筑波大学技術報告
25: 54-58, 2005

LDAP を使った認証システムの構築

川上彰
筑波大学システム情報工学等支援室（情報システム管理班）
〒305-8573 茨城県つくば市天王台 1-1-1

概要

平成１６年９月に筑波大学学術情報メディアセンター大型・分散システムの更新が行われた。このシステムの一部である経営・政策科学研究科サテライトも更新され、３０台の Windows クライアントと Windows サーバ等が導入された。それらを利用するためのユーザ認証システムとして新たに LDAP サーバを導入した。更に、この LDAP サーバの機能を利用して他の様々な認証への応用についてもテストしたので、その結果を報告する。図１に全体のシステム構成を示す。

１．はじめに

LDAP(Lightweight Directory Access Protocol)は、あるキーに関連したデータをディレクトリと呼ばれる情報の集まりから効率よく取り出すための仕組みである。この LDAP 機能を利用することによって、Windows や Macintosh、UNIX 環境のユーザＩＤとパスワードを一元化することができる。つまり、どの環境においても同じユーザ ID とパスワードによって認証が可能であり、またどの環境からパスワードが変更されても、全ての環境で同時にパスワードの変更が行われる。更に WEB ページや無線 LAN アクセスポイントへのアクセス制限としても、この ID とパスワードを利用することができる。

今回は、Linux パソコンに LDAP サーバソフトウェアをインストールし、これを使って分散システムの Windows Sever 2003 と３０台の Windows クライアントパソコンを管理することにした。今回使用したサーバ（分散システムを除く）のハードウェアのスペックおよび主なソフトウェアとそのバージョンは表１のとおりである。

インターネット・サーバ上では、WEB サーバ、ファイルサーバ、ログインサーバ、FTP サーバ等のサーバ機能に加えて、Radius 認証で使用する SSL 証明書の発行等の機能を提供する。

２．LDAP サーバ

LDAP サーバは、障害時の対策としてマスタ、ス

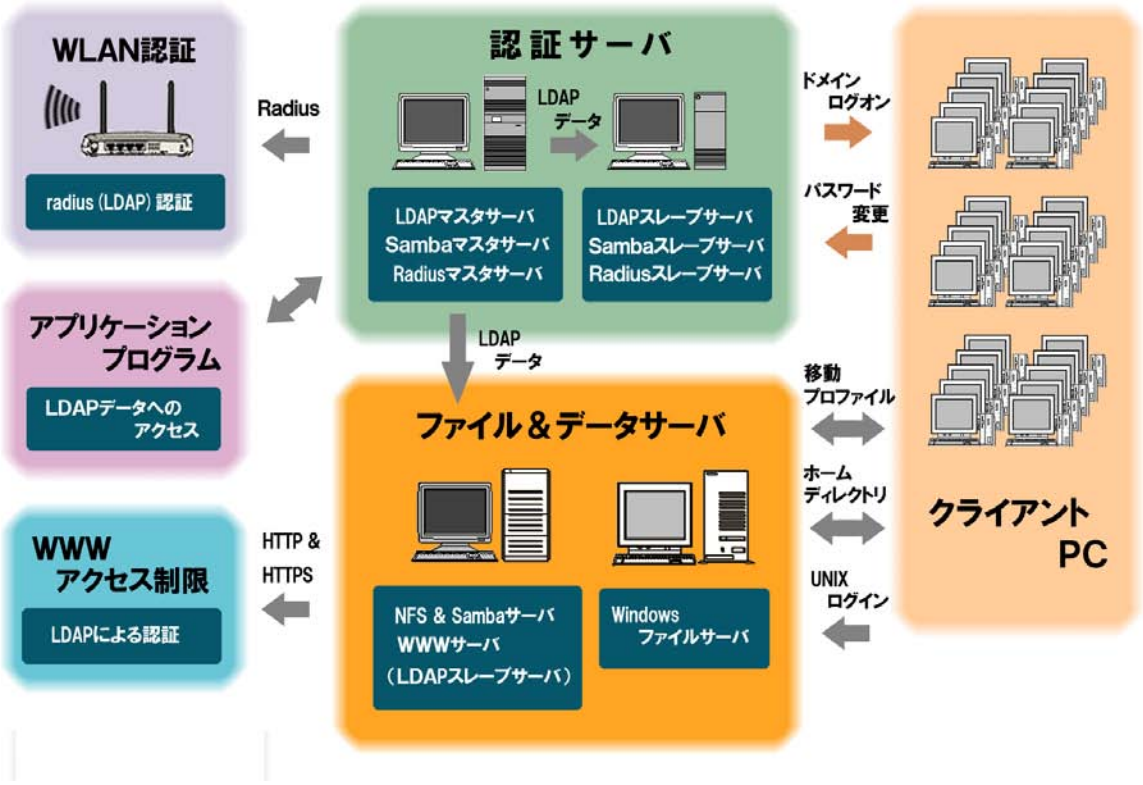

図１．システム構成

レーブ構成をとった。何れのサーバもＯＳには、Bonzai Linux（Debian Linux と互換ＯＳ）を使用し、LDAP サーバソフトウェアとしては OpenLDAP を使った。

LDAP サーバ用のソフトウェアとしては、今回使用した OpenLDAP 以外にも複数あるが、その中に Sun One Directory Server という製品が存在する。当初はこれを使う予定でいたが、ハードウェアの要求スペックや LDAP サーバと LDAP クライアントを同じ計算機上で実行できない等の制約のため断念した。ただし、Sun One Directory Server はマルチマスタ複製機能を有しているため、システム障害時の対応は OpenLDAP よりも容易なのではないかと思われる。

OpenLDAP のバックエンドのデータベースとしては BDB(BerkeleyDB)を、マスタサーバとスレーブサーバ間の通信の暗号化には OpenSSL による SSL/TLS 方式を用いた。nscd(Name Service Caching Daemon)を使用することによりアクセスの効率を上げることができるが、障害発生時の原因究明が難しくなることが懸念されたので、システムが安定して稼動した後で導入することにした。

３．インターネット・サーバ

一般ユーザのログインや FTP による接続、WEB アクセス等を行うため、安全性を考慮して認証用のサーバとは別にサーバを構築した。

3.1 WEB サーバ

WEB サーバ用のソフトウェアとしては、Apache (Version 1.3.26) を使用した。また、利用者のパソコンとサーバ間の情報を暗号化するために SSL モジュールを使用している。SSL の証明書は、このサーバ上に構築した自己署名型の認証局を使って発行し利用した。また、LDAP の情報を WEB 認証に利用するために、auth_ldap モジュールをインストールして使用した。

3.2 ファイルサーバ

経営政策科学研究科の学生は、授業等で社会工学類教育用計算機を利用する機会が多い。この計算機上の学生のホームディレクトリを経営政策科学研究科のサーバで NFS クライアントとしてマウントして利用できるようにした。

また、マウントした領域をサーバ上の Samba サーバを使って公開することにより、社会工学類教育用計算機の学生のホームディレクトリを経営政策科学研究科の Windows パソコンでマウントして利用できるようにしている。

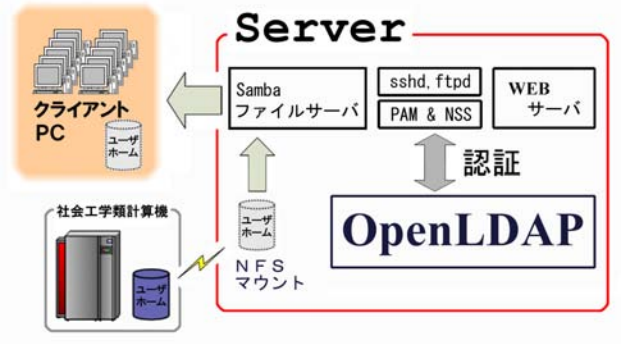

図２．ファイル共有

表１　ハードウェアとソフトウェアのスペック

		LDAP マスタサーバ	LDAP スレーブサーバ	インターネット・サーバ
ハードウェア	ＣＰＵ	Intel Xeon, 2.8GHz	Intel Pentium III, 866MHz	Intel Pentium III, 500MHz
	メモリサイズ	896MB	256MB	160MB
	ディスク容量	120GB	20GB	5GB
ソフトウェア	OS	Bonzai Linux (Ver. 3.2, kernel 2.4.20)		
	LDAP	OpenLDAP (Ver. 2.2.15)		
	Samba	Samba (3.0.4)		
	SSL	OpenSSL(0.9.7d)		
	Radius	FreeRADIUS (1.0.1)		
	WEB			Apache(1.3.26)
	FTP			WU-FTPD(2.6.2)

3.3 ログインサーバ

Telnet による通信は、ユーザ ID やパスワードを含む情報が、そのままネットワーク上を流れるため漏洩する危険性がある。このため、Telnet による接続を禁止して、SSH による接続のみ可能とした。sshd は inetd から起動することも可能であるが、ドキュメントの説明によるとデーモンとして実行することが推奨されている。これは、sshd の起動時にキーを生成する必要があり、このために時間を必要とし、クライアントは接続の度に待たされることになるためである。

また、/etc/hosts.allow と/etc/hosts.deny の２つのファイルによって、アクセスの許可と拒否を細かく設定することができる。このファイルは、TcpWrapper の設定でも使用され、inetd から起動される FTP 等の他のサービスに対するアクセスと共に設定することができる。

3.4 FTP サーバ

FTP サーバ用のソフトウェアとしては、ワシントン大学で開発された WU-FTPD が PAM(Pluggable Authentication Modules)、NSS(*Nameservice Switch)*への対応環境が整っていたので、これを使用した。また、現時点では通信内容の暗号化は行っていないが、今後検討する必要がある。接続に関しては、TcpWrapper を使用することによって特定のドメイン内からのみ接続を許可している。

3.5 SSL 自己署名型の認証局

SSL 証明書発行は、本来であれば信頼のできる認証機関によって発行してもらう必要があるが、費用や手続きの問題があるので、自己署名型の認証局を構築して利用することにした。

LDAP のマスタサーバとスレーブサーバとのデータ転送時に SSL 暗号化を行っている。これは転送データに含まれるユーザの ID やパスワードが外部に漏れることを防ぐためである。同様に WEB サーバとの通信や無線 LAN 通信における Radius サーバとの通信等に、このサーバを使って発行されたキーや証明書を使用している。

４．LDAP を利用した認証

4.1 Windows ドメイン環境

LDAP サーバ上に Samba（Version 3.0.4）をインストールし、Windows ドメインコントローラとした。LDAP マスタサーバとスレーブサーバ上に、それぞれ Samba をインストールし、同じく Samba マスタサーバと Samba スレーブサーバとした。このように設定することによって、２台のサーバの一方が障害等で停止しても継続して Windows ドメインコントローラとしての機能を提供することができる。

4.2 Linux ログインと FTP

Linux サーバへの SSH によるログインと FTP によるファイル転送については、PAM と NSS を設定することによって LDAP のユーザ情報を認証に利用することができる。

また、ログイン後にパスワードを変更すると、同時に Windows ログオン用のパスワードも変更することができる。ただし、passwd コマンドを使って変更すると、LDAP 情報内の UNIX ログイン用のパスワードは変更されるが、Samba のパスワードが変わらないため同期が取れなくなる。smbldap_tools に含まれる smbldap-passwd コマンドを使うと UNIX 用のパスワードと samba パスワードを同時に変更することができる。

4.3 無線 LAN アクセス

平成１５年度社会工学系技官研修で使用した手法をそのまま利用し、同じ環境を構築した。NAT ルータを使って既存のネットワークと無線 LAN 環境を分け、NAT ルータの DHCP サーバ機能を使ってパソコンにプライベートな IP アドレスを与える。また、無線 LAN のアクセスポイントは、IEEE802.1X に対応した製品であり、Radius サーバと交信して認証を行う。Radius サーバ用のソフトウェアとしては FreeRadius を使用した。

昨年度は EAP/TLS による認証を使用し、SSL 証明書を使った認証であったが、今回は加えて EAP/PEAP による認証もできるようにした。これは、LDAP データ内の NTLM ハッシュ値を使って行われている。

また、WEB を利用した SSL 証明書発行システムについても、昨年度作成したものに若干の修正を加えた。違いは、前回はユーザ認証の際に NIS によるユーザ ID とパスワードを使ったが、今回は LDAP データベース内のユーザ ID とパスワードによる WEB ページへのアクセス制限を利用して証明書の発行を行っている。（図３）

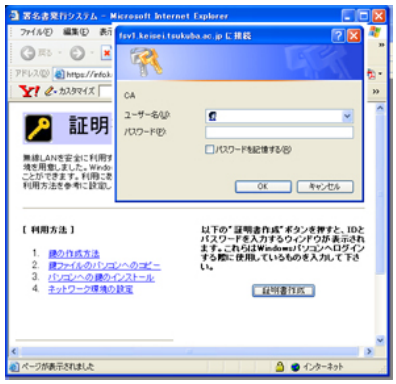

図３. SSL 証明書発行システム

4.4 WEB アクセス認証への利用

Apache に LDAP 用のモジュールを追加することによって、LDAP 内のユーザ ID とパスワードを WEB ページへのアクセス認証に利用することができる。

各利用者のディレクトリ内にアクセス制限のための設定ファイルを置くことにより、LDAP サーバに登録されたユーザ ID とパスワードによる認証が可能になる。設定ファイルの内容によって、LDAP サーバ上の全登録者、あるいは指定した特定の登録者に対してアクセスを許可し、許可された利用者はその WEB ページへのアクセスの際にユーザ ID とパスワードを入力することによってページを表示することができる。

LDAP サーバの情報を使わずに、このアクセス制限のための設定ファイルにアクセスを許可するユーザ ID とパスワードを直接記入して認証を行うことも

可能ではあるが、LDAP サーバの情報を利用することにより、ユーザ ID やパスワード管理が一元化できる点は大きなメリットである。

4.5 機器貸し出しシステム

学生に対する液晶プロジェクタやノートパソコンの貸し出しや返却を自動化するために、LDAP サーバのユーザ情報を用いた機器の貸し出しシステムを平成１６年度内の完成を目指して作成中である。

システムの構成は図４に示すとおりであり、利用者自身で機器の予約、貸し出し、返却を行うことができる。操作は全て WEB ブラウザで行い、LDAP サーバに登録されているユーザ ID とパスワードによって個人認証を行う。

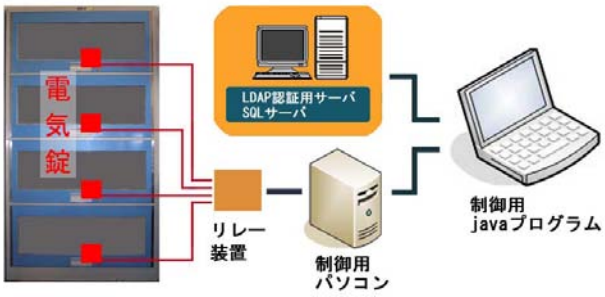

図４　システム構成

機器の予約、利用状況は図５のように表示される。利用者は、このページ上で希望する機器の部分をクリックし、自分のユーザ ID、パスワード、予約または貸し出しの期間等を入力する。貸し出しの場合は、機器を納めてあるキャビネットの扉が開錠状態になるので機器を取り出す。

ただし、完全に無人化するには若干不安な面もあるので、貸し出し用のキャビネットは一般利用者用のパソコンが設置してある部屋に置くことにした。この部屋は入室管理システムが導入されており、入室用のカードを持った利用者（経営政策科学研究科の学生および関係者）のみが入室することができる。また、監視用のカメラも設置されており、部屋の様子は常時録画されている。

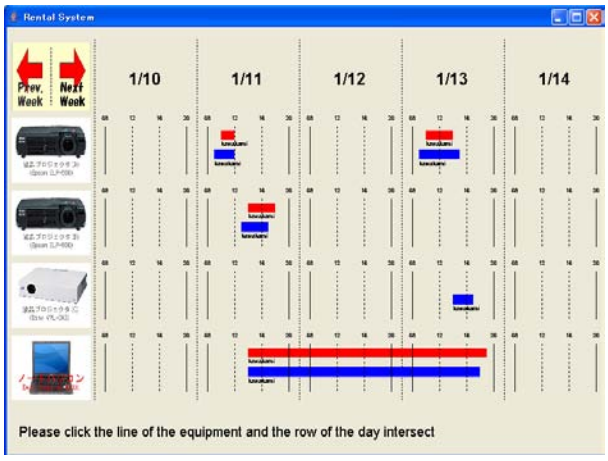

図５　貸出状況表示

５．障害時の対処

5.1 LDAP マスタサーバ障害時の対応

試験的に LDAP マスタサーバを停止して状況を確認した。Windows クライアントパソコンからドメインへのログオンは、スレーブサーバによる認証が機能することによって問題なく行うことができた。しかし、パスワードの変更は、スレーブサーバでは処理できないのでエラーが出て行うことはできなかった。UNIX 環境に於いても同じくログインは可能であるが、パスワードの変更はできなかった。WEB アクセス認証や無線 LAN アクセス認証は、問題なく行うことができた。

また、マスタサーバが復帰不能な状態に陥った場合は、次のような対処方法が考えられる。

(1) 現在 LDAP スレーブサーバとして稼動しているサーバを LDAP マスタサーバに変更して運用を続ける。
(2) 別なコンピュータを使って LDAP マスタサーバを再構築する。

(1)の方法は、スレーブサーバ上の LDAP 設定ファイル等を変更することによってマスタサーバに変更することができ、比較的短時間で対処することが可能である。ただし、スレーブサーバをマスタサーバとして利用するため、障害に対処するために新規に LDAP スレーブサーバを用意する必要がある。また、LDAP スレーブサーバと同じサーバにインストールされている Samba スレーブサーバも Samba マスタサーバとして設定を変更する必要がある。

(2)の方法の場合は、新規の LDAP マスタサーバを構築後にスレーブサーバの LDAP データベースの内容をマスターサーバにコピーする必要がある。

障害を起こしたマスタサーバの代替となる予備機がある場合は、（２）の方法で対処することが可能であるが、予備機がない場合は（１）の方法を取ることになる。

5.2 LDAP スレーブサーバ障害時の対応

LDAP スレーブサーバを停止して状況を確認した。マスタサーバが動作しているので、認証に関しては全て問題なく動作した。

次に、スレーブサーバが停止中にデータの変更があった場合、スレーブサーバが復帰後にその情報が正常に伝達され、スレーブサーバ側の情報も更新されるか確認した。パスワードの変更、新規ユーザの登録、ユーザの削除について試したが何れの場合も問題なく正常に更新された。

また、LDAP スレーブサーバを再構築した場合は、マスタサーバの LDAP データを手動でコピーした後、スレーブサーバを起動する必要がある。これは、マスタサーバ上での変更内容のみがスレーブサーバへ送信されるためである。

5.3 LDAP データベースのバックアップ

データのバックアップは、UNIX のクーロンジョブで１日に１回 slapcat コマンドを使って行っている。結果は LDIF 形式で、日にちごとに別のファイル名として保存されるようにした。

LDAP データベースの内容が壊れた場合は、バックエンドのデータベースとしてBDBを使用しているので、db_recover コマンドで修復できる場合が多かった。このコマンドで修復に失敗した場合は、LDIF 形式のファイルを使って戻すことができる。

６．今後の課題

6.1 Windows ドメイン管理

今回は、Samba サーバをドメインコントローラとして使用したが、Windows 環境のみで利用する場合はWindows サーバを使って Active Directory によるドメイン管理を行うのが一般的である。Samba をドメインコントローラとした場合、Windows サーバで提供されている機能の一部で利用できないものがある。

その１つにグループポリシー管理機能がある。これは別のソフトウェアを使って擬似的に同様のことを行うことは可能であるが、煩雑な操作を行う必要があり、また全く同じ機能を代替することはできない。このような Windows 環境固有の管理機能を Samba でどのように管理するか今後の課題である。

6.2 管理ツール

OpenLDAP には、管理用のツールとして必要最低限のものは用意されてはいるが、実際に運用するにあたっては十分とは言い難い。ユーザ情報の変更等に、その都度 LDIF 形式のファイルを作って操作するのでは非常に効率が悪い。業務として使用するためには、公開されている管理用のツールや自作ツール等を使って環境を整える必要がある。

6.3 障害対策

OpenLDAP は、LDAP データの複製方法としてシングルマスタレプリケーションを使っている。マスタサーバからスレーブサーバへデータの複製を行い、マスタサーバの障害時にはスレーブサーバが機能を代行する。別な方法としてマルチマスタレプリケーションによる複製方法がある。これは、Sun One Directory Server 等で採用されており、OpenLDAP も試験的にではあるが機能を提供している。

管理面で考えると、シングルマスタレプリケーションよりもマルチマスタレプリケーションによる複製方法をサポートしていることが望ましいのではあるが、別な方法として LDAP サーバをクラスタ構成にすることが考えられる。ただし、クラスタ構成にするためには、そのための機器とソフトウェアが必要となる。環境が揃えば、クラスタ構成による LDAP サーバの構成を試してみたい。

6.4 分散管理

LDAP は、referral という機能によって DNS のように各組織ごとに分散した管理体制をとることができる。例えば、経営政策科学研究科のユーザ情報と社会工学類のユーザ情報を別々に管理はするが、その情報を利用する上では、１つのまとまった情報として扱うことができる。今後、複数の組織への対応を含めて、LDAP の導入形態について再検討したい。

７．まとめ

LDAP によるユーザ情報の管理は、管理者のみならず利用者にとっても非常に有効な手段となりえるものと思われる。

管理者にとっては、機能別に複数のサーバに分散していたユーザ情報を１つにまとめることによってサーバの集中管理が可能になる。更に、全体を組織ごとに分割し、分散した管理を行うこともできる。

また、利用者にとっては、環境ごとに異なるユーザ ID とパスワードを利用することは非常に煩雑である。セキュリティ向上のためパスワードを定期的に変更すること等を考えると更に混乱を来たすことになるが、LDAP を利用することによって、これらを統合して１つのユーザ ID とパスワードにまとめることができる。

LDAP 環境を導入するにあたっては、いくつかの選択肢がある。今回はソフトウェアとして OpenLDAP を使用したが、他の商用ソフトウェア等も含めて、利用者の使用環境に適したものを導入する必要がある。その際は、障害時の対策やバックアップ方法、他のソフトウェアとの連携等と合わせて検討する必要がある。また、通信内容の暗号化についても必要不可欠な条件である。これらの環境は非常に速いスピードで変化しており、全てを常に最新の状態にすることは難しい。機能別に複数人でチームを作って対応する必要があるように思われる。

謝辞

LDAP 環境を構築するにあたっては、３台のパソコンをサーバとして利用した。これらの機器を提供して下さった経営政策科学研究科の糸井川研究科長ならびに高野技術専門職員に感謝いたします。また通信内容の暗号化等には SSL を使用しているが、これに関しては昨年度の「社会工学系技官研修」の成果が非常に有効であった。この研修にご理解、ご協力頂きました橋本教授には再度感謝いたします。

参考資料

[1] 稲地稔．OpenLDAP 入門－オープンソースではじめるディレクトリサービス，技術評論社(2003）

[2] Gerald Carter．LDAP－設定・管理・プログラミング－，オーム社(2003)

[3] LDAP 研究会．LDAP/OpenLDAP によるユーザ管理/認証ガイド，秀和システム(2004)

[4] 武田保真．徹底解説 Samba LDAP サーバ構築，技術評論社(2004)

[5] software Design 編集部. Software Design 2004 年 7 月号，技術評論社(2004) 17-70.