[정보보호] ITU-T SG17 웹 서비스 정책을 위한 XACML 3.0 표준

개요

XACML(eXtensible Access Control Markup Language)은 SAML(Security Assertion Markup Language)과 함께 주로 사용되며 XML 기반으로 되어있어 다양한 시스템들 사이에서 리소스 접근제어정책(Access Control Policy)를 기술하는 표준이다. XACML은 개발자들이 웹을 통해 사용자들이 어떤 리소스에 접근할 수 있는 지를 결정하는 정책들을 기술할 수 있도록 접근제어언어와 요구/응답 언어를 정의한다. 2013년 1월 OASIS(OASIS Identity in the cloud TC)에서 XACML 3.0이 제정되었다. OASIS에서는 지난 4월 본 표준을 ITU-T 표준으로 상정하였고, ITU-T SG17에서는 XACML 2.0 작업과 유사하게 본문 내용에서 Normative 부분과 Informative 부분을 분류하고 Informative 부분을 부록으로 구성하고, Normative 부분을 ITU-T의 표준 문서양식과 용어에 준하여 보완하여 ITU-T SG17 9월 회의에서 승인요청(Consent)하였다. 본 보고서는 XACML 3.0이 XACML 2.0으로부터 개선된 점과 신규 기능을 소개한다.

XACML 3.0 개선점 및 신규 기능

- **상담 요소 (Advice element)**

  이 새로운 기능은 PEPs(Policy Enforcement Point) 이 명령을 준수하지 않는 예외 의무와 비슷하다. PEPs는 명령문을 고려하거나 취소할 수 있다.

- **사용자 지정 범주 (Custom categories)**

  XACML 3.0에서는 사용자가 자신의 사용자 지정 범주를 생성할 수 있는 옵션이 제공된다. 반면 XACML 2.0의 속성은 제목, 자원, 환경, 행동으로만 구성된다.

- **콘텐츠 요소 (Content element)**

  XACML 2.0 요청에서는 자원 범주 내부에 ResourceContent 요소의 일부로 XML 콘텐츠만 있을 수 있다. ResourceContent 요소는 모든 범주에 표시될 수 있도록 콘텐츠 요소로 일반화 되었다.

- **향상된 프로파일 (Enhanced profiles)**

  - XACML 2.0에 표현된 계층 자원 프로파일이 URI 로 계층 구조를 인코딩 할 수 있도록 새로운 스키마가 허용되도록 개선되었다.
  - 다수의 의사 결정 프로파일: 여러 리소스 요청이(XACML 2.0) 여러 의사 결정 프로파일로 이름이 변경되고 새롭게 개선되었다. 프로파일은 요청자가 (일반적으로 정책 적용 지점: PEP) 하나의 XACML 요청에서 몇 가지 질문을 할 수 있도록 허용한다. PEP와 PDP(Policy Decision Point) 간의 통신 오버헤드를 감소함으로

성능을 개선하였다.

• XACML 요청 및 응답 표현 개선 (Improvement in XACML Request and Response)

사용자 지정 범주를 정의할 수 있듯이, 속성 카테고리의 많은 타입이 XACML 3.0 요청에 표현될 수 있다. XACML 2.0 요청은 단지 제목, 자원, 환경, 행동 범주를 포함할 수 있었다.

• XPath 데이터 유형 지원 개선 (Improvements in XPath)

XPath 데이터 형식이 새롭게 XACML 3.0에 도입되었다. 반면 XACML 2.0의 XPath는 네임 스페이스 접두사가 아직 결정되지 않은 시점에 문자열(String)로 정의가 된다. 또한 다중 결정 스키마 기반의 XPath가 도입되었다.

• 새로운 속성 함수와 데이터 유형 (New attribute functions and datatypes)

XACML 3.0은 속성들과 속성연결(Matching)에 사용할 수 있는 새 데이터 유형 및 기능을 제공한다. 특히 XACML 3.0은 속성을 조작할 수 있는 XPath를 사용한다.

• 새로운 프로파일 (New profiles)

- 위임(Delegation): 어떤 대상에 대하여 누가 정책을 작성할 수 있도록 정책을 정의할 수 있다. XACML에 관리 권한을 위임할 수 있는 능력은 XACML 3.0과 새로운 기능이다. 위임기능은 글로벌 관리자가 제한적인 관리 권한을 로컬 관리자에게 위임할 수 있도록 한다. 예를 들어, 전역 관리자는 조직 내 자원의 전체 집합에 대한 액세스 제어(AC) 정책을 정의할 수 있다. 관리자는 리소스 집합을 관리하는 관리자에게 권한을 위임할 수 있다. 액세스 제어 규칙을 정의하려면 관리자의 권한이 글로벌 관리자가 정의한 위임 정책에 의해 제한된다. 위임은 페더레이션 시나리오, 클라우드 기반 시나리오와 적절한 정책을 정의하기에 로컬 정보가 요구되는 광대한 도메인들 간의 환경에서 매우 유익하게 사용된다.
- XACML 3.0은 엑스포트 규정 준수에 대한 새 프로필이 엑스포트 규정 준수 시나리오에 충족할 수 있는 저자 정책을 돕기 위해 제작되었다. 유사하게, 지적 재산권 관리(IPC)에 대한 새 프로필이 도입되었다.

• 규칙 의무 (Obligations in rules)

XACML 3.0 규칙이 의무를 포함할 수 있다. XACML 2.0 에 대한 개선점 중 하나는 의무식이다. 이것으로 의무 문에 동적 표현식을 추가할 수 있다. XACML 2.0에서는 사용자 전자메일과 의무 요소를 정적으로 정의한다. 그러므로 의무 요소에 전자메일을 정적으로 구성한다는 것은 불가능한 것이다. 의무는 PEP에게 "사용자에게 전자메일을 보내주시기 바랍니다"로 말할 수 있다.

그러나 XACML 3.0에서는 각 사용자의 전자메일은 ObligationExpression 내부표현 요소로 정의할 수 있는 PIP(Policy Information Point) 방식으로 검색될 수 있다. 따라서 의무는 "주소를 user@foo.com로 전자메일을 보내주시기 바랍니다"로 PEP에게 말할

수 있다.

XACML 2.0의 의무는 정책과 정책 세트에 추가될 수 있다. 그러나 XACML 3.0은 규칙은 의무를 포함할 수 있다.

- **정책 조합 알고리즘 (Policy combination algorithms)**

  XACML은 정책이 하나의 결정을 생성하기 위하여 결합되어 있다. 각 정책은 서로 다른 의사 결정으로 이를 수 있다. 이러한 결정은 하나의 결과를 반환하기 위해 결합되어야만 한다. XACML 3.0은 XACML 2.0의 기존 조합 알고리즘을 개선하였다.

- **XPath 식의 범위 (Scope of XPath expressions)**

  XACML 2.0의 XPath 표현식은 XACML 요청의 루트에 적용된다. 그러나 XACML 3.0에서 XPath 표현식은 콘텐츠 요소의 루트에 적용된다.

- **타겟 요소 (Target element)**

  XACML 3.0의 카테고리 요소의 이집적 접속사(or) 및 접속사(and) 함수를 제거하고 AnyOf 및 AllOf 요소를 소개한다. 타겟 요소는 여전히 결합하는 접속기능을 갖는다. 하지만 XACML 2.0은 이미 any-of와 all-of 함수를 정의하고 있으나 동등 내역의 스키마 요소를 갖고 있지는 않다. XACML 3.0 사양은 XACML 3.0의 타켓 요소와 그 하부의 동작을 설명한다.

- **의무 및 정보 요소 변수 (Variables in the Obligation and Advice element)**

  관리자 값은 예를 들어, 정책 정보 포인트(PIP)를 통해 런타임에 결정될 수 있다. 이것은 부정의 경우에 요청자 라인의 관리자에게 전자 메일을 보낼 것을 PEP에게 요청한다와 같은 풍부한 시나리오를 가능하게 한다. XACML 2.0은 디자인 타임에, 이와 같이 요청이 어디에서 왔는지, 또 자신의 라인 관리자가 누구인지 알지 못하기 때문에 대응을 할 수 없다.

향후 전망

일반적으로 대 기업의 보안 정책은 매우 복잡하게 구성되며, 정보시스템 부서, 인사 부서, 법률 관련 부서, 재무부서 등등 여러 부서에 의해 각각 관리되고 있다. 현재 이와 같은 보안정책은 각각의 시스템에서 독립적으로 관리되고 있는 경우가 일반적이며, 이와 같은 보안정책의 수정에는 많은 비용이 소요되거나 신뢰성이 떨어진다. 이러한 문제에 해결점으로 보안정책을 표현할 수 있는 공통적인 언어의 필요성이 높아지고 있다. 만일 기업 전반에 걸친 보안정책이 공통 언어로 구현될 수 있다면, 정보시스템 내의 각 컴포넌트 안에 존재하는 모든 보안정책 조항들의 집행을 총체적으로 관리할 수 있게 된다.

이번 XACML3.0 표준은 그동안 널리 사용되어오던 웹 서비스의 정책 관리(XACML2.0)의 문제점을 개선한 것이다. 또한 OASIS에서 제정한 표준을 ITU-T 에 표준으로 상정한다는 것은 표준의 궁극적인 목적 상호연동을 극대화 하는 방편으로 평가된다. 산업계를 중심으로

작성된 표준이 글로벌 표준기구인 ITU-T를 통하여 새롭게 단장되고 글로벌 표준으로 영향력을 발휘하는 좋은 사례라고 사료된다.

나재훈 (한국전자통신연구원 사이버보안연구단 전문위원, jhnah@etri.re.kr)