선택적인 가입 및 탈퇴가 가능한 통합 인증체제 구축방안 연구

이상환*, 천인혁*, 신수미*, 이태석*, 신기정*
*한국과학기술정보연구원 정보서비스실
e-mail:sanglee@kisti.re.kr

A Study on Single Sign-On System Development for a Selective Admission and Withdrawal

Sang-Hwan Lee*, In-Hyeuk Cheon*, Su-Mi Shin*, Tae-Suk Lee*, Ki-Jeong Shin*
*Dept of Information Service, Korea Institute of Science and Technology Information

요 약

공공 부문이나 대기업에서 운영하는 웹 사이트의 규모가 커지면서 분야별로 사이트가 나누어지게 되는데, 사이트를 이동할 때 마다 로그인을 다시 해야 하는 불편이 있다. 따라서 최근 이용자들의 불편을 줄이기 위하여 SSO(Single Sign-On) 통합인증 체제를 도입하는 사례가 늘고 있으나 전체 패밀리 사이트를 일괄적으로 가입과 탈퇴되는 문제가 발생한다. 이에 이용자의 필요에 따라 선택적으로 가입과 탈퇴가 가능한 통합 인증체제 방안을 제안하고자 한다.

1. 서론

웹 사이트의 회원제 서비스가 공공부문이나 민간부문에서 운영하는 웹 사이트의 규모가 커지면서 세부 분야별로 사이트가 나누어지게 되어 있어서 이용자들의 등록과 인증의 불편을 줄이기 위하여 SSO(Single Sign-On) 통합 인증체제를 도입하는 사례가 늘고 있다.

일반적인 인터넷 사용자는 웹 사이트마다 반복되는 등록 절차를 매우 번거롭게 생각하고 있다. 여러 군데 등록해 두었기 때문에 주소 변경 등도 여러 군데에서 수행해야 한다. 또한 각 사이트의 ID와 패스워드를 암기하는 것은 매우 어렵기 때문에 보통 동일 ID와 패스워드를 사용하거나 패스워들 메모해 두게 되는데 이는 보안상 큰 문제가 아닐 수 없다[1].

그러나 일반적인 통합 인증시스템을 통해 인증하였더라도 통합 인증체제에서 회원 탈퇴 시 모든 패밀리 사이트가 탈퇴되는 것이 일반적이며, 이용자가 서비스 필요시 다시 가입하여야 한다.

따라서, 통합 인증체제에 가입과 탈퇴하는 것을 반복하는 것이 아니라 통합 인증체제에 한번만 가입하고 패밀리 사이트는 이용자의 필요시 가입과 탈퇴가 자유로워야 한다. 이러한 문제를 해결하기 위해 본 논문에서는 통합 인증체제하에서 회원가입을 통해 이용자가 필요시 선택적으로 가입과 탈퇴가 가능한 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구에 대해여 기술하고, 3장에서는 SSO 통합인증 회원 DB와 LDAP 정보간 동기화 방안과 선택적으로 가입 및 탈퇴가 가능한 방안을 제시하고, 4장에서는 제시한 방안에 대하여 성능 테스트 및 평가하였고, 5장에서 결론과 향후 연구방안에 대하여 기술한다.

2. 관련연구

2.1 SSO(Single Sign-On)

SSO(Single Sign-On)는 한번의 로그인을 통해 모든 서버에 접속할 수 있는 권한을 갖게 되는 개념이다. SSO 시스템의 일반적인 구성은 local authentication, credentials, service로 구성된다[2, 3].

Local authentication은 초기에 사용자를 인증하는 부분으로서 사용자 identity를 credential 정보로 매핑하는 부분이다. Credential은 커버러스의 토큰이나 아이디/패스워드 등 인증절차를 나타내는 스크립트, 사용자 권한정보, 소속 그룹 정보 등 사용자의 인증에 관한 정보들을 말한다. Service는 사용자가 접속하기 위한 응용프로그램 서비스를 말한다.

특히, 디렉토리 시스템인 LDAP 서버를 중심으로 인증서를 CA에서 받는 방식으로 응용프로그램과 SSO 서버 사이의 API 메커니즘을 이용한 여러 가지 구현 시스템들이 나오고 있다. SESAME(A Secure European System for Applications in a Multi-vender Environment), Netscape, Suitspot, Novell 등에서 SSO 모델을 제시하고 있다[6, 7].

그림 1은 기존 시스템 환경과 SSO를 적용한 시스템을 비교한 SSO 개념도이다.

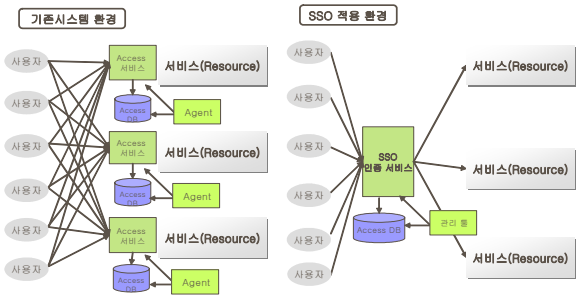

그림 1 SSO(Single Sign-On) 개념도

2.2 LDAP(Lightweight Directory Service Protocol)

LDAP은 모든 형태의 디렉토리형 자료를 표준화된 방식으로 저장하고 검색하기 위한 통신규약으로서 미국 미시간 대학에서 ITU-T의 X.500을 근거로 개발되었다[4]. X.500은 인터넷 사용이 가능한 곳이라면 전 세계 어디에서라도 이용이 가능하도록 나라, 기관, 사람, 기계 등과 같은 객체들을 관리하고 정보를 제공하는 디렉토리 서비스 표준이다[5, 8].

사용자가 X.500 디렉토리 서버로 접근하기 위해 DAP(Directory Access Protocol)이라는 프로토콜을 이용하지만 OSI 7계층을 모두 필요로 하기 때문에 자원을 많이 필요로 하지 않는 인터페이스나 경량의 프로토콜을 사용하는 인터페이스에는 적절하지 못하다는 단점이 있다. LDAP은 이러한 DAP의 문제점을 해결하기 위해 나온 프로토콜이다. 그림 2는 LDAP 계층도이다.

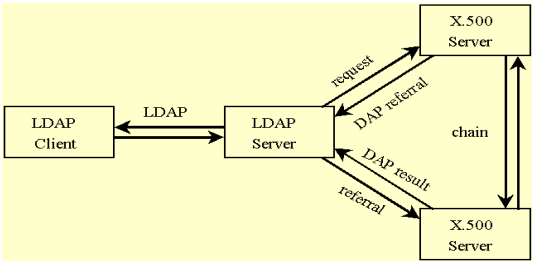

그림 2 LDAP(Lightweight Directory Service Protocol) 계층도

3. 회원정보 DB와 LDAP 동기화 방안

3.1 회원정보 DB와 LDAP 동기화 처리 개념도

회원정보 DB와 LDAP의 정보 간의 동기화가 필요한 상황은 단지 웹 사이트에서만 필요한 것이 아니라 클라이언트/서버 프로그램이나 관리자가 데이터베이스 관리 도구를 사용해서 회원 정보를 변경하였을 경우에도 필요하다.

그림 3은 LDAP 동기화 프로그램의 처리 개념도를 나타낸 것이다. 우선 LDAP 동기화에 필요한 데이터는 통합 이용자 테이블(TT_USER)과 사이트 가입 테이블(TT_USERSITE)에서 인증과 사이트 접속권한에 필요한 컬럼들을 오라클 트리거를 이용해서 임시테이블(TT_USER_LDAP)에 저장하는 방식을 채택하였다.

임시테이블에는 이용자 또는 관리자가 통합회원정보의 변경시(회원가입, 탈퇴, 수정 등) 데이터가 저장된다. 임시테이블에 저장된 데이터를 LDAP에 반영하는 역할은 인증서버 측의 웹 프로그램이나 응용 프로그램에서 하게 된다.

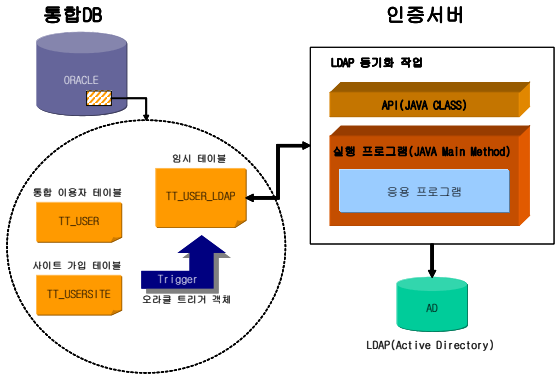

그림 3 LDAP 동기화 프로그램 처리 개념도

3.2 API를 이용한 회원정보 DB와 LDAP 동기화

LDAP 동기화를 위해 웹 프로그램에서 API를 이용하는 응용프로그램으로 처리하고자 한다. 실시간(real time)으로 이용자 정보를 LDAP에 동기화하는 방식으로 하기 위해 인증서버 측의 서비스 플랫폼을 JAVA 기반의 네이밍 서비스(Naming Service)API를 이용하였다. 이용자가 통합 회원에 가입하는 상황을 예로 들어 처리 구조를 설명하면 다음과 같다.

이용자가 회원에 가입하면 TT_USER 테이블에 회원정보가 저장되고 오라클 트리거가 작동하여 TT_USER_LDAP에 인증에 필요한 회원 기본정보를 저장한다. 웹 프로그래밍에서는 이용자 가입 처리가 끝나면 LDAP 동기화 처리 API를 호출한다. LDAP 동기화 처리 API에서는 이용자 ID로 TT_USER_LDAP 테이블에서 관련 데이터를 검색하고, LDAP에 반영하고 난 후 임시테이블에 있는 데이터를 지우는 방식으로 처리하고 있다.

응용 프로그램 방식은 TT_USER_LDAP 테이블에 미처리 데이터가 남아 있는 경우 응용 프로그램 방식으로 운용하여 통합DB와 LDAP간의 데이터 보정작업을 할 때 이용한다.

회원정보 DB와 LDAP 정보간의 동기화를 처리하는 클래스는 5개의 클래스로 처리하며, 각 해당 클래스간의 관계를 클래스 다이어그램은 그림 4와 같다.

- SyncUserData.java : 메인(main) 클래스
- LdapUtil.java LDAP : 연동 관련 클래스
- PropertyLoader.java : 프로퍼티 파일 관련 클래스
- SyncLDAP.java : 벌크로딩 관련 클래스
- SyncLdap.properties : 프로퍼티 파일

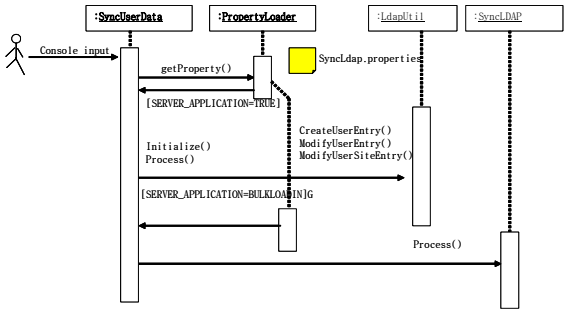

그림 4 동기화 클래스 다이어그램

3.3 선택적 가입 및 탈퇴방안

KISTI SSO(Single Sign-On)체제[9]에서 개별 사이트에서 가입 및 탈퇴시 필요한 공통정보와 회원 부가정보, 그리고 가입하고자 하는 해당 개별 사이트의 등록정보를 통해 이용자가 필요로 하는 사이트와 필요하지 않은 사이트에 대해 선택적으로 가입과 탈퇴가 가능하도록 하였다. 그림 5는 위에서 설명한 선택적 가입과 탈퇴가 가능한 ERD 구조이다.

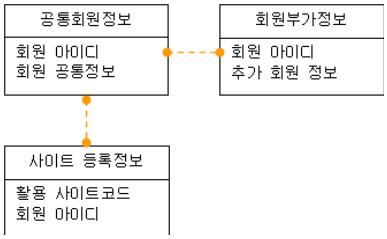

그림 5 SSO 관련 ERD 스키마

통합 인증체제에서 회원가입 후 특정 사이트에서 이용자가 원하는 서비스를 이용하고자 할 경우 그림 6과 같이 개별사이트로 가입 절차 프로세스를 진행한다.

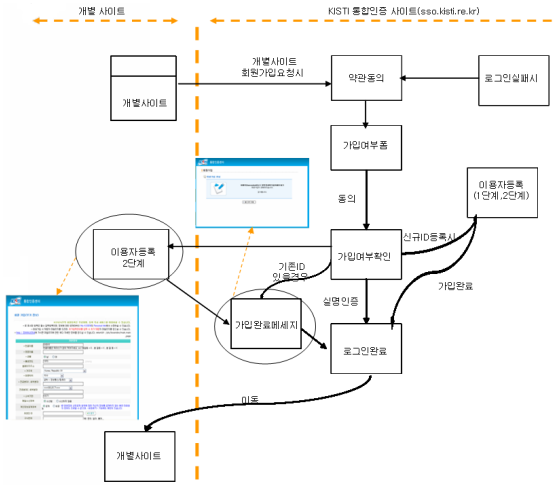

그림 6 SSO 회원 가입절차

먼저, 개별 사이트로부터 로그인 요청하고 인증정보 입력 폼에서 ID, PW를 입력한 후 SSO시스템으로부터 인증 확인되면 자동 로그인이 되면서 개별 사이트로 이동된다.

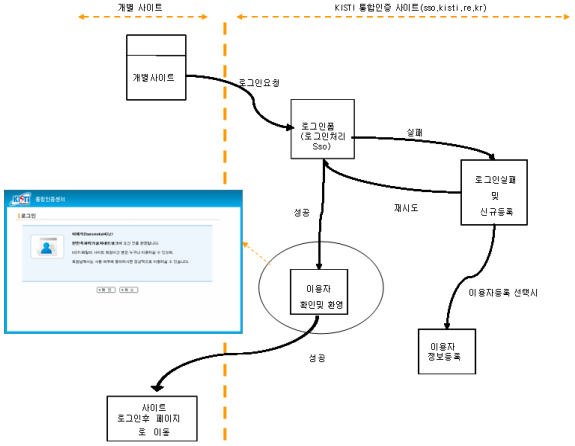

그림 7 개별 사이트 인증 절차

또한, 개별 사이트로부터 탈퇴 요청시 그림 8과 같이 탈퇴처리 프로세스에 의해 탈퇴 처리한다. 개별 사이트로부터 이용자 탈퇴 요청 시 전체 패밀리 사이트중 이용자가 가입되어 있는 사이트를 보여주며 완전탈퇴를 선택하거나 개별 사이트를 선택하여 탈퇴를 신청하면 탈퇴 처리한 후 요청 사이트 첫 페이지로 이동한다.

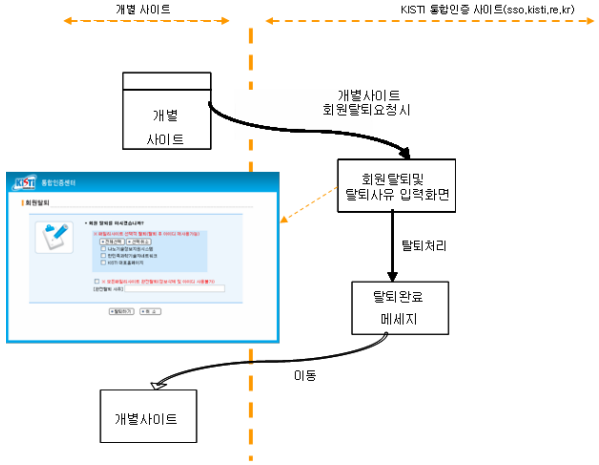

그림 8 개별 사이트 탈퇴 절차

4. 평가 및 결과

4.1 실험환경 및 방법

SSO 회원 DB와 LDAP의 정보 사이의 동기화 Loading Test를 위한 시스템 실험환경은 WINDOWS 2003서버와 오라클 8i이고, 소프트웨어 환경은 LDAP 동기화프로그램, JDK 1.4.x, ActiveX 에이전트로 구성하였다.

실험방법은 실시간으로 웹 페이지에서 동시 등록을 통해 SSO 회원 DB와 LDAP의 정보 사이의 동기화와 통합 인증체제에서 회원가입 후 패밀리 사이트 중 특정 사이트의 가입과 탈퇴를 실험하였다.

4.2 평가 결과

그림 9는 통합 인증체제에서 회원 가입 절차를 통해 KISTI 홈페이지의 로그인 화면에서 회원ID와 패스워드를 입력하면 인증됨을 볼 수 있다.

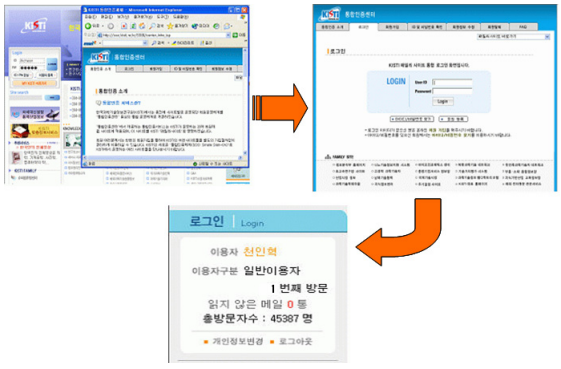

그림 9 회원정보 동기화 테스트 결과

또한, KISTI의 SSO체제에서의 회원가입 및 탈퇴 기능과 다른 종합 인증체제에서 적용되는 기능을 비교 분석하였다.

비교 대상으로는 삼성전자의 ANY PATH와 SK의 SK Telecom 통합서비스를 대상으로 하였다. 삼성의 ANY PATH라는 통합 인증체제는 삼성전자 웹 사이트, 애니콜 랜드 등 9개의 패밀리 사이트를 운영하고 있으며, SK Telecom 통합 서비스에서는 e-Station, SK 텔레콤 멤버쉽 등 5개의 패밀리 사이트를 운영하고 있다.

ANY PATH와 SK Telecom 통합인증서비스에서 회원 가입 후 탈퇴 시 그림 10과 11처럼 전체 패밀리 사이트에 대한 탈퇴 여부나 탈퇴사유를 선택한 후 탈퇴가 가능하도록 되어 있다.

그림 10 ANY PATH 통합 인증체제의 탈퇴

그림 11 SK Telecom 통합서비스에서의 탈퇴

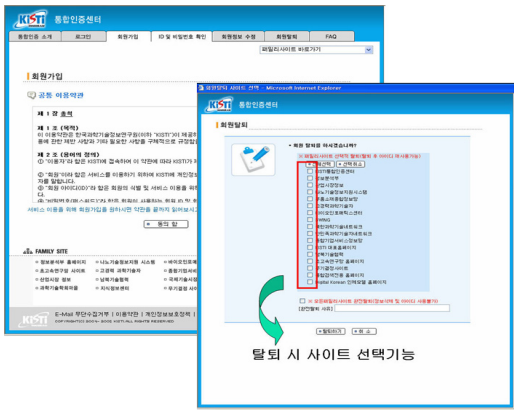

그림 12 KSITI 통합 인증체제에서의 탈퇴

KISTI의 SSO체제는 KISTI 홈페이지, 통합검색 홈페이지 등 24개 패밀리 사이트를 운영하고 있다. 그림 12처럼 통합 인증사이트에서 회원가입을 하고 특정 사이트를 최초 방문 시 자동 로그인과 동시에 해당 사이트의 정보가 등록된다. 이용자의 필요에 따라 탈퇴 시 하나의 회원ID로 가입한 사이트의 정보를 보여주며 일괄적으로 탈퇴하거나 선택적으로 선별하여 탈퇴가 가능하다.

5. 결론

웹 사이트의 회원제 서비스가 공공부문이나 민간부문에서 운영하는 웹 사이트의 규모가 커지면서 세부 분야별로 사이트가 나뉘어져서 이용자들의 등록과 인증의 불편한 문제점은 KISTI 패밀리 사이트에서도 마찬가지이다.

또한, KISTI에서 운영하고 있는 20 여 개의 패밀리 사이트가 있지만 서로 같은 이용자에 대해 중복 정보를 보유하고 있으며, 이들 회원 정보들을 효율적인 관리와 운영에도 문제가 발생하였다.

따라서, 본 논문에서는 이러한 중복문제와 대용량의 회원 인증시 동기화와 일괄적인 가입과 탈퇴문제들을 해결하기 위해 선택적으로 가입과 탈퇴를 가능한 통합 인증체제 방안을 제시하였다.

회원 통합 DB와 LDAP DB간 동기화 해결을 하기 위해 API방식으로 처리하였고, 개별 서비스를 운영중인 사이트와 이용자의 편의를 위해 한번의 회원가입으로 특정 사이트를 가입하거나 탈퇴할 수 있는 선택적인 기능을 추가하였다.

향후 연구방안으로 대용량 회원정보를 벌크 로딩 시 동기화를 처리하지 못하는 문제점을 해결하는 방안과 알고리즘이 필요하다.

참고문헌

[1] Daeseon Choi, Sangrae Cho, Seunghun Jin, Kyoil Chung, "An Information Security Model for the next Generation Application Service", IWA2002, Taiwan, October 2002.

[2] J. Hursi, "Unified Single Sign-On", Proceedings of the Helsinki University of Technology Seminar on Network Security Fall 1998. <http://www.tml.hut.fi/Opinnot/Tik-110.501/1998/papers/3singlesignon/singlesign-on.htm>

[3] P. Carden, "The New Face of Single Sign-On", 1999. <http://www.networkcomputing.com/1006/1006f1.html>

[4] W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access protocol", RFC1777, 1995. 3.

[5] W. Yeong, T. Howes, S. Kille, "X.500 Light-weight Directory Access Protocol", RFC1487, 1993. 7.

[6] White Paper, "Windows 2000 Kerberos Interoperability", Microsoft.

[7] X/Open Single Sign-On Service(XSSO)-Pluggable Authentication Modules, The Open Group, 1997.

[8] 정진원, "디렉토리 서비스의 핵심 기술 'LDAP'", Network Times, 2001.

[9] 천인혁, 이태석, 이상환, 김남근, 신기정, "SSO(Single Sign-On)체제 구축을 위한 웹 사이트 회원정보와 LDAP(Lightweight Directory Access Protocol)정보 동기화", 한국컴퓨터종합학술대회, 2005.