情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

안전한 교육정보공유체제를 위한 ID 관리 시스템의 요소 기술 분석 및 요구사항

염 흥 열*

요 약

본 논문에서는 교육정보공유체제를 위한 ID 관리시스템을 위하여 요구되는 표준화 및 기술개발 동향, 국내외 환경, 그리고 사용 시나리오를 분석하고, 교육정보공유체제를 위한 ID 관리 시스템을 위한 소요 보안 핵심 기술과 시스템 요구사항을 제시한다. 본 고의 결과는 안전한 교육정보공유체제를 위한 ID 관리 시스템 설계 시 유용하게 활용될 수 있을 것이다.

Ⅰ. 서 론

인터넷은 중요한 비즈니스, 커뮤니티, 그리고 개인 간의 상호 작용을 위한 수단으로 활용되고 있다. ID (Identification)는 신용카드 번호, 주민등록번호 등 사용자 관련 속성 정보의 집합이며, 이는 신분확인을 위하여 사용된다. 인터넷 활동을 위하여 오늘날 사용자들은 많은 신분확인 정보인 ID를 사용하고 있다. 연계된 ID(federated ID)는 여러 새로운 비즈니스 기회를 제공하는 좋은 수단으로 이용될 수 있다. 이러한 노력중의 하나가 여러 산업체들이 모여서 ID 관리를 수행하고, ID의 상호 연계와 싱글사인온(SSO: single sign-on)을 수행하기 위한 미국의 리버티 얼라이언스(Liberty Alliance) 프로젝트이며,[4,5] 아이디 연계를 지원하기 위한 핵심 표준 중의 하나가 OASIS에서 제정된 SAML 표준과 XACML 표준이다.[1]

안전한 교육정보공유체제는 시도 교육청 등 주체들에 의하여 관리되는 교육 자료를 공유하기 위한 시스템이다. 이러한 시스템을 안전하게 운영하기 위하여 필요한 중요 기술이 사용자 인증 기술이고, 이 기술을 효율적으로 구현하기 위한 기술이 ID 관리 기술이다. ID 관리 기술은 여러 조직에 의하여 운영되는 ID를 연계하여 관리함으로써 다양한 조직의 ID 관리 정책을 반영할 수 있고, 서로 동등한 수준의 사용자 인증을 가능케 하는 기술이다. ID 관리를 위하여 필요한 프레임워크와 기술은 리버티 얼라이언스에 의한 프레임워크와 OASIS에 의한 요소 기술을 각각 들 수 있다.

본 논문에서는 국내 교육정보체제를 위한 ID 관리 시스템을 위한 요구사항을 제시하기 위하여 기존 기술의 동향을 살펴보고, 기술과 연관되는 다양한 요소 기술을 살펴본다.

Ⅱ. 본 론

2.1 ID 관리 시스템

2.1.1 ID 관리 시스템의 정의

2005년도 대한민국 네티즌 보고서에 의하면 인터넷 서비스 이용이 다양화되면서 사용자마다 평균 27.25개의 웹 사이트에 가입하고 있고, 사용자당 평균 7.56개의 ID를 이용하고 있다. 따라서 사용자는 이러한 많은 ID를 관리해야 하는 부담이 있고, ID 도용의 부작용이 나타나고 있다.[2,3] 또한 ID 관리와 더불어 한번 인증 받으면 다시 인증 받지 않고 다른 서비스를 이용할 수 있는 싱글사인온 기능이 필요하며, 장기적

본 논문은 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구 결과로 수행되었음
(IITA-2005-(C1019-0502-0020))
* 순천향대학교 공과대학 정보보호학과(hyyoum@sch.ac.kr)

으로 등급화된 권한 관리 기능을 제공하는 계정 및 접근 관리(I&AM: Identity and Access Management)가 필요하다. 또한 각 조직의 ID 관리 권한을 유지하면서 싱글사이온 기능을 제공할 수 있는 ID 연계가 ID 관리를 위한 핵심기술로 대두되고 있다. 인터넷 사이트 이용이 빈번하게 일어나고 있고, ID 도용의 피해 사례가 증대되고 있으며, 개인정보의 불법적인 접근과 유통의 피해가 증대되고 있음을 고려하면 효율적이고 안전한 ID 관리는 매우 중요하다. ID 관리 서비스는 안전하고 편리한 인터넷 상의 거래를 위하여 다양한 웹 사이트에 산재해 있는 사용자의 ID와 개인정보를 안전하게 보호 및 관리하는 서비스이다. 관리되는 디지털 ID는 사이버 공간상에서 개인 식별을 가능케 하는 주민등록번호, 전자우편 주소, 계좌번호, 신용카드 번호 등을 들 수 있다. 인터넷 상에 ID 관리는 크게 중앙 집중 방식과 연계된 방식으로 구성될 수 있다. 중앙 집중화된 방식은 하나의 중앙 집중 인증 서버를 두고 관리하는 방식이고, 연계된 방식은 여러 조직이 분산된 인증 서버를 두고 서로간의 전자거래를 가능케 하는 방식이다. 이의 특징은 〔표 1〕과 같다.

〔표 1〕 인터넷 ID 관리 서비스 모델 비교

특징	중앙집중 방식	연계된 방식
응용 범위	• 기업내 그룹웨어 • 하나의 조직을 위한 사이트들로 구성됨	• 조직 간에 연계된 사이트 간에 제공됨 • 사이트 간에 협업/연계가 필요한 경우 적합함
방법	• 하나의 인증을 위한 크리덴셜 데이터베이스를 이용함	• 기존에 등록된 사용자 계정을 서로 연결하여 사용함
특징	• 다양한 ID 정책 수용 불가능 • ID 정보 관리의 자치권 확보 불가능 • 전용의 싱글사인온 제공 가능 • 단순한 구조 • 프라이버시 문제	• 다양한 ID 정책 수용 가능함 • ID 정보 관리의 자치권 확보 • 인터넷 상에서 대규모의 싱글사인온 기능 구현 가능 • 사이트간에 새로운 비즈니스 창출 가능

2.1.2 ID 관리 표준 및 기술개발 동향

현재 ID 관리를 위한 표준 기술은 여러 다양한 ID 관리를 위한 표준이 SAML v2.0으로 통합되고 있고, 특히 리버티 연계에서는 SAML v2.0을 채택하고 있으며, OASIS에서는 2005년 3월 버전 2.0 SAML을 승인하였다. 기술 개발 동향을 살펴보면 2004년부터 2008년까지 수행될 예정인 PRIME(Privacy and Identity Management for Europe)에서는 정보사회에서 개인 ID 자치권을 유지하면서 사용자의 안전한 활동을 보장하는 ID 관리 기술을 개발하고, 이를 위한 ID 관리 솔루션 구축 환경을 제공함에 그 목적이 있다. 또한 일본의 경우, 에듀마트(Edumart)라는 사업을 통하여 다양한 교육 컨텐츠를 국공립 초등학교 및 중고등학교 학생들에게 제공하는 인프라를 구축하고 있고, 여기에 ID 연계 기술이 사용되고 있다. 또한 한국에서도 한국전자통신연구원이 인터넷 ID 관리를 위한 과제를 추진하고 있고, 이는 한 번의 인증으로 여러 사이트에서 다양한 정보 서비스를 제공받을 수 있는 싱글사인온 기술과 이를 위한 웹 서비스 프레임워크 및 개인정보 공유 체제를 구축하고 있다.

2.1.3 ID 관리 시장 동향

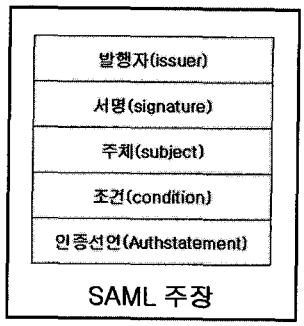
세계 ID 관리 분야의 시장은 2005년도 30억 5,850만 달러이고, 2008년에 100억 달러 규모로 성장할 것으로 예측되고 있다.(Radicati 그룹) 또한 한국의 경우, 2006년도에 537억, 2007년도에 605억원 정도의 시장규모가 예측되고 있다.(한국 IDC)

2.1.4 ID 연계를 위한 리버티 얼라이언스

리버티 연계는 인터넷 상에서 새로운 수준의 신뢰, 공동체, 그리고 상호 동작이 필요한 산업체 들에 의하여 추진되고 있다.[4,5] 네트워크 ID는 고객 이름, 전자메일 주소, 신용카드 번호, 주민등록번호, 여권 등의 개인의 속성들의 집합이라고 볼 수 있다. 리버티 연계는 고객이 네트워크 ID의 프라이버시와 안전성을 보장하게 하고, 비즈니스가 제삼자의 개입 없이 고객과의 관계를 관리하고 유지할 수 있게 하며, 분산화된 인증 기법을 유지하면서 싱글사인온을 제공하고, 새로운 네트워크 디바이스를 지원하는 네트워크 ID 기반 구조를 생성함에 그 목적이 있다. 리버티 신분확인 프레임워크는 기본적으로 ID를 연계할 수 있고, 하나의 사이트에 인증 받으면 다른 사이트에 추가의 인증 과정 수행 없이 로그온 할 수 있는 싱글사이온 기능을 제공하고 있다.

리버티 얼라이언스의 요구사항은 개방화된 시스템을 지원해야 하고, 다양한 프로그래밍 언어와 네트워크 구조를 지원해야 한다는 것이며, 리버티 클라이언트, 서비스 간에 밴더간 상호 동작을 지원할 수 있어야 한다. 리버티 얼라이언스에서 요구되는 기능 요구

사항은 ID 연계, 인증, 이명의 사용, 익명 지원 등이다. 리버티 연계의 구조는 사용자, 신분확인 제공자, 그리고 서비스 제공자로 구성되며, 사용자에 의한 웹 재지정, ID 제공자와 서비스 제공자간에 필요한 웹 서비스와 메타데이터 및 스키마로 구성된다. 웹 서비스는 통신하기 위한 프로토콜이며, 웹 재지정은 현재 설치된 사용자 에이전트에 기반을 두고 서비스를 제공하기 위한 활동이며, 메타데이터와 스키마는 여러 정보를 교환하기 위한 메타데이터와 다른 정보 형태의 공통된 집합이라고 할 수 있다. 웹 서비스를 위하여 SOAP 프로토콜이 이용될 수 있다.



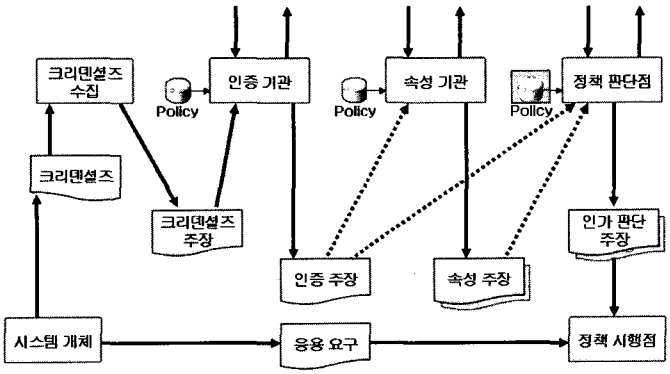
〔그림 1〕 SAML 주장

2.1.5 OASIS의 SAML 및 XACML 기술

OASIS SAML과 XACML은 웹 환경 하에서 인증과 권한 정보 등의 보안 정보를 전달하기 위한 데이터 구조를 정의하는 표준이다.[1,6-16] 2005년 3월 버전 2.0으로 진화된 SAML은 XML 기반으로 동작한다. 보안 정보는 주체에 대한 주장(assertion)의 형태로 표현되며, 주체는 하나의 보안 영역 내에서 신원을 갖는 개체이다. 주체의 대표적인 사례는 사람 또는 컴퓨터이며, 사람은 일반적으로 특정 인터넷 DNS 영역에서 자신의 전자메일 주소에 의하여 확인된다. 주장은 SAML 기관, 인가 기관, 또는 정책 판단 점에 의하여 발행되는 하나 이상의 선언(statement)을 담고 있는 정보 패키지이다. 주장 선언은 주체에 대하여 사전에 수행된 인증 선언, 주체에 대한 속성 선언, 그리고 주체가 특정 자원에 접근할 수 있도록 허용되는지를 결정하는 인가 판단 선언으로 구분된다. 다시 말해, 인증 주장 선언의 경우 특정 주체가 특정한 시점에 특정한 인증 수단으로 SAML 인증기관에 의하여 인증되었음을 나타내며, 속성 선언은 특정 주체와 관련되는 신분 및 직위 등의 속성 정보를 포함하며, 인가 판단 정보는 특정 자원에 대한 특정 주체에 대한 접근 허용 여부를 나타내는 선언을 나타낸다. 〔그림 1〕은 SAML 인증 주장의 전형적인 구조를 나타내고 있다. SAML은 클라이언트가 SAML 인증기관으로부터 주장을 요청하고, 이들로부터 응답을 수신하는 프로토콜을 정의하고 있다. XML 기반의 요구와 응답 메시지 형태로 구성되는 이 프로토콜은 많은 서로 다른 기반 통신 및 전송 프로토콜과 결합될 수 있으나, 현재는 HTTP 상의 SOAP로의 바인딩만을 정의하고 있다. SAML 기관은 응답을 생성하기 위하여 여러 발신지들의 정보를 이용할 수 있다. SAML은 주로 SSO에 이용될 수 있으며, SSO는 하나의 보안 영역에서 인증 받은 주체가 다른 보안 영역에서 재인증 과정 없이 서비스를 제공받게 한다. SAML의 여러 프로파일들이 SSO를 위한 시나리오에 활용될 수 있고, 전자거래를 위한 분산 처리와 분산된 접근 제어를 가능케 하는 다른 응용에서도 활용 가능하다. XACML (eXtensible Access Control Markup Language) 은 접근 제어 정책을 표현하기 위한 XML 표현이다. 접근 제어는 요구된 자원 접근이 허용되어야 하는지에 대한 판단 정보와 접근 결정을 시행하기 위한 정보들로 구성되어 있다. 접근 제어 정책은 접근 제어 결정을 위한 기준이 된다. XACML 핵심 규격은 인가 정책을 평가하기 위한 문법과 규칙으로 정의되고 있다. XACML은 대규모 환경에서 동작하며, 접근 제어용으로 이용되는 정보가 자동화된 주체에 의하여 관리되는 응용을 위해 효율적으로 동작하도록 설계되어 있다. XACML 정책은 〔그림 2〕와 같은 절차로 동작하며, 요구의 일시와 같은 환경 정보, 자원의 특성과 내용, 활동의 임의의 주체의 신원과 속성을 포함하여 인가 결정하기 위하여 필요한 모든 가용한 정보를 포함하고 있다. XACML은 풍부한 불리안 연산자와 데이터 조작 연산자를 규정하고 있다. XACML은 특정 접근 제어 판단에 적용할 수 있는 여러 가지 정책들을 고려하고 있고, 상충되는 판단 결과를 해결하기 위한 확장 가능한 조합 집합을 제공하고 있다. XACML은 또한 접근이 허용되고 거부될 때 취해져야 할 추가적인 행동을 규정하기 위한 광범위한 메커니즘을 제공하고 있다.

2.1.6 사용 시나리오

일본은 2005년도에 IT 리더십을 진전하기 위하여 "e-Japan 전략" 으로 알려진 국가 전략을 발표하였다.[5] 향상된 정보 통신 네트워크 사회를 이루기 위하여 만들어진 전략 본부는 2001년 1월 이후 여러 다양한 조



〔그림 2〕 인가 원리

치들을 구현하고 있다. 2005년 5월, 일본의 인터넷 사용자 비율은 60.9%에 달하고 있고, 공립학교 가운데 인터넷 사용자 비율은 거의 100%에 육박하고 있다. IT 전략 본부는 교육 향상과 인력자원을 포함하는 5개 정책 목표를 가지고 "e-Japan 우선 정책 프로그램 2002"에 기반한 대응 솔루션을 구현하고 있다. 교육 컨텐츠를 분배하기 위한 기반구조를 만들기 위하여 해결해야 할 핵심사항은 두 가지가 확인되었다. 하나는 물리적인 네트워크를 구축하는 것이고, 다른 하나는 네트워크를 통한 컨텐츠 분배이다. 2005년에 물리적 네트워크에 대한 진전이 이루어졌고, 모든 공립학교가 24시간 고속 인터넷에 연결되고 있다. 이는 40,000여개의 초등학교, 중등학교, 그리고 고등학교 사이트로 구성되어 있다. 네트워크를 통한 컨텐츠 분배는 두 가지 요구사항을 갖는다. 하나는 분배가 제한되지 않아서 여러 컨텐츠 제공자들이 자유롭게 참여할 수 있어야 한다는 것이다. 공개된 인터페이스 정의와 컨텐츠 분배 네트워크의 구성은 추가적인 조직이나 공립 기관, 그리고 개인 회사들이 인터페이스에 붙어서 자유롭게 참여할 수 있는 시스템을 가능케 한다. 두 번째 요구사항은 프라이버시와 공개성을 확립하는 것이다. 시스템의 사용자는 학생들이어서, 많은 개인정보(성적, 행동발달사항 등)가 엄격하게 보호되어야 하는 것은 기본적인 것이다. 다시 말해, 서비스 제공자가 좀 더 가치 있는 컨텐츠를 전달하기 위하여 향상된 수준의 개인 식별 정보가 필요하다는 것이 인식되었다. 프라이버시를 확보하고 공개성을 설정하는 것은 모순이다. 결과적으로, 이 시스템이 e-Japan 우선 정책 프로그램의 요구를 만족하는지 검증하기 위한 시스템을 구현하였다. 이 시제품은 일본 정부가 에듀마트(교육+시장, Edumart) 검증 시스템을 기획하면서 시작되었다. 이 프로젝트 시작 직 후, 에듀마트 검증 시험 시스템을 구축하기 위하여 채용된 기술은 다음과 같은 요구사항을 만족해야 한다고 결정되었다.

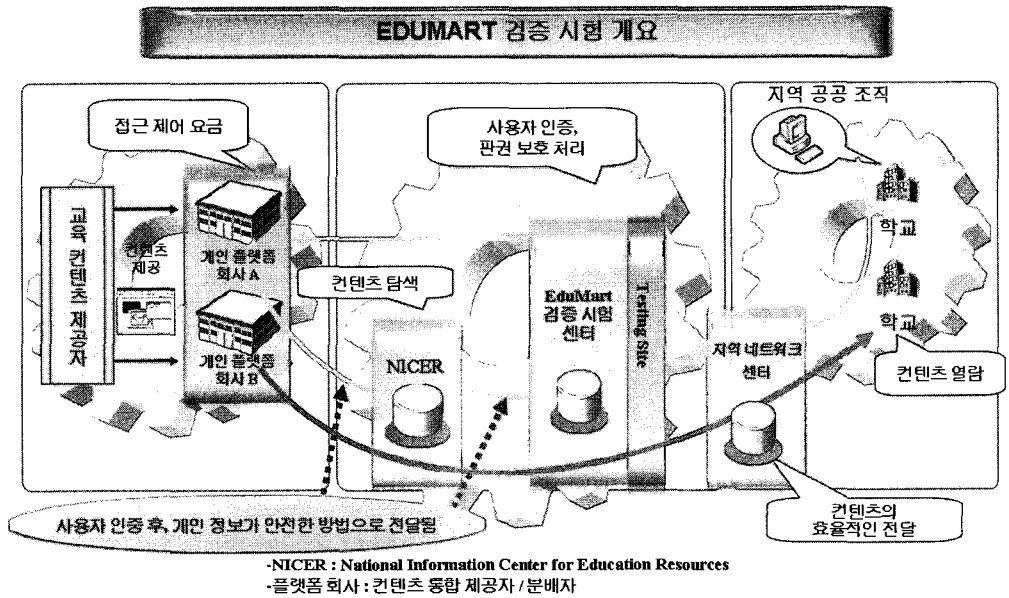
- 컨텐츠 전달의 상호연동성. 교육 컨텐츠 제공자(비디오 필름, 문서 등)에서 초등학교, 중고등학교까지 전달하기 위한 상호연동성 확보함
- 개인 정보 및 판권 관리. 시스템은 사용자 보안을 제공해야 하고, 컨텐츠 판권의 적절한 보호 및 관리를 수행해야 함
- SSO. 추가적인 인증 요구 없이 정부 및 지방정부, 학교, 그리고 개별 비즈니스에 의하여 제공되는 사용자 인증을 컨텐츠 전달과 같은 서로 다른 기능을 제공하는 시스템에 연결하는 단일 인터페이스를 제공함
- 공개성. 위의 요구사항을 만족하고 미래 사용자와 컨텐츠 제공자의 참여를 가능케 하며, 나라에 한정되거나 벤터에 한정되지 않은 공개된 기술 규격

분석 결과, 리버티 연계 단계 1 규격이 에듀마트 검증 시험을 위하여 선정되었다. 선정 시에 주요 요소는 리버티 프로토콜의 핵심 요소로 리버티가 공개한 규격에 기반하고 있고, 여러 다른 벤더로부터의 제품이 제공되고 있다는 사실이었다. 이러한 요소는 지방정부와 개별 회사가 에듀마트 e-학습 시스템의 참여를 좀더 쉽게 하였다. 세계 최초의 리버티 연계 규격에 기반한 전자 학습 시스템이다. 미들웨어 호환이 가능한 리버티 연계 규격을 선택함으로써, 에듀마트 검증 시스템은 수개월 내에 성공적으로 개설되었다. 이러한 노력은 리버티 규격에 기초한 최초의 e-학습 시스템으로

〔표 2〕 SAML/XACML 표준 집합

SAML	SAML 버전 2.0을 위한 인증 환경 /〔SAML2Auth〕	면대면 등의 초기 인증 방법, 크리덴셜 타협을 최소화하기 위한 메커니즘 (크리덴셜 갱신 주기, 클라이언트 키 생성), 크리덴셜 저장 및 보호 방법 (스마트카드, 패스워드 기반), 그리고 인증 방법 (패스워드, 인증서-기반 SSL) 등을 포함하는 인증 환경을 정의
	바인딩(Bindings)/ 〔SAML2Bind〕	SAML 요구와 응답을 송수신하기 위하여 SOAP 을 사용하는 방법을 정의하고 있음
	호환성 프로그램 규격/〔SAML2Conf〕	SAML V2.0과 호환을 주장하는 구현에 대한 강제적인 특징과 선택적인 특징을 정의하고 있음
	주장과 프로토콜/〔SAML2Core〕	SAML 주장과 관련 프로토콜의 구조를 정의하고 있음
	용어(Glossary)/ 〔SAML2Gloss〕	SAML 규격과 관련 문서에서 사용되는 용어를 정의하고 있음
	메터 데이터/〔SAML2Meta〕	확인자, 바인딩 지원과 최종점, 인증서와 키 등에 관한 시스템 개체간의 합의를 정의하고 있음
	프로파일/〔SAML2Prof〕	SAML 주장을 어떻게 프레임워크나 프로토콜에 삽입하고 추출하는지에 대한 방법에 대한 규칙을 정의하며, 발신 주체에 의하여 다른 객체 (파일 또는 PDU)로 어떻게 SAML 주장이 삽입되는지와 수신지에서 어떻게 처리되는지에 대해 기술하고 있음
	보안 고려사항/〔SAML2Secc〕	SAML이 어떻게 프라이버시 보호 문제를 다루는지, 위협과 보안 위험은 무엇인지, 다루어지지 않은 보안 위협은 무엇인지, 그리고 이 보안 위험을 감소시키는 대응책에 대한 대응방안을 제공하고 있음
	스키마 파일/〔SMAL2Schema〕	SAML 관련 스키마를 포함하고 있음
XACML	XACML핵심 XACML 버전 2.0규격 /〔XACML2Core〕	언어의 문법과 정책 평가를 위한 법칙을 정의함
	XACML 의 SAML 2.0 프로파일/ 〔XACML2SAML〕	정책 조회, 분산된 판단 요구를 위하여 SAML 스키마 요소를 확장함
	XACML의 디지털 서명 프로파일 /〔XACML2DSIG〕	디지털 서명이 XACML 정책에 어떻게 적용되는지를 정의함
	XACML 프라이버시 정책 프로파일 /〔XACML2Priv〕	XACML이 프라이버시 정책을 어떻게 시행하는지를 정의함
	XACML 계층적 자원 프로파일 /〔XACML2Hier〕	계층적 구조를 갖는 자원에 적용되는 자원에 대하여 어떻게 접근제어 정책과 접근판단 요구가 이루어지는지를 정의함
	XACML을 위한 다중 자원 프로파일 /〔XACML2Mult〕	하나 이상의자원에 대하여 동시에 어떻게 접근제어가 이루어질 수 있는지를 정의함
	XACML을 위한 계층적 역할 기반 제어(RBAC)프로파일/〔XACML2RBAC〕	XACML이 어떻게 역할 기반 접근 제어를 시행하는지를 정의함
	XML 스키마/〔XACML2Schema〕	XACML 관련 스키마 파일을 정의하고 있음

나타났다. 현재 일본 전체를 통하여 전체 98개 공립 학교에 있는 3,500여개의 터미널에게 24시간 단위로 컨텐츠를 제공하고 있다. 이 시스템은 공개성과 상호 연동성을 보장하면서 안전성과 편리성을 동시에 확보하는 리버티 연계 규격에 기초하여 구축된 최초의 사례이다.



〔그림 3〕 에듀마트 구조

2.2 교육정보공유체제 ID 관리체제

교육정보공유체제는 시,도 교육청, 교육유관기관, 교육현장 등에서 생성되는 각종 교육용 자료를 누구든지(Anyone), 언제(Anytime), 언제든지(Anywhere), 한번에(One Click)에 검색할 수 있도록 표준화된 교육정보 메타데이터 형태로 공유 유통시키는 서비스를 제공하는 시스템이다.

2.2.1 ID 관리 국내외 환경 분석

현재 국내 인터넷 이용자 비율은 2004년도 12월 통계로 세계 12위인 65.2%에 이르고 있다. ID 관리 시스템 구성 시 고려해야 할 국내 환경은 몇 가지가 있다. 정보통신부는 인터넷 사이트 가입 시 주민등록번호 등의 개인정보의 수집을 엄격히 통제할 예정이다. 이에 대한 보완으로 현재 주민등록 대체 기술을 개발하고, 본인확인 기관을 통하여 주민등록번호 대체 번호를 이용하여 사이트 가입 시에 이용할 예정이다. 또한, 정보통신부에서는 인터넷 실명제를 추진할 예정이다. 그리고 개인 정보의 프라이버시 보호가 매우 중요하다. 일본의 경우 개인정보프라이버시 보호법을 채택하여 부주의한 개인정보의 노출을 기업이나 조직에 책임을 묻고 있다. 우리나라도 현재 2개의 개인정보 안건이 국회에 계류되어 있으며, 개인정보보호법이 조만간 국회를 통과하여 시행될 예정이다. ID 관리 시스템을 위한 국외 환경은 다음과 같다. 최근 2005년 3월 ID 관리를 위한 기본 표준인 SAML V2.0과 XACML V2.0이 OASIS에서 채택되어 현재 ITU-T 국제 표준으로 표준화를 추진하고 있고, 2006년 4월 한국 회의에서 승인될 예정이다. 2006년까지 표준 기반의 ID 관리 시스템이 글로벌 2,000 기업의 50% 이상이 50% 이상의 확률로 채택될 것으로 예측되고 있다. 많은 나라에서 ID 도용이 매우 큰 사회 문제로 대두되고 있고, 이를 위한 대책이 필요한 시점이다. 일본의 경우, 2005년 초에 개인정보보호법을 시행하여 조직이나 회사에 개인정보 보호를 강제화하는 법령을 시행하고 있다. 또한, ID 연계에 근거하여 교육정보 공유시스템을 구축했다. 미국의 경우 ID 연계를 위하여 리버티 얼라이언스가 결성되어 각종 표준과 모범 사례에 대한 연구가 진행 중에 있다.

2.2.2 정의 및 현황, 보안 문제점, 보안 요구사항

교육 정보의 공유를 위한 분산화된 데이터베이스에 기반하고 있다. 또한, 사용자 친화적인 웹 환경에서 동작하고 있고, 교육정보를 공유하기 위하여 여러 다양한 사이트들이 상호 연결되어 동작하고 있으며, 각 사이트의 독자성과 상호 연결성이 요구되고 있다. 교육정보공유체제를 위한 ID 관리는 다음과 같은 문제점을 포함한다. 첫째, 분산화되어 있는 모든 사이트에서 인증관련 개인정보(특히, 주민등록번호 등)를 독립적으로 수집하고 있고, 분산화된 인증관련 정보 관리

로 인한 인증관련 개인정보의 노출 가능성이 증가하고 있다. 둘째, 공유되는 교육 자료가 개인정보를 포함하는 경우, 엄격한 접근 통제가 필요하다. 이를 시행하지 않으면 많은 사회적 논쟁이 유발될 가능성이 크다. 현재 ID 관리를 위한 환경을 살펴보면, 여러 기관이나 조직이 개별 사이트를 독립적으로 운영하고 있고, 공유 자료에 대한 프라이버시 보호를 위하여 분산화된 데이터의 저장이 요구되며, 사용자의 경우 여러 조직이 운영하는 사이트에 접근하기 위해서 여러 개의 ID/패스워드를 관리할 필요가 있으며, 여러 사이트에 접근하기 위해서는 각 사이트마다 여러 번의 인증이 요구되고 있다. 따라서 현재와 같은 문제점은 ID 관리 기술로 해결될 수 있다. 교육정보공유체제 ID 관리를 위한 보안 기술은 다음과 같다.

- 사용자 인증을 포함하는 ID 연계 기술: 특정 사용자의 신원을 온라인에서 확인함과 동시에 개인정보를 안전하게 관리하는 기술이며, 여러 사이트간에 ID 연계를 통한 새로운 비즈니스 기회를 제공하는 기술
- SSO 기술: 한 번의 인증으로 추가 인증 과정을 수행하지 않고 다른 정보서비스를 제공받게 하는 기술
- 권한 관리 기술 : 권한 있는 특정 사용자만이 특정 객체를 열람할 수 있게 하는 기술
- DRM(Digital Right Management) 기술 : 공유 정보에 대한 디지털 권한 관리 기술

교육정보공유체제를 위한 ID 관리 시스템을 위한 요구사항은 다음과 같다.

- 확장성이 높아야 함, 다시 말해, 조직 또는 사용자 측면에서 확장 가능해야 한다. 조직의 증가와 사용자의 증가에 능동적으로 대응할 수 있어야 함
- 제품 개발과 서비스 제공 측면에서 상호 연동성이 보장되어야 함
- 여러 번의 인증 과정을 줄일 필요가 있음
- 여러 번 수행해야 하는 불필요한 인증 횟수를 줄여서 인증관련 개인 정보의 노출 가능성을 줄임으로써 사용자의 편의성 증대가 요구됨
- 초기 인증 시에 여러 다양한 인증 방식의 사용이 가능해야 함. 다시 말해, 인증서를 이용한 인증 방식, ID/패스워드 인증 방식, 그리고 생체 인증 등 다양한 방법이 가능해야 함
- 인증을 위하여 필요한 개인 정보의 프라이버시 보호를 위한 대책이 필요함
- 사용자의 편리성이 최대한 보장되어야 함
- 국제표준에 준용하는 시스템의 개발이 필요함

2.2.3 ID 관리를 위한 방식 장단점 분석

교육정보 공유를 위한 방식은 크게 정보 공유 측면에서 중앙 집중 방식과 분산 방식으로 구분되며, 다시 ID 관리 측면에서도 ID 연계 방식과 ID 비연계 방식으로 구분될 수 있다. 공유정보 측면을 먼저 살펴보자. 중앙 집중화된 방식의 경우, 공유 정보가 중앙 집중화하여 관리하고 있으므로 접근 제어가 용이하게 할 수 있으나, 과도한 트래픽 집중이 발생하고, 중앙 서버의 해킹시의 공유 정보 전체가 노출될 가능성이 있으며, 공유 정보를 저장하는 중앙 서버의 해킹 시에 전체 공유 정보가 노출될 가능성이 있어서 큰 사회적 문제를 초래할 수 있다. 분산화된 방법의 경우, 공유 정보의 통제가 분산화되어 보관 관리되고 있어서 프라이버시 문제를 제기하지 않을 수 있으나, 각 사이트별 독자적인 정보 관리가 가능하나, 권한 있는 사용자만이 접근케 하는 접근 제어의 시행에 어려움이 예상되고 전체 공유 정보의 노출 가능성이 낮다. ID 관리 측면에서 살펴보자. ID 연계 방식과 ID 비연계 방식으로 구분될 수 있다. ID 연계 방식의 경우, 하나의 ID 서비스 제공자를 여러 사이트들이 연계하는 방법의 경우, 개인정보를 하나의 중앙 서버에 둠으로써, SSO(Single Sign-On) 기능의 실현이 용이하고, 사용자의 편리성이 증가하나, 여러 사이트간의 연계가 필요하며, 연계를 위한 협정 체결과 이를 위한 시스템 개발이 필요하다. 또한 개인 정보의 보관이 주로 하나의 ID 제공자에만 존재하여 개인정보의 보호가 용이하다. 다만 중앙 인증 서버가 사용자의 사이버 활동을 모두 관찰할 수 있게 되는 빅브라더(Big Brother) 문제가 발생할 가능성이 있어서 이에 대한 관리적 기술적 대책이 필요하다. 비연계 ID 관리의 경우, 사용자가 여러 개의 ID를 관리해야 하는 부담이 있고, 각 사이트마다 별도의 인증과정을 통하여 인증 받은 후 서비스를 제공받으며, 여러 사이트에 분산되어 있는 ID관련 개인정보의 노출 가능성이 매우 높다.

2.2.4 기술적 대안에 대한 바람직한 선택

정보 공유 측면에서는 분산화된 방법을, ID 관리 측면에서는 인증관련 개인정보 보호를 위하여 ID 연계 방

식을 선택하는 것이 바람직하다. 이때 빅브라더 문제를 해결할 수 있는 정책 개발과 대안의 선택이 필요하다.

2.2.5 교육정보공유를 위한 ID 관리 시스템 요구사항

먼저, 국제 표준을 준용하는 시스템 구조의 설정이 요구된다. 이렇게 함으로써, 서비스의 상호 연동성을 보장하고 구성요소 간에 상호 연동성도 보장됨. 이는 다른 회사 제품 간의 상호 연동성을 보장할 수 있고, 추가 정보 서비스의 부가가 용이해야 한다. 둘째, 확장성이 고려된 시스템 구성이 요구된다. 가입자의 수나 조직의 수가 늘어나더라도, 커다란 추가 부담 없이 시스템의 확장이 가능한 기술 구조를 선택하는 것이 바람직하다. 셋째, ID 관리 시스템 구축을 위한 국내 표준화 작업이 필요하다. 이는 시스템 간, 또는 구성요소간에 상호 동작을 가능케 한다. 넷째, 공유 정보에 대한 권한 관리가 매우 필요하다. 다시 말해, 정보를 필요로 하는 주체만이 정보에 접근할 수 있어야 하며, 이를 위한 보안 정보 교환을 위한 프레임워크 및 정보 요소에 대한 표준화가 요구된다. 다섯째, 공유정보에 대한 엄격한 권한 관리가 시행 가능해야 한다. 다시 말해 권한 있는 사용자만이 공유 정보에 대하여 접근할 수 있게 하는 것이 무엇보다도 요구되고 있다. 여섯째, 공유정보의 관리를 각 사이트에서 독자적으로 수행하는 것이 시민 단체에 의한 저항을 줄일 수 있다. 일곱째, 인증을 위한 개인정보의 수집의 최소화와 초기 인증의 강력한 사용자 편리성을 보장해야 한다.

결론적으로 교육정보공유체제를 위한 ID 관리는 국제 표준인 SAML 및 XACML 버전 2.0에 기반하여 구축되는 것이 바람직하며, ID 연계 프레임워크는 리버티 얼라이언스와 같은 표준화된 프레임워크 사용이 바람직하며, 이를 위한 국내 표준의 개발이 필요하고, 이에 입각한 제품 개발이 필요하다고 할 수 있다.

Ⅲ. 결 론

결론적으로, 교육정보공유체제를 위한 ID 연계를 위하여 다음과 같은 사항의 고려가 필요하다. 먼저 2.2.5 절에서 제시된 요구사항을 만족하는 ID 관리 시스템이 구축되어야 할 것이다. 또한, 향후 이를 위한 관련 표준의 수용 또는 국내 독자 표준의 개발이 필요하다. 그리고, 장기적으로 공유 정보의 DRM 보장을 권한 소유자 또는 조직 입장에서 고려되어 개발되어야 한다. 교육정보 공유는 분산화된 방식으로 보관되고, 엄격한 접근제어 정책의 개발과 시행을 통한 접근 제어가 이루어져야 할 것이며, 사용자 인증을 위한 과도한 개인정보가 다양한 사이트에 존재하지 않아야 하고, 필요한 개인정보도 최소화할 필요가 있다. 또한, 한 번의 신원확인은 매우 강력한 수단(인증서 방법, 신원확인증표에 의한 오프라인 방법, 은행계좌 정보, 신용카드 비밀번호, 핸드폰 문자메시지를 이용한 인증방법 등)으로 이루어져야 한다. 한 번의 인증으로 일정 시간 동안 여러 사이트를 접근할 수 있는 싱글사인온 기능이 필요하다. ID 관리를 위하여 연계 방식의 채택이 필요하다. 또한, ID 관리는 국제 표준을 준용하는 시스템의 개발이 요구되며, 개발과 함께 표준화도 추진해야 할 것이다. 제시되고 있는 ID 연계에 근거한 대안은 이러한 요구사항을 만족하는 좋은 대안 이다.

참 고 문 헌

[1] 염흥열, "OASIS가 개발한 두 기본 표준이 조만간 ITU-T 표준으로 채택 예정," TTA, TTA 위크리, 2005년 11월

[2] 진승헌, 편리하고 안전한 인터넷 이용을 위한 ID 관리 서비스, 2005.10.13. ETRI 내부 자료

[3] 진승헌, 전국교육정보공유체제를 위한 ID 관리 서비스, 2005년 10월 13일, KERIS 공청회

[4] Liberty alliance, Liberty ID-FF Architecture Overview, 2003.

[5] Liberty alliance, Use Case Study: EduMart Verification Test, 2005.

[6] **OASIS 2005** Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0.

[7] **OASIS 2005** Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.

[8] **OASIS 2005** Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0.

[9] **OASIS 2005** Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0.

[10] **OASIS 2005** Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0.

[11] **OASIS 2005** SAML protocols schema.

[12] **OASIS 2005** Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.

[13] **OASIS 2005** Security and Privacy Considerations for the OASIS Security

Assertion Markup Language (SAML) V2.0.
[14] **OASIS 2005** SAML Technical Overview.
[15] **OASIS 2005** SAML assertions schema.
[16] **OASIS 2005** eXtensible Access Control Markup Language (XACML).

〈著 者 紹 介〉

염 흥 열 (Heung Youl Youm)
종신회원

1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10, Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
〈관심분야〉 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안