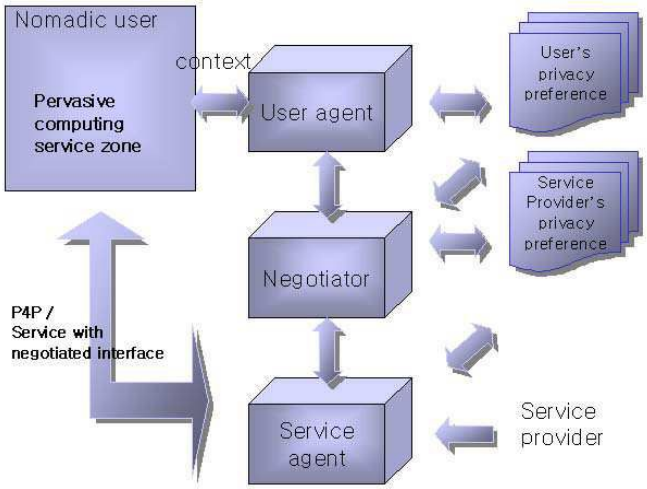
도면3


시 작
사용자 에이전트가 서비스 공급자의 P3P정책을 수신
S402
사용자의 프라이버시 정책 룰에 의한 사용자 정책의 최적 집합도출 및 협상 에이전트에게 전송
S404
협상 에이전트가 사용자와 서비스 공급자의 프라이버시 정책 비교
S406
협상 에이전트가 사용자 에이전트에게 서비스 공급자의 최적 프라이버시 정책 전송
S408
S410
사용자 정책과 부합하는가?
S314단계 수행
사용자 및 서비스 공급자의 신용을 증명하기위한 프라이버시 외의 프로파일 전송
S412
사용자 에이전트 및 서비스 에이전트는 사용자 및 서비스 공급자를 위한 더 높은 조건의 카테고리 값을 요청 후 프라이버시 정책을 최적화
S414
S306단계 수행

도면4


Service provider's requiring information
User information permitted by the user
Not allowable personal Information (service failed)
Allowable and useful personal information
Not useful personal information

도면5



도면6

Context category	Property	Examples
활동	Public Moderate Private	현재 스케줄
위치	Public Moderate Private	현재 위치
사회적	Public Moderate Private	가까이 있는 사람
연산 객체	Public Moderate Private	장치, 네트워크, TV 채널 등
물리적 환경	Public Moderate Private	온도, 기후 등

도면7

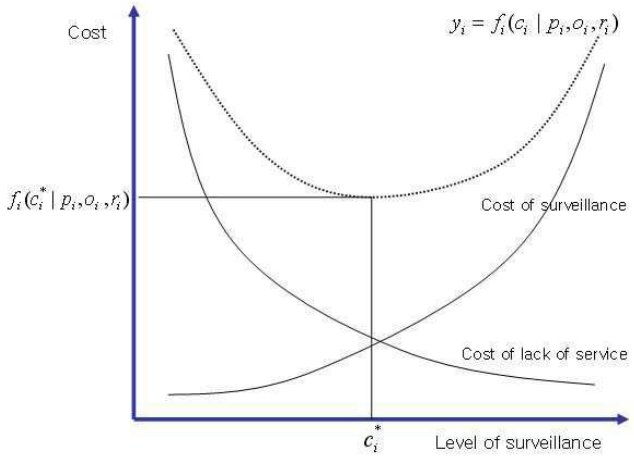
Purpose	<s_current/> <s_develop/> <s_pseudo-analysis/> <s_pseudo-decision/> <s_individual-analysis/> <s_individual-decision/> <share_small/> <share_all/> <academic/> <commerce/> <other-purpose> string <other-purpose/>	One-time getting informed activity Individual R&D (e.g. research paper) Pseudonymous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

도면8

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

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

도면9



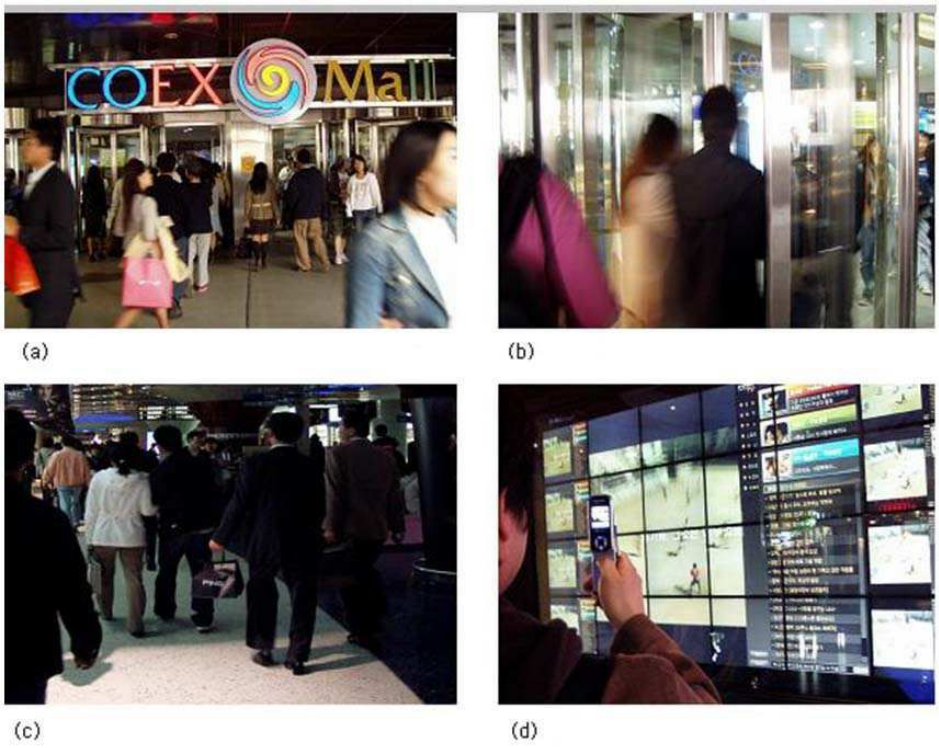
도면10

```
<p3p:DATA-GROUP>
       <p3p:DATA ref="#user.id.Activity.public">
         <p3p:CATEGORIES>
              <p3p:government/>
         </p3p:CATEGORIES>
       </p3p:DATA>
</p3p:DATA-GROUP>
<p3p:DATA-GROUP>
       <p3p:DATA ref="#user.pseudonym.Activity.private">
         <p3p:CATEGORIES>
              <p3p:uniqueid/>
         </p3p:CATEGORIES>
       </p3p:DATA>
</p3p:DATA-GROUP>
```

도면11



도면12



도면13

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

도면14

```
<appel:RULESET xmlns:appel="http://www.w3.org/2002/04/APPELv1"
               xmlns:p3p="http://www.w3.org/2000/12/P3Pv1"
              crtdby="W3C" crtdon="2000-03-18T16:41:21+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="#user.id.Activity.public">
           <p3p:CATEGORIES>
             <p3p:government/>
          </p3p:CATEGORIES>
         </p3p:DATA>
       </p3p:DATA-GROUP>
      <p3p:DATA ref="#user.phone.number">
           <p3p:CATEGORIES>
             <p3p:physical/>
          </p3p:CATEGORIES>
         </p3p:DATA>
       </p3p:DATA-GROUP>
      <p3p:DATA ref="#user.home.address">
           <p3p:CATEGORIES>
             <p3p:physical/>
          </p3p:CATEGORIES>
         </p3p:DATA>
       </p3p:DATA-GROUP>
       <p3p:DATA ref="#user.current.preference.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:connective="or">
          <p3p:tailoring/>
          <p3p:pseudo-decision/>
       </p3p:PURPOSE>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>
</appel:RULESET>
```

도면15

```
<appel:RULESET xmlns:appel="http://www.w3.org/2002/04/APPELv1"
               xmlns:p3p="http://www.w3.org/2000/12/P3Pv1"
             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 product and service data for
sharing with small group or individual research purpose. Contime?">
    <p3p:POLICY>
      <p3p:STATEMENT>
        <p3p:PURPOSE appel:connective="or">
          <p3p:share_small/>
          <p3p:s_develop/>
       </p3p:PURPOSE>
      </p3p:STATEMENT>
    </p3p:POLICY>
  </appel:RULE>
</appel:RULESET>
```

도면16

