객체 지향 접근을 통한 LDAP 상호운용성 시험도구 구현

준회원 김 연 수*, 정회원 이 승 희**, 이 종 협***

Implementation of the LDAP interoperability testing tool with object-oriented approach

Youn-sU Kim* *Associate Members*, Soong-Hee Lee**, Jong Hyup Lee*** *Regular Members*

요 약

현재 국외의 LDAP (Light-weight Directory Access Protocol) 상호운용성 시험을 위한 시험 도구가 있으나 이들은 소스가 개방 되어 있지 않아 시험 환경에 맞추기 위한 시험 항목의 수정이 어렵고, 차후 새로운 시험 항목의 추가 또한 힘든 상황이다. 그러므로 새로운 시험 도구에서는 개발 시간 단축과 시험 항목의 추가 및 변경의 용이성을 위해 객체지향 접근이 요구된다. 따라서 객체 지향 접근을 위해 객체 지향 언어인 자바를 이용해 시험 도구를 구현하였다. 구현한 시험도구는 시험 항목 정보 중에서 이미 저장되어 있는 데이터에 알맞게 일부를 수정하여 시험이 가능하다. 또한 한번의 동일한 설정으로 최대 5개의 LDAP 서버를 동시에 시험 가능하다. 구현한 시험도구를 사용하여 두 대의 LDAP 서버를 대상으로 상호운용성 시험을 수행한 결과 정상적으로 동작됨을 확인하였으며, 시험 환경에 알맞도록 시험항목의 변경과 새로운 시험 항목의 추가가 용이함을 확인하여, 설계한 아키텍처의 유용성을 검증하였다.

Key Words : LDAP, BLITS, Interoperability.

ABSTRACT

The testing tools implemented up to now for the LDAP(Light-weight Directory Access Protocol) interoperability tests are not easy to modify or add new test items since their source codes are not open. The object-oriented approach, therefore, is required to implement such a testing tool which can be easily modified or add new test items. Thus we designed the architecture for the testing tool applying the object-oriented approach. Java language, appropriate for the object-oriented approach, was used to implement the testing tool. The newly implemented testing tool can modify partly to adapt to the already stored data in the test suite information even during tests. Five LDAP servers can be tested simultaneously with the same configuration setup. Actual testing for the two LDAP servers validates the usefulness of the designed architecture with the proper working of the implemented testing tool according to the architecture.

Ⅰ. 서 론

현재 국내의 여러 업체에서는 LDAP 기능을 탑재한 제품들이 출시되고 있으며 일부 업체에서는 LDAP을 적용한 시스템 구축이 이루어지고 있다. 그 외에도 국내외적으로 디렉토리 서비스의 확산을 위해서 LDAP 기능의 경량화, 적정화, 보안대책을 강구하고 있는 LDAP v3의 표준화 작업등이 활발

* 인제대학교 전자정보통신공학과 차세대 통신망 연구실 (kys0059@hanafos.com),
** 인제대학교 공과대학 전자정보통신공학부 (icshlee@inje.ac.kr), *** 인제대학교 공과대학 전자정보통신공학부 (icjhlee@inje.ac.kr),
논문번호 : 030473-1027, 접수일자 : 2003년 10월 27일

히 이루어지고 있다. 그러나 여러 벤더들에 의해 개발된 LDAP 기능을 탑재한 제품들을 네트웍 상에서 상호 접속 운용을 하기 위해서는 표준에 적합하게 구현되었는지, 상호운용성에는 문제가 없는지 등에 대한 사전 검증이 필요하다.

이러한 검증을 위한 LDAP 상호운용성 및 표준 적합성 시험 시스템이 국내에는 구현 되어있지 않은 실정이며, 국외의 경우는 Open Group, AT&T Lab, Mind Craft 등에서 시험 도구 및 시험 스위트를 제시하고 있다. 그러나 이들은 시험을 위한 비용 부담이 많으며, 시험도구 설치를 위한 기반 OS에 따른 제약조건으로 인한 설치의 어려움이 많아 효율적이지 못하다[1][9][10].

뿐만 아니라 이들 시험도구는 시험 항목과 소스가 개방되어 있지 않아 새로운 시험항목 추가 및 시험 항목의 수정을 위한 접근이 어렵다. 이러한 문제점들을 해결하기 위한 방법으로 개발 시간 단축과 시험 항목의 추가 및 변경을 위해 객체 지향적 접근이 요구된다. 객체 지향 접근과 OS에 따른 문제를 해결하기 위해는 OS의 제약이 없고, 객체 지향 언어 자바를 이용할 수 있다. 그러므로 본 논문에서는 II장에서 LDAP 상호운용성 시험 구성에 대해 논의하고, III장에서 개발 시간 단축과 시험 항목의 추가 및 변경을 위해 객체 지향적 접근을 통한 시험 구현에 대해 기술한다. IV장에서 구현한 시험도구를 사용한 상호운용성 시험 결과 분석에 대해 기술하고 V장에서 결론을 맺는다.

II. LDAP 상호운용성 시험

LDAP은 RFC 2251에 의해 정의된 표준으로 그림 1에서 보는 바와 같이 TCP/IP 기반에서 클라이언트와 서버, 서버와 서버사이의 상호동작을 규정한 것이다.

LDAP 표준은 디렉토리 서버에 간단히 읽기/쓰기 동작을 하는 관리 프로그램이나 클라이언트 어플리케이션 프로그램에 특히 적합하도록 되어있다.

LDAP 표준을 적용한 서버 및 어플리케이션 제품들이 많이 출시 되어 있지만 상호간의 접속운용 시 상이한 표준해석이나 개발접근방법의 차이 등에 의해 문제가 발생할 수 있는 소지를 안고 있다. 따라서 동일한 LDAP 표준에 의해 구현된 제품들이라도 상호간의 접속운용 시 상호운용성에 대한 시험이 우선되어야 한다.

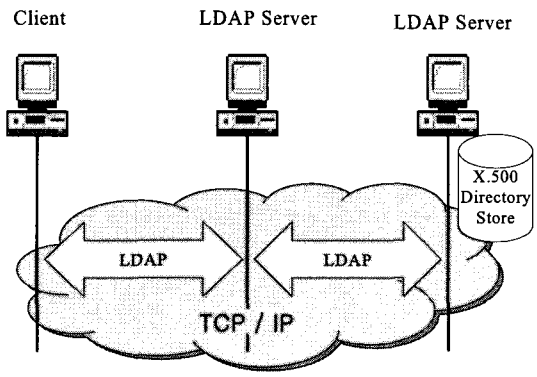


그림 1. LDAP 적용 범위

LDAP에 관한 시험으로는 LDAP를 기반으로 구현한 제품의 세부적인 기능들이 RFC 문서(2251~2256)에서 기술한 표준규격의 내용과 일치하는가를 시험하기 위한 표준 적합성 시험과 여러 벤더에서 구현한 LDAP 서버의 기능을 확인하고 서버와 클라이언트 사이에서 클라이언트의 요구에 대한 서버의 응답이 올바른지를 시험하기위한 상호운용성 시험이 있다. 표준 적합성과 상호운용성 시험의 관계는 그림 2에서와 같이 표준적합성 시험이 선행되어야 하며, 표준 적합성이 검증되지 않은 제품에 대한 상호운용성의 시험은 의미가 없다.

그러므로 구현한 시험도구의 타당성 검토를 위한 시험에서 시험 대상이 된 두개의 LDAP 서버는 표준 적합성 시험을 완료한 것으로 가정하였다.

현재 표준 적합성과 상호운용성 시험을 위해 구현된 시험도구가 국내에는 구축되지 못한 실정이며, 국외 벤더에 의해 구현된 시험도구로는 OpenGROUP의 VSLDAP과 "Security Testing of Protocol Implementation"의 프로젝트의 부산물로 나온 test suite로 PROTOS Test Suit : c06-ldapv3가 있다.

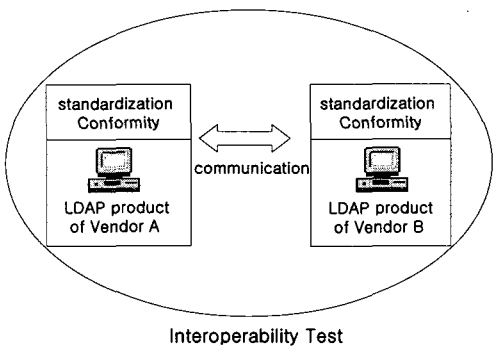


그림 2. 표준 적합성과 상호운용성의 관계

PRPTOS Test Suit의 경우는 총 6688개의 Test case가 있으나 시험 항목의 내용은 확인을 할 수가 없다. 그리고 시험 항목으로는 AT&T Lab에서 LDAP 클라이언트/서버 사이의 상호운용성 시험을 위해 고안한 BLITS가 있다[7][9]. 현재 BLITS는 OpenGROUP에서 관리되며, 현재 BLITS 3.0 Test Cases로 되어있다. 그러나 이들 시험도구는 소스가 개방되어 있지 않아 새로운 시험항목의 추가 또는 시험항목의 삭제를 위한 접근이 어려운 실정이다. 또한 LDAP 시험을 위해서는 많은 비용을 부담해야 하는 어려움이 있어 국내 실정에 맞는 LDAP 시험 도구 구현이 요구된다.

다음 장에서 일반에게 개방되어 있어 누구라도 시험항목을 이용해 시험도구를 개발할 수 있는 BLITS를 기반으로 한 LDAP 시험 도구 구현에 대해 기술 한다.

Ⅲ. LDAP 시험 도구 구현

BLITS는 시험을 수행하기위한 시험 항목과 시험 대상이 되는 서버에 저장될 데이터로 구성되어 있다. 서버에 저장될 데이터는 ldif 파일로 되어 있으며, OpenGROUP 홈페이지에서 다운받아 시험하고자 하는 서버에 먼저 저장되어 있어야 한다.

BLITS에서 제시된 시험항목들은 그림 3과 같이 LDAP에서 정의된 클라이언트의 요구에 따른 서버의 응답에 대한 동작으로 구성되어 있다.

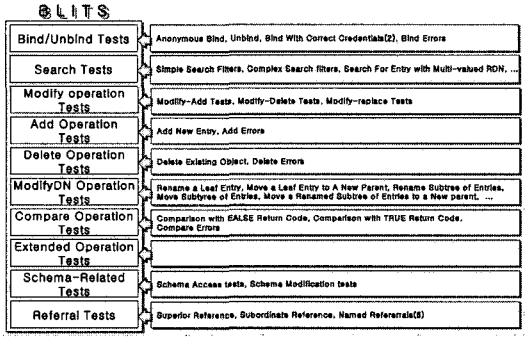


그림 3. BLITS에서 제시한 시험 항목 구성

BLITS에 제시된 시험 수행 과정은 클라이언트에서 요구 메시지를 생성하여 서버로 전송하고, 서버로부터의 응답을 받아 예상된 결과와 비교하여 처리하게 된다. 또한 상호운용성 시험 결과는 시험 대상인 LDAP 서버들로부터 같은 결과를 받았을 때 상호운용성이 가능한 것으로 평가할 수 있다[7].

객체 지향 접근에 의해 시험도구의 개발을 용이하게 하기 위해 BLITS 시험항목 중 가장 기본이 되는 시험항목들을 선정하였다. 객체 지향 접근을 위한 기본 시험항목들은 그림 4와 같다. 기본 시험항목들을 바탕으로 객체를 생성하여 새로운 시험항목 추가 시 상속받아 재사용이 가능하다.

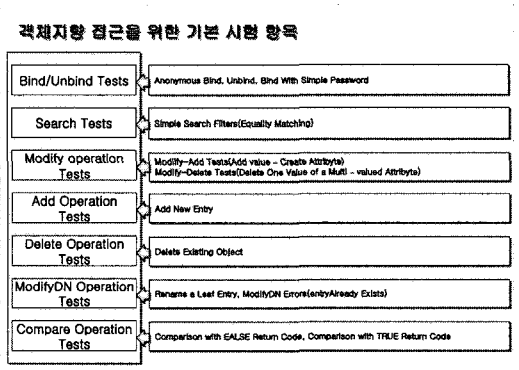


그림 4. 객체 지향 접근을 위한 기본 시험 항목

BLITS에 정의된 동작을 구현하기 위한 프로그래밍 언어로 OS의 제약이 없고, GUI 환경의 소프트웨어 구현이 쉬우며 객체 지향 언어인 JAVA를 사용하였다. 그리고 프로그래밍의 편의를 위해 Netscape에서 배포한 Netscape Directory SDK4.0을 사용하였다[8].

이러한 개발도구들을 사용하여 LDAP 메시지 생성을 위한 변수들과 LDAP 동작들을 수행하기 위한 메소드들을 가진 LdapTest 객체를 생성하였다. 객체에 포함된 메소드들과 메소드에 정의된 인자들의 자료형은 그림 5와 같다.

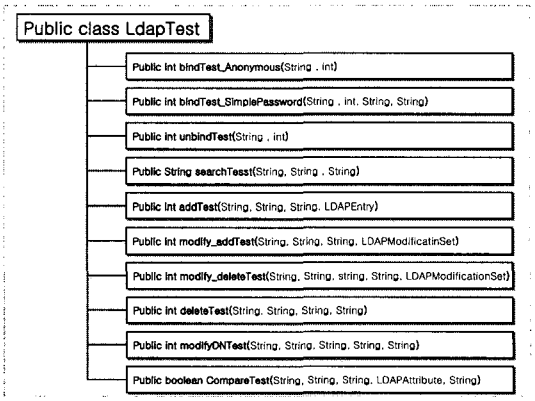


그림 5. LdapTest 객체에 정의된 메소드들과 인자의 자료형

새로운 시험항목을 추가할 경우 객체 지향 접근을 위해 LDAP의 기본 항목들을 정의한 LdapTest 객체의 상속을 통해 기본 항목에 새로운 데이터를 추가하여 시험을 위한 LDAP 메시지를 구성할수 있다. 새로 정의된 메시지를 전송하기 위해서는 LdapTest 객체에 정의된 메소드를 이용하여 전송할 수 있다. 또한 새로운 메시지를 전송하지 못 할 경우 LdapTest 객체를 바탕으로 메소드를 재 정의하여 메시지를 전송할 수 있다.

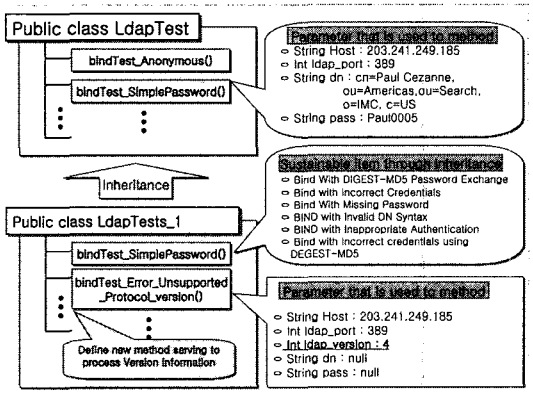


그림 6. LdapTest 객체 상속을 통한 Bind 시험 항목 추가

그림 6은 Bind 시험 항목 중 LdapTest 객체의 상속을 통한 시험 항목 추가를 나타낸 것이다. LDAP 서버 주소, 포트번호, dn, 패스워드와 같은 정보를 가지는 LDAP 메시지는 Bindtest_Simple Password() 메소드를 이용해 전송이 가능하다. 그러므로 시험 항목 중 Bind With DIGEST-MD5 Password Exchange, Bind with Incorrect Credentials, Bind with Missing Password와 같은 시험항목들은 LdapTest 객체를 상속받아 Bindtest_SimplePassword() 메소드를 재사용하여 메시지를 생성하고 메시지를 전송하는 것이 가능하다. 그러나 Bind with Unsupported Protocol Version 항목은 그림 6에서와 같이 버전에 대한 정보를 추가로 가지므로 버전정보를 가지지 못하는 Bindtest_Simple Password() 메소드로는 메시지 생성과 전송을 수행할 수 없다. 그러므로 LdapTest 객체를 상속 받아 버전 정보를 처리할 수 있는 메소드를 생성하면 버전 정보를 가지는 시험 항목에 대한 시험을 수행할 수 있다.

LDAP Search 시험 항목 중 서버주소, BaseDN, SearchFilter 정보만을 가지는 항목들은 searchTest() 메소드를 이용해 시험 가능하다. 그러나 그 외

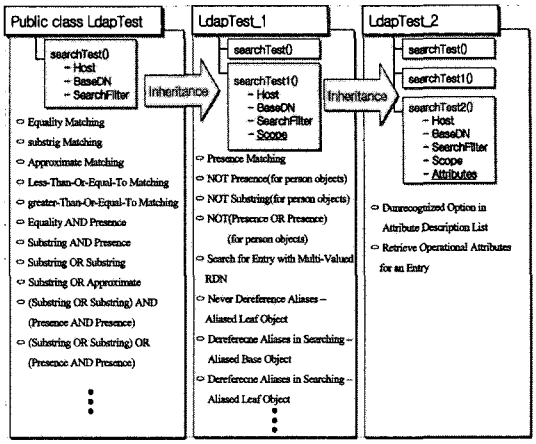


그림 7. LdapTest 객체 상속을 통한 Search 시험 항목 추가

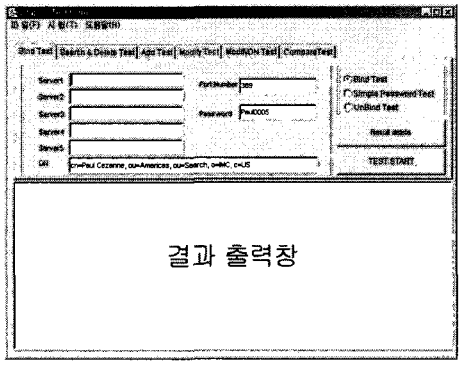
Scope과 Attribute 정보를 가지는 시험항목은 새로운 메소드를 정의해야 한다. 이 경우 LdapTest 객체를 상속받아 Scope 정보를 처리할 수 있는 메소드를 생성하면 Attribute 정보를 필요로 하는 두개의 항목을 제외한 모든 항목들에 대해 LDAP 메시지를 생성하고 메시지를 서버로 전송할 수 있어 시험항목 구현이 가능하다. 또한 LdapTest 객체를 상속 받아 생성한 객체를 다시 상속 받아 Attribute 정보를 처리할 수 있는 메소드 정의 하면 BLITS에서 제시한 모든 항목들에 대해 LDAP 메시지 생성과 메시지 전송이 가능하게 된다. 이후 새로운 항목을 추가할 경우 이 객체를 상속 받아 필요한 정보처리를 위한 매개 변수와 메소드들을 정의하면 항목을 쉽게 추가를 할 수 있다.

설계한 객체의 타당성을 확인하기 위해 기본 항목에 대해 시험을 수행할 수 있는 시험도구를 구현하였다. 구현한 시험 도구의 사용자 인터페이스는 그림 8의 (a), (b)에서와 같이 각각의 시험 항목별로 나누어 6개의 탭폼으로 구성하고, 시험 결과를 출력하기 위해 결과출력 창을 두어 시험 결과를 쉽게 확인 할 수 있게 구성하였다.

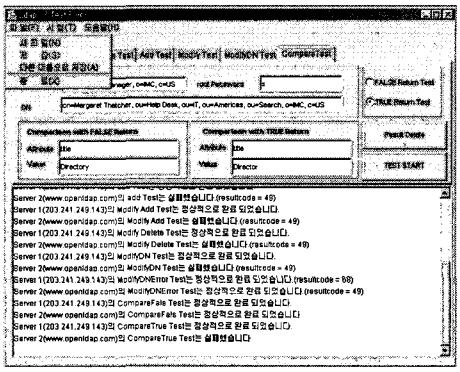
다음으로 구현한 시험도구를 사용하여 실제 LDAP 서버를 시험하고 시험 결과에 대해 기술한다.

Ⅳ. 시험 결과 분석

현재 LDAP 표준을 적용한 LDAP 디렉토리 서버가 많이 출시되어 있으나 이들 중 무료로 사용 가능한 제품은 openldap 서버가 있으며, 그 외 다른 제품은 비용을 부담해야 한다. 이런 이유로 구현한



(a) 초기 화면



(b) 시험 완료화면

그림 8. 시험도구 사용자 인터페이스

시험도구의 시험대상을 많은 종류의 LDAP 서버를 대상으로 할 수 없었다. 따라서 본 논문에서 실시한 LDAP 상호운용성 시험은 무료로 사용 가능한 openldap 서버를 리눅스에 구현하고, BLITS에서 정의 되어진 데이터를 저장한 서버와 이미 구현되어 일부 데이터가 공개되어 있는 www.openldap.com의 주소를 가지는 LDAP 서버를 시험의 대상으로 선택하였다. 시험 대상이 된 LDAP서버 중 자체적으로 구현된 서버(203.241.249.185)는 관리자 권한을 가지고 있으며, 다른 하나는 관리자 권한을 가지고 있지 못하다. BLITS에서 제시한 시험항목 중 Anonymous Bind, Unbind, Search, Compare 와 같이 관리자 권한이 없이 시험이 가능한 것도 있으나 저장된 데이터의 수정이 필요한 대부분의 시험 항목은 LDAP 서버의 관리자 권한을 필요로 한다. 그러므로 관리자 권한이 없는 이미 구현된 서버에 대한 상호운용성 시험에서는 정확한 시험을 할 수가 없었다. 그러나 자체적으로 구현한 LDAP 서버는 관리자 권한을 가지고 있으므로 구현한 도구를 통해 시험한 결과 표 2에서 보는 바와 같이 선정된 시험항목에서 BLITS에서 제시한 결과와 같은 결과를 출력하여 구현한 시험도구가 정상적으로 동작함을 확인하였다.

시험 결과에서 기존 서버의 경우 Simple Search Filters 시험에서 실패라는 결과를 출력하였다. 이는 서버의 오 작동이 아닌 데이터의 불일치로 인한 것이다. 이를 증명하기 위해 이미 구현된 서버에 저장된 데이터를 기준으로 하여 시험항목을 일부 수정하고 시험한 결과 시험도구는 정상완료를 출력하였다. 이처럼 구현한 시험도구는 기존의 시험도구와 달리 데이터의 일부 수정을 통해 보다 유연성 있는 시험을 수행할 수 있었다.

표 2. LDAP v3 Test 시험 결과

시험항목	203.241.249.185	www.openldap.com
Anonymous Bind	정상 완료	정상 완료
Bind With Simple Password	정상 완료	LDAP Resultcode(49)
Unbind	정상 완료	정상 완료
Simple Search Filters	정상 완료	LDAP Resultcode(49)
Modify-Add	정상 완료	LDAP Resultcode(49)
Modify-Delete	정상 완료	LDAP Resultcode(49)
Add	정상 완료	LDAP Resultcode(49)
Delete	정상 완료	LDAP Resultcode(49)
ModifyDN(Rename a Leaf Entry))	정상 완료	LDAP Resultcode(49)
ModifyDN(entry Already Exists)	정상 완료	LDAP Resultcode(49)
Compare (FALSE)	정상 완료	정상 완료
Compare (TRUE)	정상 완료	실패

뿐만 아니라 LdapTest 객체를 이용해 구현한 시험 도구에서 기본 항목들 뿐만 아니라 그림 7에서와 같이 searchtest() 메소드를 사용해 시험 가능한 시험 항목을 대상으로 시험을 수행 하였다. 시험 결과 모든 시험에서 정상적인 결과를 출력함을 확인하여 객체지향 접근을 위해 생성한 기본 객체가 유용성이 있음을 확인 하였다.

V. 결 론

새로운 시험도구는 개발 시간의 단축과 시험 항목의 추가 및 변경을 위해 객체지향 접근이 요구된

다. 이를 위해 시험 항목 중 객체 지향 접근을 위해 선정된 기본항목들에 대해 객체를 생성하고, 생성한 객체를 이용해 시험도구를 구현하였다. LdapTest 객체와 구현한 시험도구의 유용성을 확인하기 위해 상호운용성 시험을 수행하였다. 시험 수행 결과 기본 시험 항목과 상속을 통해 시험 가능한 시험 항목들에 대해 모두 정상완료를 출력하여 시험도구의 타당성을 확인 하였다. 차후 LdapTest 객체의 상속을 통해 보다 많은 수의 시험항목을 구현 및 새로운 시험항목들을 추가할 경우에 보다 쉬운 접근이 가능할 것이다.

앞으로 국내 실정에 맞는 시험 도구를 구현하기 위해 보다 명확한 객체 구현이 필요할 것이다. 또한, 상호운용성과 표준적합성 시험뿐 아니라 서버로부터의 응답시간과 같은 정보를 이용하여 서버의 성능을 함께 시험할 수 있는 도구가 구현된다면 상호 접속 운영에 있어 많은 도움이 될 것으로 사료된다. 또한 시험도구 개발에 앞서 표준적합성 및 상호운용성 시험을 위한 시험항목의 개발과, 시험결과에 대해 인증 조건에 대한 명확한 정의가 선행 되어야 할 것이다.

참 고 문 헌

[1] M. Wahl, et. al. "Lightweight Directory Access Protocol(v3)", *IETF RFC 2251*, 1997

[2] M. Wahl, et. al. "Lightweight Directory Access Protocol(v3): attribute Syntax Definitions" IETF RFC 2252, 1997. 12

[3] M. Wahl, et. Al. "Lightweight Directory Access Protocol(v3): UTF-8 string Representation of Distinguished Naves" *IETF RFC 2253*, 1997. 12

[4] T. Howes, "The String Representation of LDAP Search Filters" IETF RFC 2254, 1997. 12

[5] T. Howes, M. Smith, "The LDAP URL Format" IETF RFC 2255, 1997. 12

[6] T. Howes, "The String Representation of LDAP search Filters" *IETF RFC 1960*, 1996. 7

[7] The Open GROUP, "BLITS 3.0 Test Cases" 2003. 4. 14 http://www.opengroup.org/dif/blit-spub/blits3.0 /cases.htm#1.

[8] Netscape Directory SDK 4.0 for Java Programmer's Guide

[9] 이승희, "LDAP 기술 및 동향 분석", *전자문서유통체계 개선방안 소과제*, 2001.11.

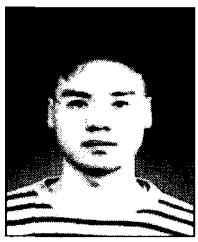
[10] 이승희, "LDAP 시험 방법 및 시험도구 분석", *전자문서유통체계 개선 방안 소과제*, 2002,03

[11] 최진주, "LDAP 프로토콜에 대한 고찰", *통신정보보호학회지 제9권 제1 호*, 1999. 03

[12] 김 철, "디렉토리 응용 서비스제공을 위한 Lightweight Directory access Protocol 구현" *한국정보과학회 봄 학술발표논문집*, 1996.

[13] 윤성순, "X.500과 LDAP의 비교 및 LDAP 프로그래밍", *한국정보과학회 가을 학술발표논문집*, 1997.

김 연 수 (Youn-sU Kim) 준회원



2002년 2월 인제대학교 정보통신공학과 졸업

2002년 3월~현재 인제대학교 전자정보통신공학과 석사과정

<관심분야> LDAP, Ehternet 시스템

이 승 희 (Soong-Hee Lee) 정회원

1987년 2월 경북대학교 전자공학과 학사

1990년 2월 경북대학교 전자공학과 대학원 석사

1995년 2월 경북대학교 전자공학과 대학원 박사

1987년~1996년 한국전자통신연구원 선임연구원

1997년 3월~현재 인제대학교 전자정보통신공학부 부교수

<관심분야> 초고속 통신망, NGcN, 통신 시스템

이 종 협 (Jong Hyup Lee) 정회원

1984년 고려대학교 산업공학과 학사

1986년 한국과학기술원(KAIST) 산업공학과 석사

1996년 한국과학기술원(KAIST) 산업공학과 박사

1986년~2004년 한국전자통신연구원 책임연구원 10GE S/W팀 팀장

2004년~현재 인제대학교 전자정보통신공학부 조교수

<관심분야> High-speed Network Design and Routing, Switch and Router Technology, Network Protocols, Internet QoS