情報保護學會論文誌
第18卷 第5號, 2008. 10

P-RBACML : 프라이버시 강화형 역할기반접근통제 정책 언어 모델*

이 영 록[1†], 박 준 형[1], 노 봉 남[1‡], 박 해 룡[2], 전 길 수[2]
[1]전남대학교, [2]한국정보보호진흥원

P-RBACML : Privacy Enhancing Role-Based Access Control Policy Language Model*

Young-lok Lee[1†], Jun-hyung Park[1], Bong-nam Noh[1‡], Hae-ryong Park[2], Kil-su Chun[2]
[1]Chonnam National University, [2]Korea Information Security Agency

요 약

개인 사용자들은 정보통신 서비스 이용을 위해 필요 이상의 개인정보를 공개하므로 프라이버시를 심각하게 침해당한다. 이러한 불완전한 개인정보관리 인프라를 보완하기 위해 P3P나 EPAL, XACML 같은 개인정보보호 플랫폼 기술이 개발되고 있지만, 이들은 개별주체들을 대상으로 보호자원에 대한 접근통제정책을 적용하므로 역할기반 접근통제를 원하는 기업이나 기관에는 적합하지 않다. 본 논문에서는 프라이버시를 강화한 역할기반 접근통제 정책을 표현하는 언어를 제안한다. 제안된 프라이버시 강화형 역할기반 접근통제 정책은 XACML을 변형한 것으로, XACML의 장점인 매칭과 조건 표현을 사용하며 프라이버시를 강화하기 위해 목적, 의무사항을 별도의 엘리먼트로 표현한다. 본 논문에서는 퍼미션 배정 정책에 관한 정책언어 모델을 제안하고, 개인정보보호 법률에 기초한 정책 시나리오와 도큐먼트 인스턴스를 제공한다. 또한 사용자의 요청컨텍스트와 그에 대한 응답컨텍스트도 제공한다.

ABSTRACT

As individual users have to provide more information than the minimum for using information communication service, the invasion of privacy of Individual users is increasing. That is why client/server based personal information security platform technologies are being developed such as P3P, EPAL and XACML. By the way enterprises and organizations using primarily role based access control can not use these technologies, because those technologies apply access control policies to individual subjects. In this paper, we suggest an expression language for privacy enhancing role-based access control policy. Suggested privacy enhancing role-based access control policy language model is a variation of XACML which uses matching method and condition, and separately contains elements of role, purpose, and obligation. We suggest policy language model for permission assignment in this paper, shows not only privacy policy scenario with policy document instance, but also request context and response context for helping understanding.

Keywords : Privacy, RBAC, XACML

Ⅰ. 서 론

지금까지 기업이나 정부, 그리고 개인들은 그들의 요구사항만을 만족하도록 그때그때 필요한 기능만을 갖춘 부분적이며 호환성 없는 독자 솔루션들을 개발해왔다. 이런 솔루션을 이용하기 위해 개인 사용자들은 필요이상의 개인정보들을 제공해야 하고, 기업과 정부는 넘칠 정도로 쌓인 개인정보들을 이용할 수 있게 되어, 개인은 프라이버시(privacy)를 침해당하는 수모를 겪고 있다[1].

프라이버시는 오늘날 고객, 회사, 연구자 그리고 법률 제정자들의 관심이 집중된 정보 기술의 하나이다. 건강 의료분야의 HIPPA[9]나 금융분야의 GLBA[10] 법규 등은 기업들에게 사용자들의 프라이버시를 보호하도록 강제한다. 비록 기업들이 P3P에 기초하여 프라이버시 정책을 웹상에 공표하고, 프라이버시 보증 프로그램들을 수용하는 등 고객 프라이버시 보호를 위한 많은 전략들을 채택하고 있지만, 그러한 전략들에는 고객의 개인정보가 수집된 이후 이들 정보가 실제로 어떻게 다루어지는지를 서술하는 체계적인 메커니즘이 없다[7].

MAC, DAC, 그리고 RBAC과 같은 전통적인 접근제어 모델들은 프라이버시 정책들을 고려하지 않고 디자인 되어 프라이버시 보호에 필수적인 사용목적, 조건, 그리고 의무사항 등의 요구사항들을 거의 만족시키지 못하고 있다. 목적, 조건, 그리고 의무사항 등의 프라이버시 보호를 위한 항목들은 OECD 가이드 라인과 미국 프라이버시 관련 법규, 그리고 잘 알려진 기관들의 공공 프라이버시 정책들로부터 수집된 공통사항들이다[7].

한편 프라이버시 정책들을 표현하는 언어는 접근제어 정책들을 표현하는 언어와 동일해야 한다. 왜냐하면 두 종류의 정책 모두 같은 자원들에 대해 접근제어하는 것이므로, 서로 충돌이 발생해서는 안되기 때문이다[7]. 이러한 연구의 시도로 프라이버시-인지 RBAC(Privacy-aware RBAC : P-RBAC)이 있다[7]. P-RBAC은 전통적인 RBAC이 프라이버시 정책들을 제공할 수 있도록 RBAC을 확장한 모델이다. 이 모델의 퍼미션 배정은 기존 RBAC 개념에 목적, 조건, 그리고 의무 사항이 추가된다.

프라이버시 보호 요구사항 중 조건(Condition)은 매우 중요하다. 조건은 어떤 액션이 실행되기 전에 반드시 만족해야 하는 요소이다. 어린이에 관한 정보가 그중 하나로, COPPA의 중요한 규칙 중 '검증 가능한 부모 동의'(Verifiable Parental Consent : VPC)가 그것이다. 예를 들면, 아이로부터 개인정보를 수집/이용/공개하기 이전에 운영자는 아이의 부모로부터 검증가능한 부모 동의를 반드시 얻어야 한다. 13살 이하의 아이들과 관련된 개인 정보를 수집하거나 접근하기 이전에 반드시 만족 되어야만 하는 조건이 VPC이다.

그러나 P-RBAC에서 표현하는 조건은 논리적인 구조의 추상적 표현이어서 표현을 쉽게 할 수 있다는 장점은 있으나 수행할 수 있는 연산의 종류가 단조롭고, 시스템에 따라 이 조건 표현이 다르게 구현될 수 있다. 조건을 구성하는 요소로는 요청자 정보와 정보소유자 정보, 자원이나 환경변수 값(접속시간 등) 등이 있는데, 조건을 풍부하게 표현하려면 이들을 대상으로 산술, 집합, 관계, 논리연산 등을 수행할 수 있어야 한다. 그러나 P-RBAC의 LC_0는 조건을 풍부하게 표현할 수 없다는 단점을 안고 있다.

기업전반에 걸친 보안정책이 공통언어로 구현될 수 있다면, 정보시스템내의 각 컴포넌트에 존재하는 모든 보안정책들의 집행을 총괄적으로 관리할 수 있다[6]. 따라서 본 논문은 프라이버시를 강화한 역할기반 접근통제 정책을 명세할 수 있는 XML기반의 정책표현 언어를 제안한다. XML은 쉽게 확장될 수 있고 플랫폼과 벤더들이 XML을 지원하기 때문에 공통적인 보안정책 언어를 XML로 표현하는 것은 극히 자연스러운 현상이다. 제안한 프라이버시 강화형 역할기반 접근통제 정책 언어는 P-RBAC의 조건을 강화시킨 모델이다.

프라이버시 강화형 역할기반 접근통제 정책은 사용자 배정과 퍼미션 배정으로 나뉜다. 역할들을 사용자들에게 배정하는 것은 정책결정을 내리는 엔티티(entity)가 다루는 범위 밖이며, 또한 사용자 배정정책이 여러 가지 형태로 만들어질 수 있다[8]. 따라서 본 논문은 퍼미션 배정 정책에 관한 정책언어 모델을 제안하고, 개인정보보호에 관한 법률에 기초해 개인정보 보호 정책 시나리오와 함께 정책 도큐먼트 인스턴스도 제공한다. 또한 사용자의 요청에 대한 결과를 한눈에 파악할 수 있도록 요청컨텍스트와 응답컨텍스트도 제공한다.

접수일 : 2008년 1월 2일; 수정일 : 2008년 6월 10일;
채택일 : 2008년 8월 14일
* 본 연구는 한국정보보호진흥원 위탁과제(KISA-WP-2007-0032) 지원사업의 연구결과로 수행되었습니다.
† 주저자, dogu@ssrc.jnu.ac.kr
‡ 교신저자, bbong@jnu.ac.kr

Ⅱ. 관련연구

프라이버시를 보호하기 위한 정책 표현언어에 대한 연구들은 다음과 같다.

2.1 P3P

W3C의 P3P(The Platform for Privacy Preference)는 정보통신서비스 제공자와 서비스 이용자 사이에서 개인정보보호정책을 자동분석할 수 있도록 XML 형식으로 표현하는 플랫폼이다[4]. 다시말해, 서비스 이용자가 웹 브라우저를 이용하여 특정 웹 사이트에 접근하면, 해당 웹 사이트는 수집될 서비스 이용자 개인정보를 어떻게 사용하는 가를 기술한 개인정보보호에 관한 정책을 사용자의 웹브라우저에게 제공하고, 사용자는 자신이 미리 설정해 놓은 프라이버시 정책에 따라 그 수준을 비교한 후 그 결과에 따라 처리하는 기술이다.

그러나 P3P는 개인정보의 수집을 정당하게 하기 위한 측면을 강조한 것이므로 서비스 이용자의 손을 떠나 정보통신서비스 제공자에게 넘어간 이후에는 그러한 개인정보가 어떻게 이용되는지에 대한 추적이 어렵다. 즉 P3P에는 개인정보를 수집당시의 목적으로 정확하게 사용되었는지에 대한 집행강제규정이 없다. 따라서 P3P는 서비스 이용자가 정보통신서비스 제공자를 무한히 신뢰한다는 가정 하에서만 의미 있는 기술이다.

2.2 EPAL

EPAL(Enterprise Privacy Authorization Language)은 기업 내 개인정보보호 운용을 포괄적으로 제시·관장하는 시스템 언어이며, IBM과 ZKS가 공동으로 개발한 기술이다[5]. 수집하는 개인정보마다 해당 정보의 사용 범위와 목적을 지정한 정보를 끼워 넣는 원리이다.

EPAL은 프라이버시 정책을 생성하기 위해 어휘(vocabularies)라는 개념을 사용하는데, 이는 기업간에 다양한 정책을 수립할 수 있도록 EPAL의 확장성을 염두에 둔 것이다. EPAL은 사용자 카테고리, 데이터 카테고리, 목적, 행위, 조건, 의무 등의 계층 리스트를 정의하고 이 어휘를 이용하여 프라이버시 정책을 생성한다.

사용자 카테고리는 데이터를 사용하는 주체에 대한 계층구조이고, 데이터 카테고리는 수집된 데이터를 프라이버시 관점에서 정의한 것이다. 목적은 데이터가 사용되는 의도를 나타낸 것이고, 행위는 데이터에 대한 연산을 의미하며, 조건은 정책판단에 요구되는 제약으로 참인 경우에만 데이터에 접근할 수 있도록 해준다. 앞에서 설명한 P3P는 EPAL과 함께 상호보완하는 기술로 사용될 수 있다.

2.3 XACML

XACML(eXtensible Access Control Markup Language)는 OASIS 그룹에서 진행한 표준화 기술로 정당한 자원 요청 개체에게만 권한을 부여하여 자원들을 접근할 수 있도록 XML 기반의 접근제어 정책 언어이다[6].

XACML은 이용자가 요청을 하면 시스템이 자동으로 정책판단을 하고 그 결과로써 응답할 수 있도록 접근제어 정책과 요청컨텍스트, 그리고 응답 컨텍스트를 XML로 명세할 수 있도록 XML 스키마를 제공한다. 시스템이 XACML을 이용해 접근통제를 수행하기 위해서는 PEP(Policy Enforcement Point), PDP(Policy Decision Point), PAP(Policy administration Point) 등의 행위자들이 상호작용해야 한다.

PEP는 자원요청자로부터 온 접근요청을 받은 후 요청컨텍스트를 만들어 컨텍스트 핸들러(context handler)에게 보내고, 컨텍스트 핸들러는 요청컨텍스트를 PDP에게 보내 권한결정을 요청한다. PDP는 PAP가 설정해 놓은 정책을 반영하여 요청자의 접근가능 여부를 판단해 응답컨텍스트(response context)를 만들어 컨텍스트 핸들러에게 보낸다. 컨텍스트 핸들러는 응답결과를 PEP에게 보내고, PEP는 의무사항이 있는지를 살펴보고 참인 경우 최종적으로 의무조치와 함께 접근을 허가한다.

2.4 P-RBAC

Qun Ni와 Bertino 등은 사용자(User), 역할(Role), 데이터(Data), 액션(Action), 목적(Purpose), 의무사항(Obligation), 그리고 조건(condition)으로 구성되는 P-RBAC(Privacy- aware Role Based Access Control) 모델을 제안하고 있다. 이들 구성 요소 중 조건을 표현하기 위해 LC_0라 불리는 특별 언어를 사용한다. P-RBAC은 일반 RBAC처럼 코어 P-RBAC, 계층 P-RBAC, 조건 P-RBAC, 일반 P-RBAC 모델들로 나뉜다[7].

코어 P-RBAC의 특징은 프라이버시 퍼미션들의 복잡한 구조에 있는데, 퍼미션 배정은 (역할, ((액션, 데이터), 목적, LC_0, 의무사항))으로 표현된다. 프라이버시 퍼미션들의 복잡한 구조는 OECD 원칙들과 프라이버시 법률들의 본질을 표현하기 위해 매우 구조화된 방식으로 프라이버시 규칙들을 표현한다. 따라서 프라이버시 퍼미션(permission)은 데이터와 그 데이터 상에서 실행되는 액션(action) 이외에도, 어떤 조건에서 퍼미션이 부여될 수 있는지와 실행 이후의 의무사항 등을 명백하게 진술하고 있다.

그러나 이들이 제안한 모델의 퍼미션 배정은 논리적인 구조의 추상적 표현이어서 표현을 쉽게 한다는 장점은 있으나 이 표현을 구현하는 측면에서는 시스템마다 다르게 구현될 수 있다. 또한 조건 표현에 있어서도 사전에 컨텍스트 변수의 도메인 영역을 설정해야 하며, 산술연산이나 관계연산, 논리연산 등의 조건표현을 풍부하게 할 수 없는 등의 문제를 안고 있다.

2.5 XACML V.2 기반의 코어 & 계층 RBAC Profile

OASIS는 코어 RBAC과 계층 RBAC을 XACML로 표현할 수 있는 프로파일을 제공한다. 이 명세는 사용자 배정(강제사항)과 퍼미션 배정(선택)으로 나누어 정책 집합과 정책, 그리고 규칙을 정의한다[8]. 그러나 이 프로파일은 프라이버시를 강조하는 요소인 목적과 의무사항 등이 포함되어 있지 않을뿐더러, 강력한 XACML의 한 단면을 보여주기 위한 시도로써 XACML의 틀 속에 RBAC을 온전히 포함시키고 있기 때문에 RBAC 개념과 철학에 어울리지 않을 뿐만 아니라 반복되는 의미없는 엘리먼트를 안고가야 하는 문제점을 지닌다.

이와 같은 문제들을 해결하기 위해서는 프라이버시를 강화시킨 역할기반 접근통제정책을 잘 반영시킬 수 있는 정책언어를 개발해야 한다. 본 논문은 이러한 정책언어 모델을 제안하고, 이 모델이 어떻게 이용될 수 있는지를 개인정보보호 관련법률에 기초한 시나리오와 함께 보여준다.

Ⅲ. 프라이버시 강화형 역할기반 접근통제정책 언어 모델

제안하는 정책언어는 다음과 같은 요구사항들을 만족한다.

1) **풍부한 조건 표현** - XACML에는 조건에 이용되는 비표준 함수를 추가하는 수단과 수많은 내장함수들을 포함하고 있다. 또한 <Apply> 요소를 이용해 임의의 복잡한 함수도 만들 수 있다. 따라서 제안한 모델은 XACML의 연산자 표현을 수용함으로써 XPath와 XQuery에서 정의된 함수들을 그대로 사용할 수 있게 되어 산술연산, 관계연산, 집합연산 및 논리연산을 이용한 제약이 가능하다.

2) **요청자의 요구와 정책 간에 쉬운 연결** - XACML은 요청자의 요구에 적용가능한 정책을 쉽게 연결하기 위해 요청자의 요청컨텍스트에 표현되어 있는 값들과 정책에 정의되어 있는 값들 간에 매칭을 이용한다. 제안한 모델은 이를 수용함으로써 프라이버시 중요도에 따른 다단계의 필터를 수행할 수 있어 정책 검색 시간을 단축시킨다.

3) **RBAC 철학 반영** - XACML은 주체에게 적용시킬 수 있는 정책들은 어떤 정책이라도 나열할 수 있으며 충돌시 결합알고리즘(combining algorithm)에 의해 해결한다. 이에반해 RBAC은 충돌되는 퍼미션 배정이 존재해서는 안된다는 것을 가정하고 있다. 그러므로 RBAC에는 결합알고리즘의 필요성이 사라진다. 또 RBAC은 역할 단위로 접근통제를 수행하므로 요청자의 역할이 정책의 역할과 일치하는지 판단이 끝나면, 그 후는 그 역할에 배정된 퍼미션에 따라 접근통제를 하면 그만이다. 따라서 XACML의 틀 속에서 RBAC을 표현하면 군더더기 엘리먼트를 포함하게 되어 시스템 구현이 비효율적이 된다.

4) **프라이버시 강화 요소 포함** - 개인정보 소유자는 자신의 정보가 시스템에서 어떻게 이용되었는지를 아는 것이 중요하다. 따라서 소유자 자신이 정보제공시 동의했던 수집목적과 이용목적이 일치하는지, 그리고 언제 이용되었는지를 소유자 자신이 알 수 있도록 로그나 SMS 문자정보 등을 통해 전달받을 수 있도록 시스템의 의무사항(obligation)등이 명세되어야 한다. 제안된 모델은 이들 요소들을 별도의 엘리먼트로 정의한다.

프라이버시를 강화하는 역할기반 접근통제 정책은 사용자 배정과 퍼미션 배정, 그리고 역할계층 관계를 포

함한다. 사용자 배정 정책은 반드시 동일한 시스템에 존재해야 하는 것은 아니고 여러 가지 형태로 정책이 만들어질 수 있는 선택사항이므로, 본 논문에서는 퍼미션 배정에 역점을 두고 표현한다. 본 논문의 정책표현 범위는 Core-RBAC과 계층-RBAC을 수용한다. 제안된 모델에서는 사전 역할계층 관계가 존재하고, 그 역할계층의 포함관계에 의해 하위계층의 퍼미션은 상위계층의 퍼미션 배정에 자동 반영됨을 가정하고, 이를 정책 스키마에 반영하고 있다.

3.1 용어정의

제안하는 정책언어의 XML 스키마에 사용되는 용어는 다음과 같다.

P-PASet : 모든 퍼미션 배정(P-PA)들을 모아놓은 것으로 같은 이름을 지닌 역할이라도 조직이 다르면 다른 임무와 책임을 수행할 수 있음을 고려함. 속성값으로 고유 식별자를 지님.

P-PA : 한 역할에 배정된 퍼미션들을 나타내는 엘리먼트. 예를 들어 역할 사장이 지니는 모든 퍼미션을 의미. 속성값으로 고유 식별자를 지님.

Role : 조직 내에서 직원 또는 사용자에게 부여된 임무와 책임을 의미하는 엘리먼트. 속성값으로 고유 식별자를 지님.

P-PermissionSet : P-Permission들을 모아놓은 엘리먼트. 속성값으로 고유 식별자를 지님.

P-Permission : 접근되는 데이터와 그 데이터에 행해지는 연산의 쌍 이외에 프라이버시를 강화하기 위해 필요한 목적, 조건, 의무사항이 추가된 퍼미션을 뜻함.

Purpose : 개인 정보를 수집한 조직에서 해당 데이터를 사용하도록 허용된 분야.

Permission : 개인정보(PersonalData)와 연산(operation)의 쌍으로 구성됨.

Condition : 어떤 액션이 실행되기 전에 만족하여야만 하는 필요조건으로 논리연산과 관계연산을 하기 위해 XPath 내장함수와 XQuery 내장함수를 사용할 수 있음. 기타 불리언 연산을 위해 변수를 새로 정의하여 사용할 수도 있음.

Obligation : 개인정보를 대상으로 행위연산이 실행된 이후 반드시 수행되어야 하는 의무사항.

PersonalDataSet : PersonalData의 집합.

PersonalData : 시스템 내에 저장된 개인정보로 요청자가 접근하고자 하는 대상.

Action : 개인데이터를 상대로 일어나는 행위 연산.

그 외 논문의 이해를 위해 사용된 용어의 정의는 다음과 같다.

Attribute : 요청 컨텍스트안에 <Attribute> 엘리먼트로 표현하며, 식별자와 데이터 타입을 속성으로 가짐. <AttributeValue> 엘리먼트를 자식엘리먼트로 가지며, 시스템내에 저장되어 있는 P-PA 정책들에 의해 참조됨.

PDP(Policy Decision Point) : 접근결정을 하는 엔티티로 요청 컨텍스트에 매칭되는 P-PA 정책이 있는지를 평가함.

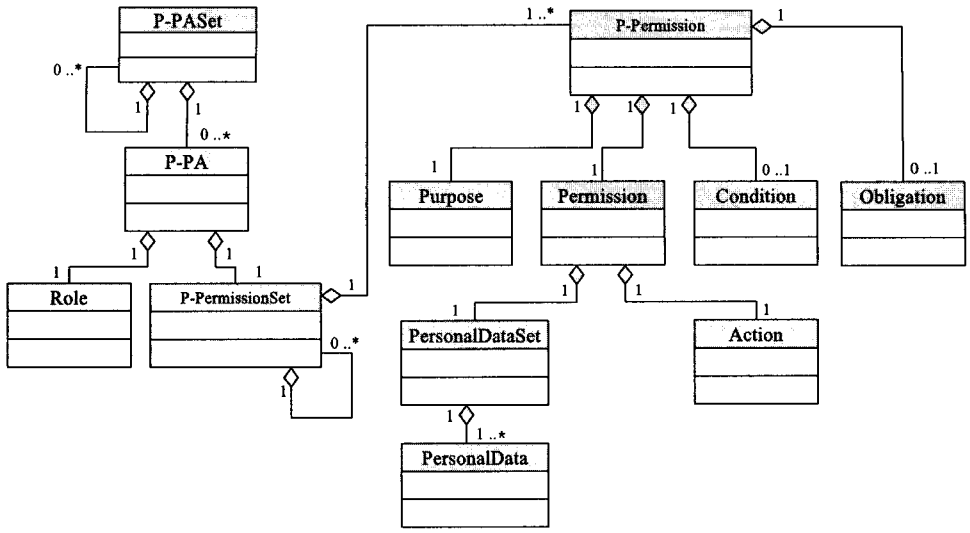
PAP(Policy Administration Point) : P-PASet이나 P-PA를 생성하는 시스템 엔티티.

컨텍스트 : 정책판단을 위해 PDP에게 보내지는 요청자의 정보인 요청 컨텍스트와 PDP에 의해 정책판단이 내려진 결과인 응답 컨텍스트로 구성됨. 이들은 모두 캐노니컬(canonical) 형태로 표현됨.

3.2 P-RBACML 정책 언어 모델

프라이버시 퍼미션 배정 정책은 [그림 1]과 같은 엘리먼트들로 구성된다. 제안된 모델은 크게 세 가지 특징을 지닌다. 하나는 요구사항에서 지적한 사항을 만족하기 위해 서브젝트인 역할과 이 역할이 수행하는 퍼미션들을 XACML의 스타일로 묶는 것이고, 또 하나는 P-RBAC이 지닌 조건의 단점을 보완하기 위해 XACML의 조건을 차용한 것이다. 그리고 나머지 하나는 프라이버시 보호를 위해 P-RBAC 모델로부터 차용한 목적과 의무사항이다. 제안된 모델의 <P-PermissionSet> 엘리먼트의 자식 엘리먼트인 <P-Permission>은 기존 RBAC의 퍼미션과 달리 다섯 개의 엘리먼트로 구성되어 있다. 역할, 개인데이터와 액션, 목적, 조건, 그리고 강제사항이 그것이다.

역할이 자원에 대해 액션을 수행하기 위해서는 요청자의 목적과 조건이 정책의 목적과 조건에 부합해야 한다.



〔그림 1〕 P-RBACML 정책언어 모델

그리고 역할이 자원에 대한 액션을 수행한 후에는 반드시 강제사항이 처리되어야 한다. 위에서 제안한 P-RBACML 정책언어 모델은 이들을 표현하고 있다. 주요 엘리먼트들에 대한 XML 스키마는 <부록>에 제공한다.

PAP(policy administration Point)는 퍼미션 배정과 관련된 정책들을 스키마에 맞는 도큐먼트 인스턴스로 명세하여 PDP에게 제공한다. PAP는 관리자가 역할에 지정하는 고유한 퍼미션들을 배정하는 것 이외에 역할계층 관계를 고려하여 그보다 하위계층 역할의 퍼미션들도 지정역할에 포함시켜야 하므로, <P-PermissionSet> 엘리먼트내에는 자식엘리먼트로 <P-PermissionSet> 엘리먼트가 포함되도록 명세하고 있음을 알 수 있다.

3.3 정책 시나리오 및 정책 도큐먼트 인스턴스 예

3.3.1 정책 시나리오

"정보통신서비스제공자등(예, 마켓팅 부서)이 만 14세 미만의 아동에 대한 개인정보(예, 전자우편, 사용자 이름)를 이용하고자 할 때에는 그 법정대리인의 동의를 얻어야 한다."

3.3.2 개인정보 DB

프라이버시 보호 정책 시나리오에 반영될 개인정보 DB는 [그림 2]와 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<PInfo xmlns="urn:example:e-com:schemas:PersonalInfo"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <p-data>
    <p-id>mk2mj</p-id>
    <p-name>hong gil dong</p-name>
    <national-id-no>550505-1234567</national-id-no>
    <passport-number/>
    <p-id>honggun</p-id>
    <date-of-birth>1955-05-05</date-of-birth>
    <e-mail>hong@e-commerce.com</e-mail>
    <phone>02.123.1234</phone>
    <guardian-info/>
    <consent-info>
        <consent-value> YES </consent-value>
    </consent-info>
  </p-data>

  <p-data>
    <p-id>kkk2</p-id>
    <p-name>kim cho co</p-name>
    <national-id-no>950110-1234567</national-id-no>
    <passport-number/>
    <p-id>kimgun</p-id>
    <date-of-birth>1995-01-10</date-of-birth>
    <e-mail>kim@e-commerce.com</e-mail>
    <phone>062.123.1234</phone>
    <guardian-info>
      <g-name>kim nam su</g-name>
    </consent-info>
  </p-data>
</PInfo>
```

〔그림 2〕 개인정보 DB

3.3.3 정책 도큐먼트 인스턴스 예

[그림 3]의 정책 인스턴스가 시스템에 적용되는 예는 다음과 같다. 먼저 요청자의 인증과 함께 요청자의 요구

```
<?xml version="1.0" encoding="UTF-8"?>
<P-PASet xmlns="urn:jnu:ssrc:PPA:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:jnu:ssrc:PPA:1.0 pPA.xsd" xmlns:ec="urn:example:e-commerce:schemas:PersonalInfo"
xmlns:xf="http://www.w3.org/TR/2002/WD-xquery-operators-20020816/#" P-PASetId="urn:jnu:ssrc:P-PASet:1.0:P-PASetId:1">
<P-PA P-PAId="urn:jnu:ssrc:P-PASet:1.0:P-PA:P-PAId:1">
  <Role RoleId="urn:jnu:ssrc:P-PASet:1.0:P-PA:Role:RoleId:1">
    <RoleMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        urn:jnu:ssrc:P-PASet:1.0:P-PA:Role:Marketing</AttributeValue>
      <RoleAttributeDesignator AttributeId="urn:jnu:ssrc:P-RBACML:1.0::Role:role-id"
        DataType="http://www.w3.org/2001/XMLSchema#string" />
    </RoleMatch> </Role>
  <P-PermissionSet P-PermissionSetId="urn:jnu:ssrc:P-PASet:1.0:P-PA:P-PermissionSet:P-PermissionSetId:1">
    <P-Permission P-PermissionId="urn:jnu:ssrc:P-PASet:1.0:P-PA:P-PermissionSet:P-Permission:P-PermissionId:1">
      <VariableDefinition VariableId="20071108">
        <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:date-less-or-equal">
          <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
            DataType="http://www.w3.org/2001/XMLSchema#date"/>

          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration">
            <AttributeSelector RequestContextPath="/ec:PInfo/ec:p-data/ec:date-of-birth/text()"
              DataType="http://www.w3.org/2001/XMLSchema#date"/>
            <AttributeValue DataType="http://www.w3.org/TR/2002/WD-xquery-operators-20020816#
              yearMonthDuration">
              <xf:dt-yearMonthDuration> P13Y </xf:dt-yearMonthDuration>
            </AttributeValue> </Apply> </Apply> </VariableDefinition>
      <Purpose>
        <PurposeMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> Promotion </AttributeValue>
          <PurposeAttributeDesignator AttributeId="urn:jnu:ssrc:P-RBACML:1.0:purpose:purpose-id"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </PurposeMatch> </Purpose>
      <Permission PermissionId="urn:jnu:ssrc:PPA:1.0:permissionId:1">
        <PersonalDataSet>
          <PersonalData>
            <PersonalDataMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                /ec:PInfo/ec:p-data/ec:p-name
              </AttributeValue>
              <PersonalDataAttributeDesignator AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:pdata:p-name"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </PersonalDataMatch> </PersonalData>
          <PersonalData>
            <PersonalDataMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                /ec:PInfo/ec:p-data/ec:p-email
              </AttributeValue>
              <PersonalDataAttributeDesignator AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:pdata:e-mail"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </PersonalDataMatch> </PersonalData> </PersonalDataSet>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> read </AttributeValue>
            <ActionAttributeDesignator AttributeId="urn:jnu:ssrc:P-RBACML:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ActionMatch> </Action> </Permission>
      <Condition>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
          <VariableReference VariableId="20071108"/>
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <PersonalDataAttributeDesignator
              AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:guardian-info:national-id-no"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
            <AttributeSelector RequestContextPath="//ec:PInfo/ec:p-data/ec:guardian-info/ec:national-id-no/text()"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Apply> </Apply> </Condition>
    </P-Permission> </P-PermissionSet> </P-PA> </P-PASet>
```

[그림 3] 프라이버시-퍼미션 배정 정책 인스턴스 예

컨텍스트가 PDP에 전달된다. PDP는 요청자의 요구 컨텍스트의 내용 중 요청자의 역할이 "영업부서(marketing)"인지를 따져본다. 참이면 그 다음으로 목적이 "판촉(promotion)"인지를 따진다. 그리고 요청자가 접근하려는 개인정보가 "전자우편"인지, 접근해서 수행할 연산일 "읽기"인지를 판단한다. 모두가 참(통과하면)이면,

마지막으로 전자우편 소유자의 나이가 14세 이하인지, 이하라면 법정대리인의 동의가 있는지를 따져본다. 이들 모두가 참이면, 비로소 요청자인 마케팅 역할의 사용자가 전자우편 주소에 접근을 허가하여 읽어갈 수 있도록 한다. 이 퍼미션 배정정책이 어떻게 적용되는가는 다음 절의 요청 컨텍스트를 보면 알 수 있다.

3.3.4 요청 컨텍스트와 응답 컨텍스트 예

[그림 4]는 PDP에 전달되는 요청 역할이 수행하고자 하는 요청컨텍스트로써 정책판단에 필요한 정보들을 지닌다. 요청 컨텍스트가 PDP에 전달되면 PDP는 수많은 정책들 중 요청컨텍스트의 역할과 일치하는 퍼미션 정책이 있는지를 검색한다. 다행히 [그림 3]에 있는 퍼미션 배정 정책의 역할이 "marketing"으로 일치함을 인지하고, 그 역할에 배정된 프라이버시 퍼미션들을 검색해나간다. PDP는 [그림 3]의 10라인에 있는 <P-PermissionSet>의 첫 번째 퍼미션 배정인 <P-Permission>을 요청컨텍스트에 적용해 판정하기 위한 매칭작업을 시작한다. [그림 3]의 12라인에 변수정의를 하고 있는데, 이는 나중 조건 테

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <pPA-context:Request xmlns:pPA-context="urn:jnu:ssrc:PPA:1.0:context:schema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:jnu:ssrc:PPA:1.0:context:schema
   pPA-context.xsd">

03 <pPA-context:Role>
04    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:P-RBACML:1.0::Role:role-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string">
05       <pPA-context:AttributeValue> urn:P-RBACAML:1.0:ssrc:jnu:ac:kr:P-PASet:P-PA:Role:Marketing
06       </pPA-context:AttributeValue>
07    </pPA-context:Attribute> </pPA-context:Role>
08
   <pPA-context:PersonalData>
09    <pPA-context:PersonalDataContent>
10       <PInfo xmlns = "urn:example:e-commerce:schemas:PersonalInfo"
11             xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance">
               <p-data>
12                        <p-name>hong gil dong</p-name>
13                        <e-mail>hong@e-commerce.com</e-mail>
14                        <guardian-info>
15                                 <g-name>kim nam su</g-name>
16                                 <g-e-mail>namsu@e-commerce.com</g-e-mail>
17                                 <phone>062.123.1234</phone>
18                                 <national-id-no>560909-1234567</national-id-no>
19                        </guardian-info>
20             </p-data>    </PInfo>    </pPA-context:PersonalDataContent>
21    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:pdata:p-name"
22                        DataType="http://www.w3.org/2001/XMLSchema#string">
23       <pPA-context:AttributeValue> //pPA-context:PersonalDataContent/PInfo/p-data/p-name/text()
         </pPA-context:AttributeValue>    </pPA-context:Attribute>
24    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:pdata:e-mail"
                        DataType="http://www.w3.org/2001/XMLSchema#string">
25       <pPA-context:AttributeValue>  //pPA-context:PersonalDataContent/PInfo/p-data/e-mail/text()
26       </pPA-context:AttributeValue>    </pPA-context:Attribute>
27    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:P-RBACML:1.0:example:guardian-info:national-id-no"
                        DataType="http://www.w3.org/2001/XMLSchema#string">
28       <pPA-context:AttributeValue> //pPA-context:PersonalDataContent/PInfo/p-data/guardian-info/national-id-no/text()
         </pPA-context:AttributeValue>    </pPA-context:Attribute> </pPA-context:PersonalData>
29
30 <pPA-context:Action>
31    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:PPA:1.0:request:consent-info:action"
             DataType="http://www.w3.org/2001/XMLSchema#string">
32       <pPA-context:AttributeValue> read </pPA-context:AttributeValue>
      </pPA-context:Attribute>
33 </pPA-context:Action>
34
35 <pPA-context:Purpose>
36    <pPA-context:Attribute AttributeId="urn:jnu:ssrc:P-RBACML:1.0:purpose:purpose-id"
             DataType="http://www.w3.org/2001/XMLSchema#string">
37       <pPA-context:AttributeValue> Promotion </pPA-context:AttributeValue>
38    </pPA-context:Attribute>
   </pPA-context:Purpose>
39 </pPA-context:Request>
```

[그림 4] 요청 컨텍스트의 도큐먼트 인스턴스 예

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <pPA-context:Response xmlns:pPA-context="urn:jnu:ssrc:PPA:1.0:context:schema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:jnu:ssrc:PPA:1.0:context:schema
   pPA-context.xsd">
03         <pPA-context:Result>
04                 <pPA-context:Decision>Permit</pPA-context:Decision>
05         </pPA-context:Result>
06 </pPA-context:Response>
```

〔그림 5〕 응답 컨텍스트의 도큐먼트 인스턴스 예

스트에서 사용하기 위함이다. 변수정의에 사용된 식별자 <VariableDefinition VariableId="20071108">는 접근되는 개인데이터 소유자의 나이가 14세 미만인지를 테스트하여 그 결과로 "True" 값을 지니게 된다. PDP는 [그림 3]의 20~25라인을 보고 요청자의 사용목적과 접근되는 개인데이터의 제공목적이 같은지를 검사한다. 제공목적은 [그림 3]의 22라인에 있는 "promotion"임을 알고, 요청자의 사용목적도 같은지를 알기 위해 [그림 3]에 있는 개인정보보호 정책 인스턴스 23라인의 <Purpose AttributeDesignator AttributeId= "urn : jnu : ssrc : P-RBACML : 1.0 : purpose : purpose-id"> 속성 값과 일치하는 값이 [그림 4]의 요청 컨텍스트에 있는지 따져본다. 다행히 [그림 4]의 36라인에 존재하므로 속성 값인 "Promotion"을 가져와 제공목적 "Promotion"과 비교해 일치하므로 "True"값을 반환한다. 이런 식으로 요청자의 Action과 조건들을 차례로 비교하고 이들 요소들이 모두 "True"임이 판명되면, 이 <P-Permission> 엘리먼트의 결과값으로 "True"를 반환하여 요청자가 개인정보를 읽을 수 있도록 허가한다.

[그림 5]는 PDP가 [그림 3]을 [그림 4]에 적용해 본 결과 값인 응답 컨텍스트를 보여주는데, 결과 값으로 "Permit"을 PEP에게 반환시켜줌을 알 수 있다.

Ⅳ. 분석 및 결론

개인정보보호를 위한 플랫폼인 P3P 등은 개인정보를 정보통신서비스 제공자에게 넘겨 준 이후에 개인정보 소유자 중심의 통제가 어렵다. 반면에 XACML은 개인정보소유자와 개인정보보호정책을 밀접하게 연관지어 일정한 통제를 가할 수 있도록 융통성을 제공한다. 하지만 기업이나 조직이 필요로하는 역할기반접근통제 정책을 그대로 반영시키기에는 여러 가지 문제를 안고 있다. 더욱이 프라이버시 보호를 강화할 목적으로 시도되는 연구는 추상적인 수준에서만 이루어지고 있는 실정이다. 본 논문은 사용자 중심의 통제를 강화하기 위해 프라이버시를 강화하는 역할기반 접근통제 정책을 XML로 표현한 정책정의 언어를 제안한다.

〔표 1〕 제안한 정책언어와 다른 정책언어 비교

	P3P	XACML	제안한 P-RBACML
조건 표현	불가능	풍부	풍부
사용자 중심 통제	불가능	가능	가능
역할기반 접근통제	불가능	불완전	완전
프라이버시 고려	가 능	불완전	완전
요청과 정책연결	불가능	쉬움	쉬움

제안한 언어는 XACML의 장점인 매칭기법과 풍부한 조건표현을 그대로 수용하고 있으면서도 역할기반접근통제 개념에 충실하도록 모델링하여 설계되어 있다. 제안한 언어를 XACML이나 기타 다른 정책 표현언어와 비교분석하기에는 적절하지 않지만 몇 가지 측면을 살펴보면 [표 1]과 같다.

제안된 언어는 프라이버시를 고려한 퍼미션 배정이 다시 퍼미션 배정을 포함할 수 있게 하고 있는데, 이는 원-스톱 서비스 형태로 정책판단을 수행하도록 배려한 것이다. 다시 말해 성능이 좋지 못한 머신에 탑재된 PDP라고 하더라도 요청자의 요청에 대해 한 번에 정책판단을 할 수 있도록 수행효율성을 배려한 것이다. 따라서 조직개편이 있게되면 정책반영을 위해 시스템을 정지시키고 새로운 퍼미션 배정을 해야하는 문제를 안고 있다. 이는 역할기반 접근통제 모델의 장점을 살리지 못한 결과를 초래할 수도 있다.

실제 프라이버시 강화형 역할기반 접근통제 프로토타입 시스템을 구축하기 위해서는 요청자의 요청을 자동 분석하는 것과 그 요청에 맞는 퍼미션 배정정책을 검색하는 것이 필수이다. 이를 위해서는 요청자의 요구가 바로 요청컨텍스트 생성으로 쉽게 이어져야 하며, 또한 적용가능한 정책 검색이 빠르게 진행되어야 한다. 현재 사용자 요구가 바로 요청 컨텍스트로 생성될 수 있도록 GUI를 개발 중에 있으며, 한편으로는 정책과 요청

컨텍스트간에 연결을 위한 AttributeId 값들을 일관성있게 정의하는 일을 수행하고 있다. 또한 개발된 시스템의 활용측면을 위해 개인정보 보호 관련법률에 기초한 시나리오 개발도 병행하고 있다. 현재 PDP가 탑재될 머신이 강력한 것으로 가정하고 한 역할에는 고유한 퍼미션들만을 배정하고 역할간의 계층 관련성은 PDP가 다시 역할계층 정책을 참조하여 정책판단을 수행할 수 있도록 향상된 P-RBACML 언어를 개발 중에 있다.

참고문헌

[1] PRIME White Paper V2 version 1.0 27 June 2007.

[2] A. Rezgui, A. Bouguettaya, and M.Y. Eltoweissy, "Privacy on the Web : Facts, Challenges, and Solutions," IEEE Security & Privacy, Vol.1, 2003.

[3] 노종혁, 진승헌, "웹 환경에서 정책 기반 개인정보보호 기술," 전자통신동향분석 제22권 제4호, 8월 2007년.

[4] W3C, "The Platform for Privacy Preferences 1.1(P3P 1.1) Specification," 2006.

[5] W3C, "The Enterprise Privacy Authorization Language(EPAL 1.2)," 2002.

[6] OASIS, eXtensible Access Control Markup Language(XACML) Version 2.0, Committee Draft 04, 2004.

[7] Qun Ni, "Privacy-aware Role Based Access Control," SACMAT'07, June, 2007.

[8] OASIS, "Core and hierarchical role based access control(RBAC) profile of XACML v2.0", February 2005.

[9] United State Department of Health. Health insurance portability and Accountability act of 1996.

[10] U.S. Senate Commitee On Banking, Housing, and Urban Affairs. Information regarding the gramm-leach-bliley act of 1999.

〈부록〉 P-RBACML 정책 XML 스키마

```
〈?xml version="1.0" encoding="UTF-8"?〉
〈xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:PPA="urn:jnu:ssrc:PPA:1.0"
 targetNamespace="urn:jnu:ssrc:PPA:1.0"
 elementFormDefault="qualified"
 attributeFormDefault="unqualified"〉

〈xs:element name="P-PASet"〉
〈xs:complexType〉
  〈xs:sequence〉
    〈xs:element ref="PPA:Description" minOccurs="0" /〉
    〈xs:element ref="PPA:P-PASetDefault" minOccurs="0" /〉
    〈xs:choice minOccurs="0" maxOccurs="unbounded"〉
      〈xs:element ref="PPA:P-PA" /〉
      〈xs:element ref="PPA:P-PAIdReference" /〉
      〈xs:element ref="PPA:P-PASetIdReference" /〉
    〈/xs:choice〉
  〈/xs:sequence〉
  〈xs:attribute name="P-PASetId" type="xs:anyURI"
    use="required"/〉
〈/xs:complexType〉
〈/xs:element〉

〈!-- Description, P-PASetDefault, 명세 생략 --〉

〈xs:element name="P-PA" type="PPA:P-PAType"/〉
〈xs:complexType name="P-PAType"〉
  〈xs:sequence〉
    〈xs:element ref="PPA:Role"/〉
    〈xs:element ref="PPA:P-PermissionSet"/〉 〈/xs:sequence〉
  〈xs:attribute name="P-PAId" type="xs:anyURI"
    use="required"/〉
〈/xs:complexType〉

〈xs:element name="Role" type="PPA:RoleType"/〉
〈xs:complexType name="RoleType"〉
  〈xs:choice〉
    〈xs:element ref="PPA:RoleMatch"/〉
    〈xs:element ref="PPA:RoleIdReference"/〉 〈/xs:choice〉
  〈xs:attribute name="RoleId" type="xs:anyURI"
    use="required"/〉
〈/xs:complexType〉

〈xs:element name="P-PermissionSet"
  type="PPA:P-PermissionSetType"/〉
〈xs:complexType name="P-PermissionSetType"〉
  〈xs:sequence〉
    〈xs:choice minOccurs="1" maxOccurs="unbounded"〉
      〈xs:element ref="PPA:P-Permission"
        maxOccurs="unbounded"/〉
      〈xs:element ref="PPA:P-PermissionIdReference"
        maxOccurs="unbounded"/〉 〈/xs:choice〉
    〈xs:choice minOccurs="0" maxOccurs="unbounded"〉
      〈xs:element ref="PPA:P-PermissionSetIdReference"/〉
    〈/xs:choice〉
  〈/xs:sequence〉
  〈xs:attribute name="P-PermissionSetId" type="xs:anyURI"
    use="required"/〉
〈/xs:complexType〉

〈xs:element name="P-Permission"
  type="PPA:P-PermissionType" /〉
〈xs:complexType name="P-PermissionType"〉
  〈xs:sequence〉
    〈xs:element ref="PPA:VariableDefinition" minOccurs="0"
      maxOccurs="unbounded"/〉
    〈xs:element ref="PPA:Purpose"/〉
    〈xs:element ref="PPA:Permission"/〉
    〈xs:element ref="PPA:Condition" minOccurs="0"/〉
    〈xs:element ref="PPA:Obligation" minOccurs="0"/〉
  〈/xs:sequence〉
  〈xs:attribute name="P-PermissionId" type="xs:anyURI"
    use="required"/〉
```

```
</xs:complexType>

<xs:element name="Purpose" type="PPA:PurposeType"/>
<xs:complexType name="PurposeType">
  <xs:sequence>
    <xs:element ref="PPA:PurposeMatch"/> </xs:sequence>
</xs:complexType>

<xs:element name="PurposeMatch"
  type="PPA:PurposeMatchType"/>
<xs:complexType name="PurposeMatchType">
  <xs:sequence>
    <xs:element ref="PPA:AttributeValue"/>
    <xs:element ref="PPA:PurposeAttributeDesignator"/>
  </xs:sequence>
  <xs:attribute name="MatchId" type="xs:anyURI"
    use="required"/>
</xs:complexType>

<xs:element name="Permission">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="PPA:PersonalDataSet"/>
      <xs:element ref="PPA:Action"/>  </xs:sequence>
    <xs:attribute name="PermissionId" type="xs:anyURI"
      use="required"/>
  </xs:complexType>
</xs:element>

<xs:element name="PersonalDataSet">
  <xs:complexType>
    <xs:sequence maxOccurs="unbounded">
      <xs:element name="PersonalData">
        <xs:complexType>
          <xs:sequence>
            <xs:element
              ref="PPA:PersonalDataMatch"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="PersonalDataMatch"
  type="PPA:PersonalDataMatchType"/>
<xs:complexType name="PersonalDataMatchType">
    <xs:sequence>
      <xs:element ref="PPA:AttributeValue"/>
      <xs:element
        ref="PPA:PersonalDataAttributeDesignator"/>
    </xs:sequence>
    <xs:attribute name="MatchId" type="xs:anyURI"
      use="required"/>
</xs:complexType>

<xs:element name="Action" type="PPA:ActionType"/>
<xs:complexType name="ActionType">
    <xs:sequence>
      <xs:element ref="PPA:ActionMatch"/>
    </xs:sequence>
</xs:complexType>

<xs:element name="ActionMatch"
  type="PPA:ActionMatchType"/>
<xs:complexType name="ActionMatchType">
    <xs:sequence>
      <xs:element ref="PPA:AttributeValue"/>
      <xs:element
        ref="PPA:ActionAttributeDesignator"/>
    </xs:sequence>
    <xs:attribute name="MatchId" type="xs:anyURI"
      use="required"/>
</xs:complexType>
```

```
<xs:element name="Condition" type="PPA:ConditionType"/>
<xs:complexType name="ConditionType">
    <xs:sequence>
      <xs:element ref="PPA:Expression" />
    </xs:sequence>
</xs:complexType>

<xs:element name="Obligation" type="PPA:ObligationType"/>
<xs:complexType name="ObligationType">
    <xs:sequence>
      <xs:element ref="PPA:Notify" minOccurs="0"
        maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ObligationId" type="xs:anyURI"
      use="required"/>
    <xs:attribute name="FulfillOn" type="xs:string"
      use="required"/>
</xs:complexType>

<xs:element name="Notify" type="PPA:NotifyType"/>
<xs:complexType name="NotifyType" mixed="true">
    <xs:complexContent mixed="true">
      <xs:extension base="PPA:AttributeValueType">
        <xs:attribute name="NotifyId"
          type="xs:anyURI" use="required"/>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>

<xs:element name="P-PAIdReference" type="xs:anyURI"/>

<!- 지면 관계상 생략되는 엘리먼트들은 다음과 같다.
  P-PASetIdReference, RoleIdReference,
  P-PermissionSetIdReference, P-PermissionIdReference,
  VariableDefinition, Expression, VariableReference, Apply,
  RoleMatch, AttributeValue, AttributeSelector,
  PurposeAttributeDesignator,
  EnvironmentAttributeDesignator,
  PersonalDataAttributeDesignator,
  AttributeDesignator,
  ActionAttributeDesignator 엘리먼트들은
  지면관계상 명세서를 생략 ->

</xs:schema>
```

〈著者紹介〉

이 영 록 (Young-lok Lee) 정회원
1986년 2월 : 전남대학교 계산통계학과 학사
1990년 2월 : 전남대학교 전산통계학과 석사
2003년 2월 : 전남대학교 전산학과 박사
2003년 3월~현재 : 전남대학교 시스템보안연구센터 연구교수
<관심분야> 개인정보보호, 유비쿼터스 컴퓨팅, 보안정책 및 지침

박 준 형 (Jun-hyung Park) 정회원
2000년 8월~2006년 2월 : 전남대학교 시스템보안연구센터 연구원
2006년 2월 : 전남대학교 대학원 정보보호협동과정 박사
2006년 3월~2007년 2월 : 피츠버그대학교 LERSAIS 연구소 박사후연구원
2007년 3월~현재 : 전남대학교 시스템보안연구센터 연구교수
<관심분야> 디지털포렌식, 악성봇넷 탐지

노 봉 남 (Bong-nam Noh) 종신회원
1978년 2월 : 전남대학교 수학교육 학사
1982년 2월 : 한국과학기술원 석사
1994년 2월 : 전북대학교 정보보호 전공 박사
1983년 9월~현재 : 전남대학교 전자컴퓨터공학부 교수
2000년 8월~현재 : ITRC 시스템보안연구센터 센터장
<관심분야> 디지털포렌식, 유닉스/리눅스 보안, 데이터베이스 보안

박 해 룡 (Hae-ryong Park) 종신회원
1999년 2월 : 전남대학교 수학과 학사
2001년 2월 : 서울대학교 수학과 석사
2006년 8월 : 전남대학교 정보보호협동과정 박사
2000년 12월~현재 : 한국정보보호진흥원 선임연구원
<관심분야> 전자서명 알고리즘/암호프로토콜 설계 및 분석

전 길 수 (Kil-su Chun) 종신회원
1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
<관심분야> 암호학, PET, Digital ID Management