韓國IT서비스學會誌
第5卷 第3號
2006年 12月

공공기관의 특성을 고려한 PMI기반의 XML 접근제어 모델에 관한 연구*

조창희** · 이남용***

A Study of the PMI-based XML Access Control Model in Consideration of the Features of the Public Organization*

Chang-Hee Cho** · Nam-Yong Lee****

■ Abstract ■

The local public organizations, to secure the Confidentiality, Integrity, Authentication and Non-Repudiation of cyber administrative environment is giving it a try to consolidate the official documents among them by standardizing all the documents into XML formats together with the establishment of the GPKI(Government Public Key Infrastructure). The Authentication System based on the PKI(Public Key Infrastructure) used by the GPKI, however, provides only the simple User Authentication and thus it results in the difficulty in managing the position, task, role information of various users required under the applied task environment of public organizations. It also has a limitation of not supporting the detailed access control with respect to the XML-based public documents.In order to solve these issues, this study has analyzed the security problems of Authentication and access control system used by the public organizations and has drawn the means of troubleshoot based on the analysis results through the scenario and most importantly it suggests the access control model applied with PMI and SAML and XACML to solve the located problem.

Keyword : Privilege Management Infrastructure, Security Assertion Markup Language, Government Public Key Infrastructure, eXtensible Access Control Markup Language

* 본 연구는 숭실대학교 교내연구비 지원으로 수행되었습니다.
** 법제처 컴퓨터담당 사무관
*** 숭실대학교 컴퓨터학부 교수

1. 서 론

국내공공기관의 인증 및 접근제어 시스템은 사용자관리 및 접근권한관리 정책이 기관별, 업무별로 구성되었으며, 이를 각 기관에서 분산·운영하고 있다. 이러한 시스템의 사용자들이 업무를 수행하기 위해서는 접근제어시스템의 인증을 거쳐 정보시스템 내부의 접근권한관리 정책에 의해 접근할 수 있도록 사용자 인증 및 접근권한을 부여받아야 한다. 최근에는 공개키 기반의 인증시스템이 범용 적으로 사용됨에 따라 공공기관에서는 인증 및 접근제어 시스템을 공개키 기반의 행정전자서명인증체계(GPKI : Government Public Key Infrastructure)와 연동하여 인증을 시행하고 있다. 하지만 행정전자서명인증체계는 신원확인을 위한 간단한 사용자 인증 수준에 머물고 있어 다양한 행정업무 환경에서 요구되는 접근권한, 역할정보 등을 효율적으로 관리하기에는 부족한 실정이다[5].

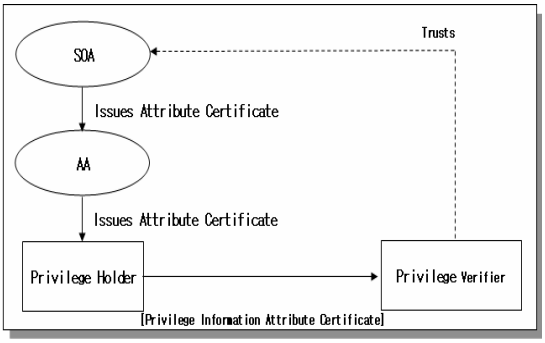
이러한 한계점을 해결하기 위하여 정부 및 연구기관에서는 조직의 임무, 지위, 역할 등 다양한 속성정보에 대한 인증을 제공하는 X.509 속성인증서를 이용하는 PMI의 도입과 공공기관의 인증 및 접근제어시의 보안문제점을 해결하기 위한 표준 인증기술과 접근제어기술에 관한 연구가 진행중이다. 하지만, 공공기관에 적합한 PMI 기술과 XACML과 두 기술의 연동에 관한 연구가 미흡한 상태이기 때문에 이에 대한 추가적인 연구가 필요한 상황이다[4].

본 논문에서는 공공기관의 안전한 접근제어를 위하여 공공기관의 프로젝트 수행 시 발생할 수 있는 시나리오를 작성하고 그 내용을 바탕으로 공공기관에서 발생할 수 있는 인증 및 접근제어 문제점을 도출하였다. 그리고 이러한 문제점의 해결을 위하여 공공기관의 특성을 고려하여 X.509 속성인증서와 OASIS(The Organization for the Advancement of Structured Information Standards)의 XML 인증 및 접근제어기술 표준인 SAML과 XACML을 연동한 PMI기반의 XML 접근제어 모델을 제시하였다.

2. 관련연구

2.1 PMI(Privilege Management Infrastructure)

PMI는 인증서 구조에 사용자에 대한 속성 정보를 제공하여 권한 관리가 가능하도록 하는 속성인증서 기술과 속성 인증서를 발급, 저장, 유통을 제어하는 기반구조이다. PKI가 단순한 사용자의 신원확인만을 제공하는 여권이라면 PMI는 사용자의 속성정보를 통해 다양한 접근제어가 가능한 비자와 같은 역할을 수행한다. 이러한 속성 인증서가 정보보호 메커니즘으로 활용되기 위해서는 속성 인증서의 발급, 저장, 유통이 속성 인증서 생성 기관, 속성 인증서 소유주, 응용 서비스 시스템 등에서 원활히 동작할 수 있어야 한다[11, 16]. PMI는 속성 인증서의 발급, 저장, 유통, 검증 등을 포괄하는 권한관리 기반구조로서 PMI를 구성하는 다양한 방법에 의해서 속성 인증서의 활용 방식과 응용 서비스 환경이 영향을 받게 된다. [그림 1]은 PMI의 구조를 표현하고 있다[1].



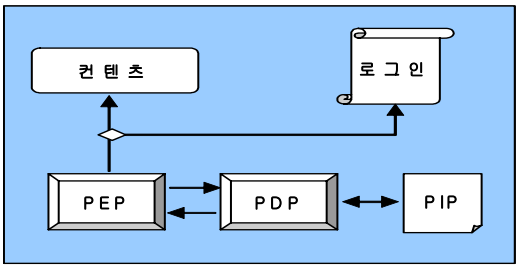
[그림 1] PMI의 구조

SOA(Source Of Authority)는 전자서명기반의 루트CA(Certificate Authority)와 유사한 역할을 하는 기관으로 Privilege Verifier가 신뢰하는 속성인증기관이다. AA(Attribute Authority)는 SOA

로부터 권한의 전부 또는 일부를 위임받아 속성인증서 발급업무를 수행한다. Privilege Holder는 인증서를 통해 AA로부터 권한에 대한 소유권을 보증 받은 자로서 전자서명기반의 End-Entity에 해당한다. Privilege Verifier는 속성인증서를 받아 권한을 판별한다[16, 2].

2.2 SAML(Security Assertion Markup Language)

SAML은 보안 정책을 표현하는 XACML과 함께 사용되며 인터넷상에서의 인증, 권한 부여 및 승인 정보 교환 서비스를 가능하게 해 주는 OASIS의 XML기술이다. SAML의 장점은 XML을 기반으로 하여 XML의 장점을 사용할 수 있다는 점과 한번 인증정보를 입력하면 다른 다양한 영역에서도 인증을 받을 수 있는 싱글사인온(SSO : Single Sign On)이 가능하다는 점, 그리고 SOAP이나 ebXML 등의 프로토콜과 함께 사용할 수 있다는 점 등을 들 수 있다[13, 6].

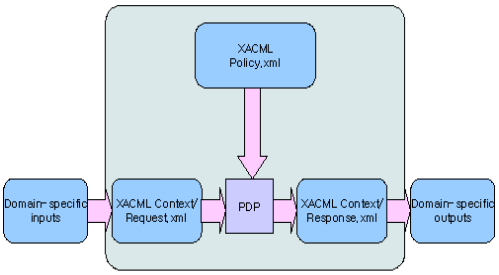


[그림 2] SAML 권한결정 예시

[그림 2]는 SAML 권한결정 예시이다. SAML이 설치된 인증 담당 애플리케이션에 SAML 토큰을 전송하게 되면, PEP(Policy Enforcement Point)는 권한부여요청에 응답하고 권한부여 결정을 받아 시행하는 역할을 한다. PEP는 PDP(Policy Decision Point)에게 권한부여요청을 보내게 되고, PDP는 PIP(Policy Information Point)에 저장되어 있는 보안 정책을 이용하여 권한부여결정 작업을 수행한다. 그러면 PDP는 Authorization decision Assertion을 반환하게 된다. 권한이 주어지면, 사용자의 SAML 토큰에 Assertion attribute가 추가되어, 자원에 대한 접근 권한을 얻게 된다[14, 8]. 권한이 주어지지 않으면 이를 얻기 위해 로그인 화면으로 이동하게 할 수도 있다.

2.3 XACML(eXtensible Access Control Markup Language)

OASIS의 XACML은 접근제어 정책을 통해 보안이 요구되는 자원에 대해 상세한 접근제어 서비스를 제공 할 수 있는 XML 기반의 언어이다[17]. XACML의 정의에 따라 각각의 사용자 별 XML 데이터 접근 정책을 수립하고 적용 할 수 있다. SAML과 함께 주로 사용되며 XML 기반으로 되어있어 다양한 시스템 사이에서 접근제어정책을 기술한다. XACML은 개발자들이 웹을 통해 어떤 사용자들이 접근할 수 있는 지를 결정하는 정책을 기술할 수 있도록 접근제어언어와 요구/응답 언어를 포함하고 있다. 다음 [그림 3]은 XACML에서 정의하는 표준 영역을 나타낸 것이다.



[그림 3] XACML 정책결정

XACML에서 정의하고 있는 부분은 [그림 3]에서의 어두운 부분으로 정책 언어와 응답/요청 언어임을 알 수 있다. 또한, 요청 언어의 문맥으로 들어온 요청을 정책 언어로 기술된 정책들을 기준으로 처리하고 다시 응답 언어로 그 결과를 생성하는 정책 결정 부분 등이 표준에 기술되어 있다[6, 12].

3. 공공기관의 인증 및 접근제어시스템의 보안 문제점 도출

현재 공공기관의 대부분의 정보시스템은 시스템을 유지관리하고 지원하는 주관기관이 있고, 실제로 해당 시스템을 이용하는 사용자 기관이 따로 있다. 이 경우 사용자와 기관별로 권한관리 담당자를 두어야 한다. 이 때 직원 인사이동으로 권한관리담당자가 변경 되었을 경우 해당 업무별로 문서처리를 해야 하며, 계정을 신규로 부여하거나 기존의 계정을 승계하는 방법을 취해야 하는데 이는 오용 및 도용의 위험이 발생될 수 있다. 본 절에서는 공공기관의 부처 간 EA(Enterprise Architecture)구축 프로젝트 시나리오를 작성하여 이를 바탕으로 공공기관의 인증 및 접근제어 시 주요 보안문제점을 분석하고 문제점이 해결될 수 있는 방안을 제시하였다.

3.1 시나리오를 통한 보안 문제점 도출

다음은 공공기관에서 일어날 수 있는 시나리오로서 이를 기반으로 인증 및 접근제어 관점에서 발생될 수 있는 문제점을 도출하였다.

3.1.1 시나리오를 위한 배경

“정부는 시범 사업의 일환으로 행정 자치부와 정보통신부의 EA구축 프로젝트를 통해 공공기관으로 EA를 확대하는 프로젝트를 계획하였다. 그러나 EA구축을 위한 기본 프레임워크의 구축을 위해서는 프로젝트의 특성상 참조모델, 관련지침 및 표준, EA 산출물 메타모델 작성을 위해서는 각 부처의 기술인력 및 부처 간 자료의 긴밀한 협조가 필요하며, 프레임워크를 설계하기 위한 외부 전문가의 참여도 필요한 상황이다. 따라서 각 부서별, 외부인력에 관한 데이터, 산출물, 권한 및 역할설정에 대한 문제가 발생하며 이를 해결하기 위하여 공공기관의 특성을 고려한 인증 및 접근제어 시스템 구축이 필요한 상황이다.”

이와 같은 배경을 바탕으로 프로젝트 구축 시 발생할 수 있는 시나리오를 작성하여 보안문제점을 도출하였다. 작성된 세 가지 시나리오는 현재 행정자치부에서 사용하고 있는 권한관리 시스템과 보안 기술의 한계점을 분석한 후에 작성된 것이다. 그리고, 시나리오를 통하여 EA 구축시점 뿐 아니라 운영 시에도 발생할 수 있는 보안문제점을 도출하였다.

3.1.2 시나리오 작성

공공기관에서 사용하고 있는 주요 보안 문제점을 시나리오의 형태를 통해 제시하였다.

[시나리오 1] 공공기관의 각 부서에 대한 권한 할당 및 접근제어

프레임워크모델을 설계하기 위해 각 부서담당자와 외부 모델링 전문가들은 조직의 업무와 시스템을 구성하는 데이터 및 정보를 종합적인 관점에서 표현하기 위해서 각 기관에 자료를 요청하였다. 하지만 요청을 받은 각 기관은 현재 사용하는 인증시스템을 통해서는 모든 자료에 대한 개별 접근권한을 주기에는 보안상 어려움과 권한관리의 복잡성으로 인하여 이를 대처할 수 있는 인증 및 접근제어 시스템이 필요하게 되었다.

[시나리오 2] 외부 전문가 도입

EA 구축 컨설팅 전문가인 이 교수는 정보통신부의 요청에 의해 EA프로젝트에 참여하게 되었다. 이 교수는 컨설팅을 하기 위해 필요한 문서자료와 기술현황 및 사용 장비에 대한 권한을 정보통신부와 행정자치부에 요청하였고 공공문서의 전자포맷 표준인 XML 문서로 자료를 전송받았다. 그러나 공공기관의 XML 문서는 엘리먼트별 혹은 페이지별로 보안 사항이 있어서 이 교수가 원하는 정보 중 일부는 볼 수 없게 되었다. XML 문서를 재요청하거나 복잡한 보안허가 절차에 따라 XML 문서에 접근하는 불편함으로 인하여 프

로젝트의 일정이 지연됨에 따라 기존의 인증 및 접근제어 시스템에 XML 문서에 대한 접근제어 기술이 추가로 필요하게 되었다.

[시나리오 3] 내부 보안문제 해결

행정자치부 김 차장은 프로젝트를 진행하기 위한 행정자치부의 책임자로, 내부적으로는 행정자치부의 내부보안을 담당하며 외부적으로는 EA구축을 위한 협조의 책임을 가지고 있다. 행정자치부에서는 현재 EAM시스템과 GPKI를 연동하여 사용하고 있으며 이를 통하여 내·외부적 보안 문제점을 모두 해결하려 한다. 그러나 각 조직 및 인원에 관한 속성인증서 발급 문제와 XML 문서의 접근제어에 관한 문제점을 해결하기에는 부족하여 이를 대체할만한 인증 및 접근제어 시스템이 필요하게 되었다.

3.2 보안 요구사항

제시한 시나리오에서 안전한 시스템의 구축을 위해서는 다음과 같은 보안요구사항이 충족되어야만 한다. 첫째, 각 부처의 유연한 정보공유가 가능하여야 하며 외부 전문가 도입에 따른 인증 및 접근제어가 완벽히 이루어 져야 한다. 둘째, 각 부처에서 현재 사용하고 있는 보안 기술이 EA구축 시 필요한 보안 및 인증을 모두 만족하는지를 확인해야 한다. 셋째, EA 구축 시 외부 전문가 및 새로운 인력도입에 따른 권한할당 등 시스템 구축 및 운영에 관한 보안 사항을 점검해야 한다. 결국 통합 프레임워크를 구축하기 위해서는 부서별로 데이터, 산출물, 사용자의 권한 및 역할할당에 관한 문제점을 해결하여야 하며 이를 위하여 공공기관의 특성을 고려한 인증 및 접근제어 시스템이 필요한 상황이다.

3.3 시나리오에서 도출된 보안 문제점 및 해결방안

[문제점 1] “시나리오 1”, “시나리오 2”에서는 공공기관의 XML 문서에 대한 접근권한 관리 시 현재의 접근제어기법으로는 단순한 허가, 거부는 가능하지만 XML 문서에 대한 보안과 XML 문서에 대한 상세한 접근제어를 지원하지 못한다는 문제가 발생한다.

[문제점 1의 해결방안] 기존 공공기관의 접근제어 기법인 강제적 혹은 임의적 접근제어 기법을 통해 공공기관의 XML 문서에 대한 접근제어를 할 경우 XML 문서에 대한 허가, 거부 같은 단순한 접근권한관리는 가능하지만 XML 문서내의 엘리먼트별 상세한 접근제어는 불가능하다. XML 문서의 상세한 접근제어를 위하여 XML접근제어 기술 표준인 XACML을 적용하여 XML 문서에 대한 동적인 권한관리를 수행하도록 한다. 이는 각각의 사용자별, 역할별 인증 정보를 바탕으로 접근제어 정책에 따라 접근권한을 평가하며 XML 문서의 상세한 접근을 가능하게 함으로써 문제를 해결한다.

[문제점 2] “시나리오 3”에서의 행정자치부에서 사용하고 있는 EAM시스템과 GPKI를 이용한 인증방식은 단순한 신원확인은 가능하지만 공공기관내의 직무, 지위, 역할 같은 다양한 속성정보가 필요한 인증 시에 적용하기에는 비효율적이다. 또한 인증된 사용자에게 개별 XML 문서에 대한 접근권한을 재할당해야 하는 문제가 발생한다.

[문제점 2의 해결방안] EA도입과 함께 정부조직의 변화에 따라 기존의 관료제적인 정부조직과 신축적인 정부조직을 위한 다양한 인증이 필요하게 되었다. 현재 사용되고 있는 국내 행정기관의 인증기반인 GPKI는 단순한 신원확인은 지원하지만 행정기관내의 임무, 지위, 역할 등과 같은 다양한 속성정보에 대한 인증기능의 제공에는 한계가 있다. 따라서 이를 해결하기 위해 기존의 공개키 인증서는 그대로 활용하여 신원확인을 하며, 사용자의 속성정보에 대한 인증을 제공하기 위해 속성인

증서를 제공하며, 속성인증서와 공개키 인증서가 병행하여 사용할 수 있도록 하였다. 그리고 인증이 된 부서 및 권한획득자에게 인증정보를 접근제어 서버로 보내어 접근제어 서버가 요청받은 인증정보를 바탕으로 XML 문서에 관한 상세한 접근제어를 가능하게 하여 필요한 정보만을 제공하도록 하여 보안문제를 해결한다.

[문제점 3] “시나리오 1”, “시나리오 2”, “시나리오3”에서의 EA 구축을 위한 공공기관간의 웹서비스를 연동할 경우 현재의 인증 보안 시스템은 동일한 서비스에 대하여 한번 의 인증이 아니라 여러 번의 사용자 인증을 거쳐야 하므로 보안시스템의 유연성이 부족하다.

[문제점 3의 해결방안] EA 프레임워크에서는 업무와 정보시스템의 연계를 위하여 다수의 기관 및 부처 간의 웹 서비스 연동에 대한 요구가 예상된다. 현재의 인증보안시스템은 SSO를 적용하지만 개별 XML 문서 및 XML 엘리먼트별 내용에 대해서 한 번의 인증으로 정의된 보안 정책에 따라 정해진 시간 동안 유효한 인증을 받기에는 한계가 있으므로 SAML과 XACML을 연동하여 이러한 보안문제점을 해결한다.

4. 공공기관의 특성을 고려한 PMI 기반의 XML접근제어모델

4.1 공공기관의 특성을 고려한 접근제어모델의 개요

앞에서 살펴본 바와 같이 공공기관에서 기존의 인증기술을 사용한 단순한 신원 확인 시에는 보안문제점이 발생하지 않지만 다양한 역할별 권한 할당, 복잡한 접근제어정책관리, XML 문서의 상세한 접근 제어시에는 보안문제점이 발생 할 수 있다. 사용자의 접근권한은 권한 관리 프로세스를 통하여 자원에 대한 접근허가 및 접근범위가 결정되며 이는 세 단계로 구성된다. 첫째, 공개키 인증서를 사용하여 사용자의 신원을 확인한다. 둘째, 사용자의 속성정보를 각 조직에서 발급한 속성인증서를 사용하여 등급별, 역할별 접근 권한을 결정한다. 셋째, 접근권한이 접근제어 정책에 위배되지 않는지를 검토하여 자원 및 XML 문서에 대한 상세한 접근제어를 결정한다[3].

4.2 제안한 모델링을 위한 가정

모델링을 위한 가정은 앞에서 제시한 시나리오를 바탕으로 모델링을 위해, 공공기관에서 필요한 가정 사항을 도출해 나타낸 것이다.

[가정 1] 현 전자정부는 공개키 기반 인증시스템에서 속성인증서를 사용한 PMI 인증시스템을 도입할 것이다.

[가정 2] 자정부 도입에 따라 공공기관에서 각 부처의 문서 형태는 XML형태로 단일화 될 것이다.

[가정 3] 부처의 문서 형태가 XML형태로 단일화 됨에 따라 XML관련 보안 기술의 연구 및 필요성이 제기 되었다.

[가정 4] 지식정부를 위한 조직 변화에 따라 기존의 관료제적인 정부 조직에서 신축적인 정부 조직으로의 변화에 따라 역할 기반의 접근제어 모델의 도입이 필요하게 되었다.

[가정 5] 인터넷 및 분산시스템의 발전에 따라 정부 및 기업/전문가 집단에서 그리드 컴퓨팅 환경의 도입에 관한 연구를 하고 있다. 이러한 연구를 바탕으로 기업뿐 아니라 정부 및 각 공공기관에서 그리드 컴퓨팅 환경이 도입될 전망이며, 공공기관의 그리드 컴퓨팅 환경을 안전하게 지원하는 보안 기술이 필요하게 될 것이다.

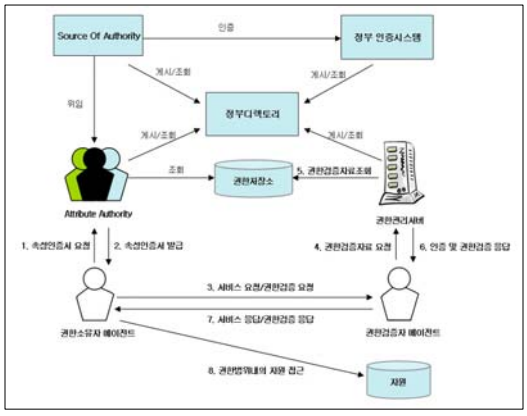
4.3 PMI기반의 XML접근제어모델

정부의 행정전자서명인증체계(GPKI)와 연동하여 속성정보를 이용한 권한관리가 가능한 PMI를 적용한 권한인증모델을 기반으로 하여 XACML 기술을 적용한 PMI 기반의 XML 접근제어 모델을 제시한다. 이를 통하여 웹환경에서 공공기관의 XML 문서에 대한 상세한 접근제어 및 권한관리가 가능하다.

4.3.1 PMI를 적용한 권한인증모델

공공기관의 권한관리를 위한 PMI모델은 [그림 4]와 같으며, 기존의 행정전자서명인증체계와 연동하기 위해 PMI의 핵심 구성요소인 권한소유자 에이전트(Privilege Holder), 권한검증자 에이전트(Privilege Verifier), 권한관리서버(Privilege Manager), SOA(Source of Authority), AA(Attribute Authority)와 전자서명인증서를 발급하는 정부인증시스템과 인증서와 인증서폐지목록을 게시하는 정부 디렉토리로 구성된다.

권한저장소는 정부디렉토리 및 통합권한저장소와 연계하여 사용자정보와 권한정보를 저장한다. 또한 전자서명인증서, 속성인증서 그리고 인증서폐지목록도 함께 저장한다. 권한관리서버는 권한관리정책을 적용하고 관리하며 SOA/AA는 권한정책을 통해 속성인증서를 발급한다. 권한검증자



[그림 4] PMI를 적용한 권한인증 모델

에이전트는 정보시스템 각각에 대해 에이전트를 설치하여 권한정보를 검증하는 역할을 수행한다. 권한소유자 에이전트는 표준 권한관리체계를 사용하는 모든 사용자 정보시스템에 각각 설치되어 인증 및 서비스 요청을 수행한다. PMI를 적용한 권한인증모델에서 사용자가 정보시스템에 접근하기 위한 권한인증 처리흐름은 [그림 4]와 같다.

1) 권한소유자 에이전트는 속성인증서 요청형식을 작성하여 AA에게 속성인증서의 발급을 요청한다.
2) AA는 각 사용자에 대한 권한정책을 참조하여 속성인증서를 권한소유자 에이전트에게 발급한다.
3) 권한소유자 에이전트는 신원인증을 위한 전자서명인증서와 속성정보를 통한 권한관리를 위한 속성인증서를 사용하여 권한검증자 에이전트에게 자원에 대한 접근서비스의 요청 및 권한에 대한 검증을 요청한다.
4) 권한검증자 에이전트는 사용자의 접근서비스를 검증하기 위해 사용자에 대한 신원인증과 권한검증을 위한 자료를 권한관리서버에게 요청한다.
5) 권한관리서버는 사용자에 대한 인증 및 권한검증을 위해 권한저장소에 접근하여 자료를 수집하며, 경우에 따라서는 정부디렉토리까지 접근하여 필요한 자료를 수집한다. 그리고 권한관리서버는 자신이 갖고 있는 SOA의 속성인증서와 권한검증자 에이전트가 전달한 최상 위 인증기관 속성인증시스템의 속성인증서를 비교하여 검증한다.
6) 권한검증자 에이전트는 권한관리서버로부터 인증 및 권한검증을 위한 정보를 수신하여 권한소유자 에이전트가 요청한 권한에 대한 검증을 완료한다.
7) 권한검증자 에이전트는 접근서비스의 응답 및 권한에 대한 검증결과를 권한검증자 에이전트에게 전달한다.

8) 권한소유자 에이전트는 권한검증결과를 받은 후에 권한정책에서 주어진 권한소유자의 권한 범위내의 자원을 접근한다.

4.3.2 PMI기반의 XML 접근제어모델

공공기관에 PMI를 적용한 인증모델은 공공기관의 특성 및 보안요구사항에 따라 다양하게 설정가능하다. [그림 4]의 PMI를 적용한 권한인증모델의 여러 구성개체들은 사용자가 실제로 업무에 접근할 경우 관계되는 항목들이다. 모델설계에서는 주로 권한관리제어 프로세스와 밀접하게 관련된 세 개의 구성개체인 권한관리서버, 권한검증자 에이전트, 권한소유자 에이전트로 접근제어모델을 설계하였다.

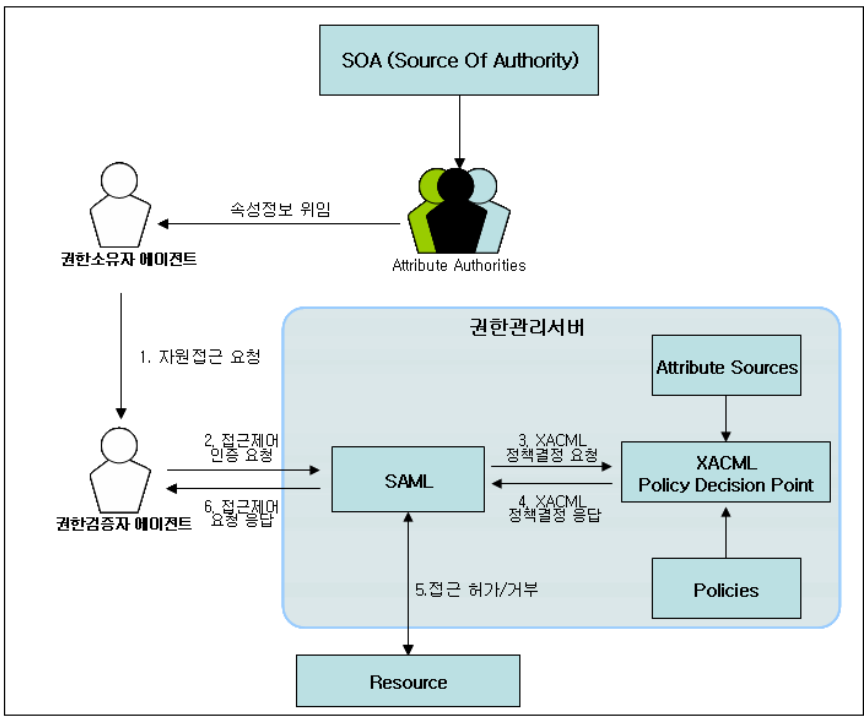
[그림 5]는 본 논문에서 제시하는 XACML을 적용한 PMI기반의 XML 접근제어모델이다. 모델을 구성하는 권한소유자 에이전트, 권한검증자 에이전트, 권한관리 서버의 주요 기능은 다음과 같다.

권한소유자 에이전트는 사용자에 대한 인증정보를 생성하고 사용자가 접근하려는 객체에 대한 권한정보를 권한검증자 에이전트에 전달하는 역할을 한다.

권한검증자 에이전트는 권한소유자에 대한 권한정보를 확인, 권한소유자가 해당 객체에 접근할 수 있도록 권한관리서버에 접근제어를 요청한다.

권한관리서버는 SAML, PDP, Attribute Sources, Policies로 구성되며 사용자의 권한정보 관리, 권한검증을 위한 환경변수 관리, 접근제어 정책 관리, 역할 및 객체와 관련된 환경변수 관리, 역할관리를 한다.

가) SAML은 사용자의 인증 여부, 요청이나 응답의 구성형식등을 확인하며 사용자로부터 받은 자원접근요청을 XACML PDP에 전달하고



[그림 5] PMI기반의 XML접근제어모델

자원접근응답을 변환한다.

나) PDP는 SAML로부터 권한요청을 받아 모든 속성정보과 적용가능한 정책의 조합에 관하여 평가하여 결과에 대한 정보를 리턴 한다. PDP는 적용 가능한 정책을 찾고 필요한 속성들을 검색한다. 정책안에는 많은 규칙이 존재하는데 규칙이 하나가 아니라 다수일 때는 각 규칙들의 결과들을 rule combining algorithm을 통하여 조합하여 결과를 생성한다. 정책의 경우는 policy combining algorithm이 있어 권한요청에 해당하는 정책들의 결과를 조합하여 평가한다. 그리고 의무조항을 포함한 정책은 의무조항을 실행하지 않거나 의무조항을 이해할 수 없다면 정책에 대한 결과는 거부가 된다. PDP는 이러한 권한부여 결정과 의무조항을 포함하여 SAML에 전송한다[17, 10].

다) Attribute Sources, Policies는 [그림 4]의 정부 디렉토리 및 권한저장소에 저장된다. Attribute Sources는 권한 속성으로서 사용자는 권한이 있는 자원에 대하여 속성을 게시하여 권한관리를 할 수 있다. Policies는 권한정책으로서 권한 속성을 기반으로 하여 접근결정을 하며, 발행자의 속성을 결정하고 속성에 대한 위임과 사용에 대한 방법에 대해 규정할 수 있다. 권한정책은 XML 문서에 대한 동적인 접근제어 정책 및 권한관리를 위하여 XACML규칙으로 생성되어야 하며 정보자원관리자와 이해관리자의 자원에 대한 사용을 최종적으로 제어한다[7, 9, 18].

[그림 5]의 화살표의 번호는 일반적인 접근 요청과 권한부여 순서를 나타낸다. 권한소유 에이전트가 권한검증 에이전트에 자원 접근을 요청하게 되면, 권한검증 에이전트는 사용자의 인증 정보를 요청하며 사용자는 인증 정보를 권한검증 에이전트에 전달한다. 권한검증 에이전트는 인증정보를 SAML로 보내며 SAML은 사용자의 인증정보를 확인하고 사용자에게 자원 접근에 관한 정책을 결정하기 위해 PDP로 정보를 보내 사용자 별 정책을 결정하게 한다. PDP로부터 정책에 관한 결정을 응답 받은 XACML권한모듈은 자원에 관한 접근 허가/거부를 정책 및 속성에 따라 사용자/엘리먼트별로 구분하여 사용자의 자원 접근에 대한 권한을 할당한다[3, 15].

4.4 문제해결 및 적용방안

4.4.1 공공기관의 보안 문제점 해결방안

본 절에서는 현재 공공기관에서 사용하는 GPKI 모델에 대한 보안기술문제는 생략하고 제안한 접근제어모델과 GPKI모델이 유기적으로 동작하는데 문제점을 검토하여 해결방안을 제시한다. 다음

〈표 1〉 보안 문제점 및 해결방안

공공기관의 보안 문제점	적용한 보안기술	모델 제시를 통한 해결방안
웹서비스환경에서 XML을 이용한 다양한 사용자 인증, 권한부여, 승인 정보 교환 불가	SAML과 XACML의 연동	사용자 인증 정보를 SAML을 사용하여 XML로 변환하고 XACML과 사용자의 인증 정보 및 권한 속성의 교환을 통하여 안전한 사용자 인증 제공
자원에 대한 허가 또는 거부 같은 단순한 접근제어를 확장한 XML 문서의 엘리먼트 별 상세한 접근제어 지원 불가	XACML	XML문서의 복잡한 접근제어정책 및 동적 접근 권한결정을 제공하여 XML문서에 대한 상세한 접근제어 지원
동일한 서비스에 대하여 중복된 사용자 인증을 거쳐야 하므로 다양한 서비스간 다른 인증방식의 연동 불가	SAML	보안 서비스를 요구하는 공공기관 시스템간의 표준 인증방식을 제공하여 상호운영성 확보
기존의 공개키 기반의 인증 시스템을 사용하는 경우 공공기관내의 직위, 임무, 역할등과 같은 다양한 속성정보를 이용한 인증시 비효율적	PMI	속성정보 인증을 위하여 PMI역할모델을 적용한 X.509 속성인증서를 사용하여 다양한 속성인증 및 역할기반 접근제어 지원

<표 1>은 공공기관의 보안문제점을 해결하기 위하여 제안한 모델에서 적용한 보안기술과 해결 방안이다.

4.4.2 비교평가

제안한 모델을 인증 및 접근제어관점에서의 비교를 위하여 ISO/IEC15408 : 1999 - Common Criteria(CC)의 키 관리, 인증, 접근제어, 역할관리와 관련된 컴포넌트의 보안기능을 기반으로 평가표를 작성하였다. CC를 기준으로 암호키관리를 위해서는 암호키의 접근 유형에 관하여 명세할 것을 의무화하고 있으며 접근통제와 정보보호통제를 위한 주체와 정보간의 접근 규칙과 보안속성을 시스템에서 설명할 수 있어야 한다. 그리고 사용자 인증을 위한 사용자 보안속성과 인증 메커니즘을 위한 사용자의 그룹, 우선 순위등 에 대하여 권한을 명세해야 한다.

PMI 기반의 XML 접근제어 모델은 기존 모델에 비하여 암호키접근 측면과 보안역할의 할당 및 역할제한에 대한 보안 기능을 제공하는 장점이 있다. 그리고 속성인증서의 역할과 권한의 변경에 대한 관리가 용이하다.

〈표 2〉 제안한 모델의 비교평가

클래스	CC 패밀리	CC 컴포넌트	Easy Access	Cardea	PRIMA	PMI기반의 XML 모델
암호지원 (FCS)	암호키관리 (FCS_CKM)	암호키접근	△	X	△	O
사용자 데이터 보호 (FDP)	접근통제기능 (FDD_ACF)	보안속성에 기반한 접근통제	O	O	O	O
	정보흐름통제기능 (FDP_IFF)	계층적 보안속성	O	△	△	△
식별 및 인증(FIA)	사용자속성정의 (FIA_ATD)	사용자 속성정의	O	O	O	O
	사용자인증 (FIA_UAU)	인증	△	△	O	△
보안관리 (FMT)	보안속성관리 (FMT_MSA)	보안속성관리	△	O	O	O
	보안역할관리 (FMT_SMR)	보안역할	O	△	△	O
		보안 역할의 제한	△	△	△	O
		역할위임	X	X	X	△

※ O : 완벽히 지원, △ : 부분지원, X : 지원하지 못함

<표 2>는 제안한 모델과 기존모델을 CC의 보안기능으로 비교한 것이다.

제안한 모델은 PMI를 기반으로 암호키에 대한 접근 정책과 기술을 제공하고 있다. 기존 모델의 경우 인증을 통해 공개키인증서를 사용하지만 별도로 암호키에 대한 검색과 관리를 위한 기능을 지원하지 않으며 XML 기반 문서에 대한 암호키 관리 문제에 대한 해결책을 제시하지 못하고 있다. 본 논문에서 제안한 모델에서는 암호키의 안전한 사용을 통하여 다양한 인증 접근 방법의 제공과 함께 XML 문서의 암호키 관리시의 효율성을 증대시켜준다.

비교한 모델 중 Cardea와 PRIMA의 경우에는 XACML을 사용하여 속성을 이용한 접근통제를

수행하지만, XACML의 문법적 한계에 의한 역할 구조를 사용하는데 한계가 있다. 제안한 모델에서는 PMI역할모델을 사용함으로서 계층적인 보안 속성을 부분적으로 지원가능하다.

4.4.3 제안한 모델의 기대효과

기존의 공공기관에서 사용하는 보안기술과 제안하는 모델을 연동함으로써 갖는 기대효과는 다음과 같다.

첫째, 기존의 공개키인증서에 추가로 속성인증서를 병행하여 사용함으로 다양한 속성에 대한 인증이 가능해진다. 예를 들어, 해당 분야의 법률 및 규정을 잘 알고 있는 공무원이 퇴직하였을 경우 업무 수행에 관한 문제가 발생할 수 있다. 이런 문제점의 해결을 위해 공공기관 사이트 내에 지식커뮤니티를 구축하여 업무 수행에 필요한 양식과 템플릿뿐만 아니라 지식과 경험을 지식커뮤니티를 통해서 공유를 한다. 하지만 불완전한 정보 혹은 중요한 업무내용에 대해서는 제안하는 PMI 기반의 XML 접근제어 모델을 연동하여 공무원의 역할, 직급 등의 정보를 참조하여 제한적 접근을 허용하여 보안상의 문제를 해결할 수 있다.

둘째, 접근제어정책의 재설정을 통하여 개별 사용자가 자신의 정보 및 자료에 대한 동적인 접근권한관리가 가능해진다. 예를 들어 공무원이 지식경영에 대한 것을 전자정부 포털사이트에서 검색하면 전자정부 포털사이트에 해당분야의 전문가의 프로파일 및 참고자료를 찾을 수 있다. 만약 검색결과에 프로파일 및 자료가 전자정부 포털사이트에 올려지는 것을 원하지 않는다면 프로파일과 참고자료에 접근제어정책을 재설정하면 된다. 이를 통해 보안등급, 사용자, 직위 등에 관한 인증정보를 바탕으로 정보에 대한 동적인 접근권한관리가 가능하다.

셋째, XML 기반 접근제어를 사용함으로써 XML 문서 및 다양한 정보자원에 대한 상세한 접근제어가 가능하다. 예를 들어, 공공기관의 시스템의 내부데이터에는 전사적 데이터 웨어하우스(또는 연계된 데이터 마트)가 있어 재무, 인사, 조달 데이터 뿐만 아니라 고객에 관한 데이터까지 확보되어 있다. 외부 데이터에는 마케팅 동향, 각 부처간의 관련 프로젝트, 구매조달 정보 등이 존재한다. 이러한 내/외부의 데이터에 대한 접근제어를 위하여 각 사용자의 역할, 직급 등을 XACML을 사용한 접근제어관리를 통하여 XML 문서의 엘리먼트별 접근 및 권한충돌방지 등 정보자원에 대한 상세한 접근제어가 가능하다.

5. 결론 및 향후연구

현재 공공기관의 인증을 위한 행정전자서명인증체계는 신원 확인을 위하여 PKI 기반의 사용자 인증을 사용하고 있는데, 이는 다양한 속성정보를 이용한 인증 시 한계점이 있으며 접근권한 및 역할정보 등을 효율적으로 관리할 수 없는 단점이 있다. 그리고 공공기관의 부처별로 독립적으로 접근제어시스템이 구축되고 운영됨에 따라 공공기관을 위한 통합권한관리체계 구축 시에 상호연동성과 호환성에 문제가 발생 할 수 있다. 본 논문에서는 이러한 문제점의 해결을 위하여 다섯 단계를 거쳐 공공기관의 특성을 고려한 PM I기반의 XML 접근제어모델을 제시하였다.

첫째, 공공기관에서 EA 프로젝트시 발생할 수 있는 문제점을 중점으로 시나리오를 작성하였다. 둘째, EA를 위한 공공기관의 특성을 고려하고 사용되고 있는 보안기술을 적용하여 주요 보안요구사항을 도출하였다. 셋째, 도출된 보안요구사항을 해결하기 위하여 표준 인증기술 및 접근제어기술을 적용한 접근제어 모델을 제시하였다. 넷째, 제시한 접근제어모델을 현재 공공기관에서 사용하고 있는 행정전자서명인증체계와 연동 및 개선을 위하여 PMI역할모델을 적용한 속성인증서를 병행하여 사용함으로써 사용자의 다양한 속성정보에 대한 인증이 가능하게 하였다. 다섯째, OASIS의 표준 XML 보안기술인 SAML과 XACML을 연동하여 싱글사인온과 복잡한 권한관리정책관리

및 XML 문서에 대한 상세한 접근제어가 가능하도록 하였다.

향후 연구로는 제시한 모델을 기반으로 OASIS의 XACML과 W3C의 XML 서명, XML 암호화, XKMS(XML Key Management Specification)와 연동을 위한 프로파일의 개발 및 테스트에 관한 연구를 진행할 것이다. 또한 XACML의 표준화 진행에 따른 NIST의 역할기반 접근제어의 단계별 적용에 대한 연구도 병행할 예정이다.

참 고 문 헌

[1] 강명희, "PMI : Privilege Management Infrastructure 개요", *퓨처시스템* Technical Report, June 2002.

[2] 김봉환, 김기수, 원유재 "RBAC을 이용한 PMI기반 권한관리, *한국정보처리학회", 정보처리학회지*, Vol.10, No.2(2003).

[3] 심완보, 박석 "애드호크러시 조직의 특성을 고려한 역할기반모델". *한국정보보호학회, 정보보호학회지*, 12(4), 2002. 8.

[4] 진승헌, 최대선 "속성인증기술과 PMI", *한국정보보호학회, 정보보호학회지*, Vol.10, No.4 (2000).

[5] 추경균, "정부의 행정전자서명인증체계(GPKI) 활성화 및 발전방안", *정보보호학회 논문지*, 2004. 4

[6] 한국전산원, "e-비즈니스 보안인증을 위한통합접근관리방안 연구", 연구용역보고서, 2003. 10.

[7] Ahn, G. and R. Sandhu, "Role-based Authorization Constraints Specification", *ACM Transactions on Information and System Security*, November 2000.

[8] Ahn, G., R. Sandhu., M. Kang, and J. Park, "Injecting RBAC to secure a Web based workflow system", *In Proceedings of 5th ACM Workshop on Role-Based Access Control*, July 2000.

[9] Ferraiolo, D., J. Cugini, and D. RKuhn. "Role Based Access Control : Features and Motivations", *In Annual Computer Security Applications Conference, IEEE Computer Society Press,* 1995.

[10] Hang, L., G. Ahn, and B. Chu, "A Rule-Based Framework for Role-Based Delegation", *In Proceedings of ACM Symposium on Access Control Models and Technologies*, May 2001.

[11] ITU-T, "ITU-T Recommendation X.509. Information Technology : Open Systems Interconnection - The Directory : Public - Key And Attribute Certificate Frameworks", *ITU-T*, 2000.

[12] Markus Lorch, "First Experiences Using XACML for Access Control in Distributed Systems", *ACM Workshop on XML Security*, 2003.

[13] M. Thompson, W. Johnston, S. Mudumbai, G. Hoo, K. Jackson, and A. Essiari. "Certificate-based Access Control for Widely Distributed Resources", *In Proceedings of the 8th USENIX Security Symposium*, August 1999.

[14] Park, J., Ahn, G., and R. Sandhu, "RBAC on the Web using LDAP", *In Proceedings of the 15th IFIP WG 11.3 Working Conference on Database and Application Security*, July 2001.

[15] Park, J., R. Sandhu, and G. Ahn., "Role-based Access Control on the Web", *ACM Transactions on Information and System Security*, February 2001.

[16] S. Farrell and R. Housley, "An Internet Attribute Certificate Profile for Authorization", *PKIX WorkingGroup*, June 2001.

[17] Sandhu. R., “Role-hierarchies and Constraints for lattice-based access control”, *In Proceedings of 4th Enropean Symposium on Research in Computer Security*, 1996.

[18] Sandhu, R., E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role Based Access. Control Model”, *IEEE Computer, February* 1996.

◈ 저 자 소 개 ◈

조 창 희 (cchlaw@paran.com)

현재 숭실대학교 컴퓨터학과 박사과정중에 있으며, 법제처 CIO보좌관, 전산사무관으로 재직하고 있다. 공공기관 SW발주체계관련 현행법제도 조사 및 분석연구, 법령정보 데이터베이스 설계에 관한 연구 등이 주요 연구결과이며, 법령정보시스템 구축에 관한 연구를 한국정보과학회지의 국내 학술지에 발표하였다

이 남 용(nylee@comp.ssu.ac.kr)

현재 숭실대학교 컴퓨터학부 교수로 재직하고 있다. 현대정보기술대학원 (프로젝트관리론) 강사, 국민대학교 경영정보대학 (경영정보/전문가시스템) 강사, 성균관대학교 행정대학원 (컴퓨터시스템감사론) 강사, 건국대학교 경영대학 (전문가시스템/그룹웨어) 겸임교수, 연세대학교 경법대학 (객체시스템/전자상거래) 겸임교수 등의 경력이 있으며, 한국정보통신기술사협회 회장으로 활동 중이다. 최근에는 소프트웨어 테스팅/품질보증, MIS, 정보보호 등을 연구하고 있다.